CHAPTER 21

Detecting Deceptive Intentions: Possibilities for Large-Scale Applications

Bennett Kleinberg, Arnoud Arntz and Bruno Verschuere

Introduction

In the 9/11 attacks, terrorists posed as regular passengers when they boarded and hijacked American Airlines Flight 11 (e.g., Wilgoren & Wong, 2001). What if one could have detected that they did not have the benign intention like other passengers of flying to San Francisco but that they instead had the malicious intent of committing a devastating terrorist attack. For law enforcement and intelligence practitioners, it is key to identify people with benign intent and those who need further security checks *before* they board an airplane. Terrorist attacks in New York, Madrid, London, and Brussels have motivated the academic deception community to develop methods that allow for the detection of deceptive intentions.

The vast majority of academic research on deception detection is limited to detecting deception on past events (Mac Giolla, Granhag, & Vrij, 2014; Vrij, Granhag, & Porter, 2010). However, as the 9/11 attacks illustrate, from a practitioner's perspective, it is the temporal dimension of the future that is of critical

B. Kleinberg (✉) · A. Arntz · B. Verschuere
University of Amsterdam, Amsterdam, The Netherlands
e-mail: bennett.kleinberg@ucl.ac.uk

A. Arntz
e-mail: A.R.Arntz@uva.nl

B. Verschuere
e-mail: B.J.Verschuere@uva.nl

B. Kleinberg
Department of Security and Crime Science, University College London, London, UK

T. Docan-Morgan (ed.), *The Palgrave Handbook of Deceptive Communication*, https://doi.org/10.1007/978-3-319-96334-1_21

importance when it comes to crime prevention, especially in the context of current threats of terrorist attacks. The aim of this chapter is to give an overview of the dominant deception detection theories and discuss existing interviewing approaches, methods, and cues to detecting deceptive intentions. We also outline which requirements an applied intentions-detection framework must meet.

Throughout this chapter, we focus on the applicability of existing approaches to real-world security processes on a large scale. We illustrate the challenges and requirements for applied deception detection tools on intentions through the example of airport passenger security operations. Throughout this chapter, we will adhere to Mac Giolla et al.'s (2014) definition of true and false intent. Accordingly, "true intent refers to a future action which [someone] *intends* to carry out, while [...] false intent refers to a future action that [they do] *not* intend to carry out" (p. 155). Since false intent does not necessarily imply a criminal element, we define malicious intent as *a future action someone intends to carry out that causes harm to others*. Although from a researcher's perspective both the detection of false *and* malicious intent are worth investigating, it is mainly the malicious intent in which practitioners working in crime prevention are interested. For example, prospective passengers lying about flying to New York for a conference hiding that they are having an affair there (false intent) are less relevant than someone hiding that they are planning to carry out an attack (malicious intent). We will discuss and address this challenge in this chapter as well.

This chapter is structured as follows. First, we discuss the problem of low base rate settings and then define a set of *criteria* for the detection of deceptive intentions on a large scale paying particular attention to the requirements from an applied perspective. We will use these criteria to evaluate the dominant deception theories, interviewing approaches, methods, and deception cues in the next sections. Second, we give a brief overview of main *theories of deception*, namely arousal-based and cognition-based deception detection, and evaluate to what extent they may guide large-scale applications. Third, we examine which *interviewing approaches* are most useful for deception detection. Fourth, we discuss some *information elicitation methods* that may help to increase deception detection validity. Fifth, we discuss which *cues* are most applicable to the airport screening context.

The Paradox of the Low Base Rate in Applied Settings

For the course of this chapter, we define the following context to which the deception detection system (i.e., *the system*) could be applied. Consider the problem of airport security professionals who have to determine for vast numbers of passengers, whether they potentially have malicious intent with their trip or not. With change on its way toward more seamless passenger flows during the whole security process (i.e., ideally minimizing the number of security checks and making them as least intrusive as possible), an area of interest for practitioners is the *pre*-screening of passengers *before* they arrive at the airport. Security processes at the airport could then flexibly be targeted at the specific intelligence requirements (e.g., which information needs further clarification) about each passenger. As such, a prospective screening system applied to that problem could function as the first filter in a system of multiple security layers, each of which would only subject those passengers to its test that "failed" the previous layers. By doing so, this system would address the problem of finding a needle in a haystack (e.g., someone with terrorist intentions among millions of ordinary passengers) by successively decreasing the size of the haystack. For the sake of argument, we will assume that the system will have to be able to screen up to 200,000 passengers each day on a single airport (e.g., London Heathrow: 205,000, Amsterdam Schiphol: 159,000, Paris Charles de Gaulle: 180,000; Airports Council International, 2016).

The large numbers of passengers, however, pose a particular statistical challenge for any screening tool. Let us assume a screening tool has a remarkable sensitivity (i.e., correctly identifying those that have malicious intent) and specificity (i.e., correctly identifying those that *do not* have malicious intent) of both 90%. What makes this particular context difficult, even for this highly accurate screening tool, is the low base rate (i.e., the small number of passengers with malicious intent). When the base rate is low (e.g., 0.0001, see Honts & Hartwig, 2014), even a highly accurate screening tool results in a large number of false positives; that is, it classifies ordinary passengers incorrectly as having malicious intent, simply as a function of the imbalance toward passengers without malicious intent. Table 21.1 illustrates that for 200,000 passengers, the percentage of correct identifications of malicious intentions when the screening tool indicates "*malicious intention*" (i.e., the precision of the screening tool) is effectively only 0.09%. Consequently, 99.91% of the cases when the screening tool signals "*malicious intention*" are false positives. This base rate paradox emphasizes the challenge of the passenger screening context and highlights the need for successive filters.

A cascading filter system could address this problem given that the assumption of statistical independence of indicators is met. Let us assume

Table 21.1 Illustration of the base rate problem for a fictitious screening tool with sensitivity and specificity of 90%

Outcome screening tool					
		Malicious intent	*No malicious intent*	*Total*	*Recall*
Reality	Malicious intent	18	2	20	**90%** (=sensitivity)
	No malicious intent	19,998	179,982	199,980	**90%** (=specificity)
	Total	20,016	179,984	200,000	
	Precision	**0.09%**	**99.99%**		

the screening tool A indicates the deceptive state X based on the criterion C_A with a sensitivity and specificity of 90% (Table 21.1). This, per definition, results in 10% false negatives and 10% false positives. Now let us further assume that the additional screening tool B is applied that also indicates deceptive state X but bases this decision on criterion C_B which is independent of (i.e., uncorrelated to) criterion C_A. In this case, the probabilities are conditional, that is, the percentages of miss-classifications[1] are multiplied and decrease to $0.10*0.10 = 0.01 = 1\%$. For n cascades, the probability of miss-classification is 0.01^n (e.g., for $n = 4$: $0.01^4 = 0.0001 = 0.01\%$). In the latter case, the precision of signaling "malicious intent" would increase from 0.09% ($n = 1$) to 50.00% ($n = 4$).

It is critical that cascades of security filters be independent of each other so that the occurrence of criterion C_B does not depend on the occurrence of criterion C_A; that is, both criteria are indicators of deceptive state X but measure it in different, unrelated ways. An example could be a system that indicates deception through the verbal content (e.g., what someone says) and the verbal style (e.g., how someone says it; see below). If both indicators are independent, this will allow for a combination of cascaded indicators through the analysis of verbal statements.

Criteria for Large-Scale Intention Detection Systems

A deception detection system applicable within the context of prospective airport passenger screening also poses particular challenges from an applied perspective. In this part of the chapter, we describe which requirements—besides high accuracies of identifying passengers correctly—such a system must meet. We discuss specific elements of an applied large-scale deception detection system that refer to its applicability on real-life purposes such as prospective airport passenger screening. To grasp applicability in its full complexity, we briefly outline sub-criteria relevant to the applicability of deception detection systems on large scale (see Table 21.2 for a summary).

Large-Scale Data Collection

The process of gathering data useful for an assessment of whether a passenger is to be believed or not is referred to here as data collection. While many deception studies relied on face-to-face interviews after participants committed a mock crime (e.g., preparing to place a malware USB stick in a shopping mall; Sooniste, Granhag, Knieps, & Vrij, 2013), the applied context here precludes such procedures. Collecting data through face-to-face interviews is to date the most corroborated form of eliciting cues to deception. However, it is logistically not realistic to conduct interviews with all passengers at the airport or to perform any other kind of disruptive intervention in the natural flow of passengers such as hands-on psychophysiological measurements (but see

Table 21.2 Summary of applicability criteria for large-scale deception detection systems

Criterion	*The deception detection system…*	*Research agenda*
Large-scale data collection	… permits collecting statements/responses from vast numbers of airport passengers simultaneously	Which are techniques and methods most suitable for the screening of 200,000 passengers per day?
Real-time data analysis	… entails an instant, automated analytical process to derive veracity judgments	Can deception cues (and the veracity of statements) be assessed reliably in real time?
Implementability	… is practically and logistically fit to be used in existing passenger procedures	How can validated techniques be incorporated into existing airport procedures?
Customer friendliness	… does only require a minimal amount of time and effort from the passenger	Can prospective passenger screening be done in short time with little passenger effort?
Theory-based	… is based on scientific theory and has withstood scientific evaluation	Which techniques and methods are the most promising for the detection of deceptive intentions?
Flexibility	… can flexibly be adapted to security requirements	Which techniques and methods allow for the highest flexibility in veracity assessments?
Granularity	… can determine the veracity of units of analysis smaller than the whole statement (e.g. single utterances)	Can the analysis of statements be fine-tuned toward the detection of deception in single utterances?

Panasiti et al., 2016; Warmelink et al., 2011). That impediment suggests that alternative forms of data collection must be explored and adopted. For example, a more likely approach is to use existing procedures in the airport security process where passengers could be asked brief questions, such as the standard queuing for baggage screening or online check-in processes that are becoming the norm. Large-scale data collection implies that the system is scalable to scores of passengers. The scalability means that the deception detection method is suitable to be applied to a large number of travelers (e.g., 200k per day) and can relatively easily be *up*-scaled without extensive investments in human workforce and training.

Real-Time Data Analysis

The analytical process must be automated to derive near real-time veracity judgments. Standard procedure from interviewing studies is that participants deliver a verbal statement about, for example, their whereabouts during an alleged mock crime. That oral statement is then transcribed and handed over to one, or preferably more, independent human coders who score statements on a range of criteria such as level of detail or plausibility (Sooniste et al., 2013; Sooniste, Granhag, Strömwall, & Vrij, 2015; Vrij, Granhag, Mann, & Leal, 2011; Warmelink, Vrij, Mann, & Granhag, 2013a). Manual coding is time-consuming and is currently not done in real time. Similarly, the number of tasks and checks performed by trained human coders—aside from the time constraints—is limited and prevents more complex tasks like verification of provided information and fine-grained coding of provided text statements (e.g., looking deeper than the overall text).

Implementability

A precondition for an approach to be used in real life is that it can be implemented into existing processes or by extending existing methods. For example, conducting face-to-face interviews with every passenger is not only logistically difficult, but it is also not implementable into the actual flow of current airport security systems because it takes too long and is too costly. In contrast to the general umbrella term of applicability, implementability has an additional, practical dimension, given logistical challenges, the feasibility of actually implementing a tool into security processes, as well as the potential of scaling the tool up to large numbers of people. From this follows that implementability subsumes applicability, but not vice versa.

Customer Friendliness

A further challenge for the application of deception detection tools is the inevitable compromise between academic rigor and stakeholders' interests. Although there are multiple aspects where the stakeholders' point of view might conflict with an academic's proposal (e.g., financial, ethical, theoretical), a noteworthy issue is the brevity of the developed system and the inconvenience caused to passengers. For external stakeholders, time is a premium and passengers' satisfaction is a vital ingredient for a thriving business. However, this puts the academic researcher into an unusual position. A standard polygraph examination, for instance, typically takes several hours (Meijer & Verschuere, 2010). Applied deception detection systems should ideally not exceed a few minutes' duration and should require as little effort from the passengers as possible (Honts & Hartwig, 2014). Computer-automated techniques would greatly facilitate data collection and veracity judgments within a short time.

Theory-Based

We think another requirement for a large-scale deception detection system is that it is built on a sound scientific theory. A simple "whatever works" approach is questionable for the airport screening context in the absence of a guiding theory. Without a theoretical base for the tools used, any future development within that line of deception research will hang loosely in a vacuum of results without being able to derive predictions on how these results came about. With an increasing acceptance in psychological research of methods from machine learning, however, it will be interesting to see how large data-driven investigations compare to typically smaller, theory-led approaches (for an overview paper on the issue, see Yarkoni & Westfall, 2017).

To illustrate the need for scientific theory in the development of security tools, consider the extreme example of the IED detector called *Advanced Detection Equipment* (*ADE-101*). The *ADE-101* was sold to various governments with the promise that this device could "pick up the most minuscule traces of explosives, drugs, ivory and even money" (Morris, Jones, & Booth, 2013, para. 1). In fact, that device was little more than a golf ball finder sold by a fraudulent businessperson. The *ADE-101* had cost the Iraqi authorities alone more than GBP 55 million (Booth, 2013). Besides the obvious fraud involved in this case, there was no theory behind the alleged working mechanisms of the device, nor was there an empirical validation of its effectiveness.

Flexibility

A system applied for passenger screening purposes must be flexible on passenger numbers, security risk estimations, and specific flight characteristics. For example, when there is a heightened security risk (e.g., due to previous terrorist attacks), a large-scale screening system must be able to adapt to that situation by adjusting the cutoff used to make a decision. Dynamic filtering would imply altering the compromise between sensitivity (i.e., the true positives) and specificity (i.e., the true negatives). Under specific circumstances, specificity might be favored over higher sensitivity; under other circumstances, the opposite might be needed.

Granularity

Granularity refers to how fine-grained the judgments made by a deception detection tool are. That is, granularity represents a continuum from coarse judgments (e.g., liar vs. truth-teller) to finer resolutions such as single utterances. Whereas in controlled experimental studies, the liars are typically instructed to tell an outright lie (e.g., pretending to have played a game whereas, in fact, they stole money; Vrij, 2008), a lying passenger can likely *embed* their lie into a mainly honest account (see Mac Giolla et al., 2014). This implies that it does not longer suffice to use the person who is lying as the unit of analysis (i.e., who is a liar and who a truth-teller). Rather a more granular analysis is needed that permits the investigator to determine, ideally, *what* someone is lying *about*. As we will see later in this chapter, current verbal content-based cues perform relatively poor on this requirement, whereas stylometric cues (e.g., Fornaciari & Poesio, 2013) may offer a path for the future. Alternatively, steps toward within-subjects deception investigations (i.e., having the same person tell a truthful account as well as a lie) might also offer a way to discern single deceptive aspects within whole statements (Vrij, 2016).

Deception Detection Theories

Most studies conducted on deception detection fall, broadly speaking, into one of the two dominant theories on deception: arousal-based versus cognition-based deception detection. They are rooted in different assumptions about the relationship between the mental state of deception and the cues through which this mental state is detectable.

Arousal-Based Deception Detection

The arousal theory holds that the mental state of lying can be inferred from arousal associated with lying (Vrij et al., 2010). The arousal-based assumption holds that the involuntary display of physiological signs of arousal is informative to the mental state of deception. For example, research into micro-expressions (Ekman, 2009; Schubert, 2006) poses that minimal muscular activity in the facial area is a cue to deception. Likewise, methods such as the Screening Passengers by Observation Technique(s) (SPOT; Honts & Hartwig, 2014) assume that lying is uniquely related to physiological and behavioral signs including body language and micro-expressions (see Honts & Hartwig, 2014; Perry & Gilbey, 2011). Consequently, a liar would be detectable through the mere observation of their overt behavior (Panasiti et al., 2016; Warmelink et al., 2011).

Cognition-Based Deception Detection

Starting with the notion that lying is cognitively more demanding than telling the truth (e.g., Zuckerman, DePaulo, & Rosenthal, 1981), the rationale of cognition-based deception detection is that increased cognitive load that comes along with lying results in the leakage of cues to deception (Masip, Sporer, Garrido, & Herrero, 2005; Oberlader et al., 2016; Vrij & Granhag, 2012). Various aspects reasonably make the act of lying harder than telling the truth. Consider a passenger flying to New York City (NYC) for a geography conference. When interviewed about the conference, they can easily tell about their plans and the preparation involved in their trip. Now let us assume a terrorist is planning an attack on NYC, but who claims to fly to NYC for the geography conference. The liar's task of convincing the investigator is probably harder than that for the truth-teller. Not only can the liar be thought of operating two accounts of their trip simultaneously, but they also have to maintain a convincing false account without risking the leakage of any hints alluding to their malicious plans.

Evaluation

The primary concern about arousal theory is that it falls prey to the so-called Othello error (for a historical explanation, see Vrij et al., 2010). The Othello error means that one ignores alternative explanations for the display of alleged cues to deception. While signs of stress may well accompany someone's lying, this does not exclude the possibility that someone telling the truth shows the same signs of stress. In a context such as an airport passenger screening, the issue of innocent stress becomes evident when one realizes that passengers rushing to catch their flight or traveling with small children will display physiological signs similar to those that are postulated to be uniquely related to lying.

There is increasing support for the cognition-based deception theory (Meissner et al., 2014; Vrij, Fisher, & Blank, 2017; but see also the critique by Levine, Blair, & Carpenter, 2018; and the response by Vrij, Blank, & Fisher, 2018). Despite the substantial evidence, it merits attention that the Othello error could also be at play for cognition-based deception theory. First, the rationale that lying is harder than telling the truth might not hold true for well-prepared or repeated lies. For example, if someone is repeatedly flying to NYC under pretense, the false story (e.g., a conference covering for an affair) is rehearsed and might therefore not be more difficult to tell than the truthful story. Second, the relative ease of telling the truth also depends on the complexity of the truth. Someone telling a complex true story (e.g., that they meet at a secret government facility for a classified meeting) may find it difficult to appear convincing—similar to someone lying about an activity. If someone is flying to a secret meeting about which they are not supposed to talk, the truthful account might be more difficult to tell than a simpler false account (i.e., that they are flying to a conference). Although the Othello error is arguably less problematic for cognition-based deception theory, future research should address these questions to refine cognition-based deception theory further.

Based upon the scientific support, the cognitive deception theory seems more promising than arousal-based deception detection in the context of passenger screening. Regardless of the particular deception theory, cues to deception (i.e., nonverbal and verbal indicators of the interviewee that are informative to the veracity of the statement made by the interviewee) are small and unreliable (DePaulo et al., 2003). The use of those cues for deception detection, therefore, requires approaches that can increase the occurrence of the cues in truth-tellers and decrease the occurrence in liars, or vice versa (Vrij & Granhag, 2012). In the next part of this chapter, we discuss approaches to eliciting cues to deception.

Approaches to Suspect Interviewing

No matter how brief (e.g., “No”) or long (e.g., “I booked my ticket last Thursday online through…”), the minimal requirement for any deception detection approach is a statement. There are two broad approaches to eliciting a statement from an interviewee (Meissner et al., 2014): the accusatorial approach and the information-gathering approach.

The Accusatorial Approach

The accusatorial approach to suspect interviewing is based on the rationale that the interviewer needs to engage actively in the interview to elicit admissions of intentional wrongdoing (Meissner et al., 2014). The accusatorial approach involves an interviewer who is trained to exert control over the interviewee, applies techniques to manipulate the interviewee psychologically, and typically asks closed (e.g., yes/no) questions. A formulation of the widely used accusatorial approach is the Reid technique (Gallini, 2010; Kassin et al., 2010), which consists of two phases. In the first step, the suspect is interviewed to determine whether they are indeed a likely suspect. The second phase of the Reid technique consists of techniques targeted at obtaining confessions from the suspect through a set of techniques that manipulate the suspect (i.e., custody and isolation, confrontation, minimization; see Kassin and Gudjonsson, 2004).

The Information-Gathering Approach

According to Meissner et al. (2014; see also Swanner, Meissner, Atkinson, & Dianiska, 2016), the key ingredients of the information-gathering approach are establishing rapport with the interviewee (e.g., positive affirmations, interest, calmness; see Evans et al., 2014), using positive confrontation and asking open-ended questions. The goal of the information-gathering approach—eliciting information—is strikingly different from the accusatorial approach which is obtaining confessions. Rooted in the cognitive interview (e.g., Fisher & Geiselman, 1992; Fisher, Geiselman, & Amador, 1989; for a recent meta-analytical overview, see Memon, Meissner, & Fraser, 2010), the information-gathering approach has a clear focus on treating the interviewee as a source of information rather than the possessor of guilt. As a result, the interviewing of victims, witnesses, and suspects does not radically differ since the goals are always to obtain relevant information.

Evaluation

Opponents of the accusatorial approach have voiced concerns about the fairness of the approach toward innocent interviewees. Studies suggest that the accusatorial approach does elicit confessions in guilty suspects but fails to protect those who have not committed any crime. Innocent subjects were found to provide false confessions merely as a function of a coercive interviewing style (Loney & Cutler, 2016; Meissner et al., 2014). Meissner et al. (2014) found the information-gathering approach better able to elicit true confessions and reduced the rate of false confessions as compared to the accusatorial approach. Not only does the elicitation of false confessions conflict with ethical standards in most countries (e.g., Soukara, Bull, Vrij, Turner, & Cherryman, 2009), they also impede the validity of the investigative interview (i.e., they do not elicit useful information). The accusatorial interviewing approaches (e.g., the Reid technique, see Kassin et al., 2010; the Behavioral Analysis Interview, Inbau, 2013) are the standard interviewing procedure in the US but have been banned from European countries as well as from the British, New Zealand, and Australian judicial system (Kassin et al., 2010; Meissner et al., 2014). Looking ahead, the release of the FBI's High-Value Detainee Interrogation Group (HIG) report (High-Value Detainee Interrogation Group, 2016) suggests that the US is also moving toward actively advocating an information-gathering approach. It is the information-gathering approach that has become the standard approach used in academic deception research (Vrij et al., 2017) and has been proposed for law enforcement and intelligence applications (Granhag, Vrij, & Meissner, 2014).

Since the accusatorial approach works mainly for the elicitation of confessions, one can imagine how this conflicts with the applicability. Given the low base rate of airport passengers with malicious intent, an approach that is inherently biased toward false positives such as the accusatorial approach, will lead to unsatisfyingly large numbers of false alarms. An unnecessarily inflated large number of false positives is highly undesirable from both a security practitioner's point of view since it redirects resources away from the actual problem (i.e., finding the true positives) and from the airport authority's perspective since each false alarm implies a falsely accused customer.

The accusatorial approach inherently assumes guilt, making an interview resemble an interrogation and putting interviewees directly under suspicion. To the contrary, the information-gathering approach is embedded in conservative assumptions about information that truth-tellers can provide but liars cannot, which has been shown to yield both more true confessions and fewer false confessions than the accusatorial approach. The information-gathering approach is more applicable to low base rate settings and is less offensive toward airport passengers of which the vast majority (e.g., 99.999%) has no malicious intent. Despite the moderate accuracy rates of the information-gathering approach, its conservative assumptions about the relationship between behavior and deception make it a more suitable approach for prospective airport passenger screening than the accusatorial approach.

Sooniste et al. (2015) found support for the information-gathering interviewing approach for the detection of true and false intent. Half of the participants planned a mock crime (i.e., installing malware on a university computer), whereas the other half planned an innocent activity (i.e., organizing a protest). Before enacting their task, both groups were instructed to convince an interviewer that they were organizing the protest. When participants were interviewed with the information-gathering approach (i.e., using the cognitive interview by establishing rapport, reinstating memory, and encouraging rich descriptions of activities) compared to a standard interviewing technique (i.e., without any of the information-gathering techniques), both liars and truth-tellers provided more detailed information. Crucially, the amount of information provided in the information-gathering interviews allowed for better truth–lie discrimination.

Based on the available scientific support and the higher customer friendliness, we believe the information-gathering interviewing approach is more suitable for airport passenger screening than the accusatorial approach. In the next part, we outline and evaluate different methods to eliciting information used within the information-gathering approach.

Methods for Eliciting Information

Within the information-gathering interviewing approach, several specific methods have been used to obtain more diagnostic veracity information from interviewees. In this part, we outline three promising methods relevant to the context of airport passenger screening.

Imposing Cognitive Load

An important method of cognition-based deception detection is imposing additional cognitive load to make the interview situation more cognitively demanding (Vrij et al., 2017). In particular, building on the existing differences in the cognitive effort involved in telling the truth versus lying, actively imposing additional cognitive load is postulated to create a situation that is even more difficult for the liar than for the truth-teller. Note, however, that imposing cognitive load is only one method of the cognitive approach to deception detection and these terms should not be used interchangeably (Vrij & Fisher, 2016). The rationale is that by directing mental efforts to a secondary task (e.g., maintaining eye contact, Vrij et al., 2010; holding a weight, Debey, Verschuere, & Crombez, 2012), cognitive resources become scarcer for the liar. Without many cognitive resources left, the liar will find it even harder to maintain a convincing false story; that is, they will have more trouble to lie successfully. Similarly, Vrij et al. (2008) proposed to instruct interviewees to recall an event in the reverse order. While this should be easier for truth-tellers, liars will be confronted with heightened cognitive load (see below).

Asking Unanticipated Questions

Based on the assumption that liars prepare for a suspect interview, Vrij et al. (2009) reasoned that providing spontaneous stories would be harder for liars than for truth-tellers (see also DePaulo et al., 2003; Masip et al., 2005). Whereas the liar and the truth-teller would be able to provide convincing answers to those questions that they expect, only the truth-teller will be able to do so for less expected questions where an answer needs to be formulated on the spot.

The Model Statement Technique

Recently, the information-gathering approach has been extended by providing an example of a detailed answer (e.g., Harvey, Vrij, Nahari, & Ludwig, 2017; Leal, Vrij, Warmelink, Vernham, & Fisher, 2015). The idea behind the so-called model statement technique is that although interviewees are typically asked to provide highly detailed answers, it is not certain whether they are aware of exactly how detailed that answer must be. One way to help interviewees is to provide them with an example of a detailed account of an event containing the expected level of detail.

Evaluation

Imposing cognitive load: Vrij et al. (2008; see also Evans, Michael, Meissner, & Brandon, 2013) imposed additional load on interviewees by asking half of their participants to recall an event in the regular, chronological order (i.e., beginning with the most distant), whereas the other half was instructed to remember the event in the reverse order (i.e., starting with the most recent and going stepwise back in time). Differences between truth-tellers and liars were magnified in the reverse order technique and allowed for better discrimination (for conflicting evidence, see Fenn, McGuire, Langben, & Blandón-Gitlin, 2015).

Asking unanticipated questions: In a first experiment, Vrij et al. (2009) devised an interview that asked a set of both anticipated questions (e.g., "Can you tell me in as much detail as possible what you did in the restaurant?") and *un*anticipated questions (e.g., "In relation to the front door, where did you sit?"; Vrij et al., 2009, p. 162) about the truthful or deceptive accounts of participants' whereabouts in a restaurant. Unanticipated questions revealed larger truth–lie differences than expected questions, especially if the unanticipated questions were about the spatial arrangement of the restaurant. The unexpected questions method has been used in multiple studies successfully (e.g., Shaw et al., 2013; Warmelink, Vrij, Mann, Leal, & Poletiek, 2013) and has emerged as a valuable method for exploiting and increasing differences between truth-tellers and liars (Vrij et al., 2017).

To test the unanticipated question technique on deceptive intentions, Sooniste et al. (2013) gave participants either an innocuous mission (i.e., buying gifts) or a mock criminal mission (i.e., placing a malicious USB stick in a shopping mall). Both groups prepared for this task, but those with a mock criminal story also developed their cover story, which was conceptually the same as the innocuous task. The authors found that questions about the planned activities directly did not elicit truth–lie differences. However, when asking questions regarding the planning of the activity (e.g., “What was the main goal of your planning?”), the truthful answers were perceived as more detailed than lies. A potential implication of this finding is that liars plan the activity in a different way than truth-tellers do. Although not many studies have investigated this explicitly yet, a possible explanation could stem from the questions anticipated by the liar: Sooniste et al.’s findings suggest that liars were more prepared to answer intentions-related questions than planning questions.

The model statement technique: Leal et al. (2015) presented participants with an audio-taped statement about an event (e.g., a Formula 2 race) unrelated to the research scenario (e.g., false or genuine insurance claims). They found that receiving the model statement previous to giving the statement affects truth-tellers and liars in different ways. For liars, there was no change in the human-judged plausibility between those who did and did not receive the model statement. To the contrary, for truth-tellers, the model statement resulted in more plausible statements, which suggests that the model statement was beneficial to the overall classification accuracy (non-cross-validated accuracies: 62.5% vs. 80.0%, without and with the model statement, respectively; for null-findings regarding the model statement see Bogaard, Meijer, & Vrij, 2014; Brackmann, Otgaar, Roos af Hjelmsäter, & Sauerland, 2017). To date, the model statement technique has not been assessed for the detectability of deceptive intentions.

Of the information elicitation methods discussed, the model statement method and asking unanticipated questions are the most promising for the detection of deceptive intentions (see also Vrij & Fisher, 2016). Imposing cognitive load is less applicable to the context of prospective passenger screening since it often requires active engagement with a secondary task or is related to future events that have not yet happened (e.g., for the reverse order technique). While the unanticipated questions method has successfully been used in experimental studies on intentions, for the model statement technique future research will have to explore how well they are suited for the study of deceptive intentions. Box 21.1 highlights important challenges for the research agenda of the detection of deceptive intentions. We will next discuss verbal cues that are used to detect deception.

Verbal Cues to Deception

Hundreds of cues have been proposed to determine whether a suspect is answering truthfully or deceptively (DePaulo et al., 2003). Cues range from behavioral (e.g., head nods, fidgeting) and physiological (e.g., eye muscle

Box 21.1 Outlook on the research agenda for the detection of deceptive intentions on a large scale

Research agenda
–Does model statement technique facilitate detection of deceptive intentions?
–Is the verifiability of detail rationale applicable to the detection of deceptive intentions?
–Can the scoring of verbal cues be computer-automated?
–Can the information-gathering approach be automated and shortened (e.g., chat-based information elicitation)?
–Can stylometric analysis be used to determine the content of lies?
–Can two (or more) independent (i.e., uncorrelated) verbal deception cues be derived from verbal statements (for cascaded screening)?

movements) to speech-related (e.g., vocal tension, pitch) and content-based cues (e.g., spontaneous corrections). From the perspective of the implementability, large-scale data collection, and granularity, we focus on verbal cues to deception, whereby we differentiate between content-based cues, the verifiability of information, and stylometric cues.

Content-Based Cues

Verbal deception detection assumes that the content of a statement (i.e., *what* the suspect says) is informative to the veracity of the declaration. Reality Monitoring provides a theoretical backcloth as to why the content of deceptive versus truthful statements would differ. Originally developed by Johnson and Raye (1981; Johnson, Bush, & Mitchell, 1998; Nahari & Vrij, 2014), Reality Monitoring was used to identify the source of a memory of an event. According to Reality Monitoring, a memory can be attributed either to an external source or to an internal source. A memory originating from the internal source has been constructed through cognitive operations (i.e., forming a memory of how the event *could have been*), whereas a memory attributable to the external source has been obtained through perceptual processes (i.e., the event *has been experienced genuinely*). The verbal accounts of events would, therefore, represent the source of the corresponding memory. If a memory stems from the external source, the account of the event in question should be richer in temporal, spatial, and perceptual details and should be more realistic, "reconstructable," and richer in affect than accounts of memories from the internal (i.e., fantasized) source.

The Verifiability Approach

An important addition to verbal cues to deception originates from the Verifiability Approach (Nahari, Leal, Vrij, Warmelink, & Vernham, 2014; Nahari, Vrij, & Fisher, 2014a). Liars face the dilemma between providing a believable account with sufficient detail and, at the same time, not mentioning any potentially incriminating information (i.e., those details that the interviewer could verify). Research showed that liars evade this dilemma by providing unverifiable details (Nahari et al., 2014a). For example, "I booked the trip together with someone I know" contains some details but is mainly non-verifiable, whereas "I booked the flight to New York with my friend Paul last Thursday" adds verifiable context to the same proposition. The Verifiability Approach set out to exploit this strategy by looking at how many verifiable details true and false statements contain.

Stylometric Cues

Rather than looking at *what* people convey in their verbal reports, researchers have also attempted to differentiate truthful from deceptive statements through *how* people convey their stories. The technique of stylometry postulates that one can attribute the identity of the author of a text to the stylistic features used in the text (e.g., Fornaciari & Poesio, 2013; Luyckx & Daelemans, 2008). In a stylometric analysis, a text is decomposed into features pertaining to *how* the text is written rather than which content the text conveys. Within stylometric analysis, Schler, Koppel, Argamon, and Pennebaker (2006) distinguish between surface-related features (e.g., the use of grammatical function words) and content-related features (i.e., the meaning of the words). In contrast to verbal content cues, the content-related features in stylometric analysis often stem from lexicons (e.g., the Linguistic Inquiry and Word Count software, Pennebaker, Boyd, Jordan, & Blackburn, 2015), assigning each word to a psychological dimension, for example. Whereas verbal content cues are about the semantic qualities of a whole statement, in the stylometric and linguistic analysis, the content-related features often are about the meaning and/or function of single words or tokens. Researchers typically use techniques from supervised machine learning to build algorithmic classifications of truthful and deceptive texts using a number of stylometric features (e.g., Fornaciari & Poesio, 2013, 2014; Mihalcea & Strapparava, 2009; Ott, Cardie, & Hancock, 2013; Ott, Choi, Cardie, & Hancock, 2011).

Evaluation

Content-based cues and Reality Monitoring: Using verbal content-based cues for the detection of deceptive intentions has only occurred since recently (e.g., Kleinberg, Nahari, Arntz, & Verschuere, 2017; Vrij, Granhag, et al., 2011; Warmelink, Vrij, Mann, & Granhag, 2013b). Vrij, Granhag, et al. (2011) conducted the first study using information-gathering interviewing principles to detect lies about intentions. In their experiment, they instructed departing passengers at an airport to either tell the truth about their upcoming flight or lie about it. In a subsequent interview, each participant answered a set of questions that were then transcribed and coded by human judges on content-based variables. They found that truth-tellers' statements were more plausible than liars' statements, contained more complications and more spontaneous corrections. Moreover, in another experiment, researchers compared the level of detail and plausibility of true and false statements about both past events and intentions (Vrij, Leal, Mann, & Granhag, 2011). They found that truthful answers to intention-related questions were more detailed and more plausible than deceptive answers.

Masip et al. (2005) found that the Reality Monitoring verbal content analysis tool is useful for the discrimination between truthful and deceptive statements with classification accuracy rates ranging between 65 and 75%. Separate cues from Reality Monitoring that have been shown to differ between deceptive and truthful statements are especially the plausibility of a statement (e.g., Leal et al., 2015; Vrij, Granhag, et al., 2011) and the richness of detail (e.g., Vrij et al., 2008; Warmelink, Vrij, Mann, Jundi, & Granhag, 2012).

The Verifiability Approach: A series of studies (e.g., Harvey et al., 2017; Jupe, Leal, Vrij, & Nahari, 2017; Nahari et al., 2014a) found that by looking at the amount of verifiable details, the discriminatory accuracy of verbal content analysis can be increased further with accuracy rates ranging between 67 and 90%. It is noteworthy that the Verifiability Approach seems relatively robust against countermeasures. When liars and truth-tellers were informed that verifiable details are indicative of the truthfulness of a statement, truth-tellers but not liars were able to provide more verifiable details (Nahari, Vrij, & Fisher, 2014b). Liars might simply not be willing to risk providing highly detailed information that the interviewer could potentially use against them (see also Kleinberg, Nahari, & Verschuere, 2016). Research on the Verifiability Approach for the detection of false intent is emerging and seems a worthwhile avenue for future research (Jupe et al., 2017).

Stylometric cues: With advances in computational methods, stylometric analysis has become more widespread in deception research (Fitzpatrick, Bachenko, & Fornaciari, 2015). For example, Ott et al. (2013) used machine learning classifiers to predict whether hotel reviews were truthful or deceptive. By adding variables such as the use of self-references (e.g., personal pronouns) and use of negative affect in the hotel reviews, they were able to devise a classifier that achieved up to 89.3% accuracy (see also Mihalcea & Strapparava, 2009; Ott et al., 2011). Using the same hotel review dataset, Feng and Hirst (2013) built stylometric profiles of deceptive and truthful hotel reviews (i.e., an average of a deceptive/truthful hotel review) and compared the profile compatibility of each review with the mean profile. They obtained a classification accuracy of up to 90.1%. Recent findings suggest that a combination of methodologies from computational linguistics (e.g., lexicon approaches and named entity recognition) might be a fruitful way to synthesize verbal deception theory and automated classification approaches (Kleinberg, Mozes, Arntz, & Verschuere, 2018).

Granularity

Content-based verbal cues such as the richness of detail are relatively ill-equipped to identify the veracity of smaller units of analysis (e.g., sentences, propositions, or utterances), but evidence suggests that stylometric cues might be useful to obtain a more granular level of analysis. For example, by zooming in on smaller parts within the entire statement, researchers changed the unit of analysis from whole texts to unique propositions made in court statements (Bachenko, Fitzpatrick, & Schonwetter, 2008; see also Fornaciari & Poesio, 2013). When the authors modeled verbal content constructs like inconsistencies using different indicators (e.g., verbal hedges: "maybe," "I guess"; verb tense change, thematic role change, noun phrase changes), they were able to correctly identify 75.6 and 73.8% of false and true propositions, respectively. Similarly, the verifiability of details might also offer paths toward more granular analyses: If the verifiability is used as a test of deception, rather than obtaining overall counts of verifiable details for a whole statement, one could explore whether small bits of verifiable information (e.g., names in single utterances) are informative to the truthfulness of parts of the entire declaration.

All of the three classes of verbal cues seem promising for the context of airport passenger screening. The more granular stylometric analysis and the paths open for the verifiability of details make these two types of cues particularly promising. Box 21.1 highlights questions for the research agenda on deceptive intentions.

The Controlled Cognitive Engagement

The Controlled Cognitive Engagement (CCE; Ormerod & Dando, 2015) is an illustration of a promising system that incorporates several of the discussed elements. To date, the CCE is the most extensive investigation of cognition-based deception detection on a larger scale in an airport screening context. The authors formulated six cornerstones for the CCE. The CCE method (1) was built on strategic interviewing principles, (2) aimed to elicit rich verbal accounts, (3) included tests of expected knowledge (e.g., someone claiming to fly to NYC should know where they are staying), (4) restricted verbal maneuvering (i.e., that the interviewee takes over the conversation), (5) contained elements that raised the cognitive load of respondents, and (6) looked at the content of statements to assess their veracity. Key features of the developed CCE method were question cycles consisting of an open question (e.g., "Please tell me about your plans in New York." [answer: "I'm attending the Geology conference there."]), a related focus question (e.g., "Who will you meet at the conference?" [answer: "Paul Johnson"]), and a test question (e.g., "Where do you know Paul Johnson from?" [answer: "He was my dissertation supervisor"]). By formulating this structure of asking questions without specifying the exact questions to be asked, the CCE method is sufficiently flexible to allow for custom-made interviews depending on each passenger's context. After training airport security practitioners in the use of CCE, Ormerod and Dando (2015) compared how well CCE-trained officers were able to identify participants who tried to pass through airport security with a fake identity. The CCE method (66% of mock passengers identified) outperformed the widely adopted yet not scientifically corroborated suspicious signs method (3%, i.e., identifying passengers based on their physical display of suspicious behavior). Despite its successful test in the reported experiment, the CCE method has yet to replicate independently. Moreover, further research must establish how systems similar to the CCE can be useful for prospective passenger screening while meeting the specific applied requirements formulated in this paper (e.g., for 200k passengers in a fast, non-intrusive way). In particular, the issues of scalability and the requirement to screen passengers before they arrive at the airport merit special attention. Nevertheless, the CCE illustrates how theory-based techniques can be used for airport passenger screening purposes, and it is imaginable that a system for prospective passenger screening is combined with in situ CCE screening in a cascaded system. Future research will have to extend such techniques toward even shorter, possibly non-intrusive methods (e.g., chat-based information elicitation online).

Conclusions

This chapter set out to review deception detection research for the applied context of prospective airport passenger screening. As a guideline for the various research aspects (theories, interviewing approaches, methods to information elicitation, and verbal cues to deception), we defined a set of requirements of an applicable deception detection system. The cognition-based deception theory and the information-gathering approach seem most promising. Both were found to be more supported by evidence and to fit the applied requirements better. Furthermore, asking unanticipated questions and the model statement technique are promising methods for the elicitation of useful information. Lastly, it was found that three kinds of verbal deception cues are relevant for the applied context (i.e., content-based cues, the verifiability of details, and stylometric cues), with the verifiability of details and the stylometric cues to be the most promising. This chapter closed with an illustration of the Controlled Cognitive Engagement as a potential predecessor tool for a truly large-scale prospective airport passenger screening tool.

Note

1. Here, miss-classification refers to both false positives and false negatives given that we assume a sensitivity and specificity of both 90%.

References

Airports Council International. (2016). Year to date passenger traffic, December 2015. Retrieved from http://www.aci.aero/Data-Centre/Monthly-Traffic-Data/Passenger-Summary/Year-to-date.

Bachenko, J., Fitzpatrick, E., & Schonwetter, M. (2008). Verification and implementation of language-based deception indicators in civil and criminal narratives. In *Proceedings of the 22nd International Conference on Computational Linguistics—Volume 1* (pp. 41–48). Association for Computational Linguistics. Retrieved from http://dl.acm.org/citation.cfm?id=1599087.

Bogaard, G., Meijer, E. H., & Vrij, A. (2014). Using an example statement increases information but does not increase accuracy of CBCA, RM, and SCAN: Using an example statement with truth tellers and liars. *Journal of Investigative Psychology and Offender Profiling, 11*(2), 151–163. https://doi.org/10.1002/jip.1409.

Booth, R. (2013). Fake bomb detector conman jailed for 10 years. *The Guardian*. Retrieved from https://www.theguardian.com/uk/2013/may/02/fake-bomb-detector-conman-jailed.

Brackmann, N., Otgaar, H., Roos af Hjelmsäter, E., & Sauerland, M. (2017). Testing a new approach to improve recall in different ages: Providing witnesses with a model statement. *Translational Issues in Psychological Science*, *3*(2), 131–142. https://doi.org/10.1037/tps0000116.

Debey, E., Verschuere, B., & Crombez, G. (2012). Lying and executive control: An experimental investigation using ego depletion and goal neglect. *Acta Psychologica, 140*(2), 133–141. https://doi.org/10.1016/j.actpsy.2012.03.004.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*(1), 74–118. https://doi.org/10.1037/0033-2909.129.1.74.

Ekman, P. (2009). *Telling lies: Clues to deceit in the marketplace, politics, and marriage* (4th ed.). New York: W. W. Norton.

Evans, J. R., Houston, K. A., Meissner, C. A., Ross, A. B., LaBianca, J. R., Woestehoff, S. A., & Kleinman, S. M. (2014). An Empirical Evaluation of Intelligence-gathering Interrogation Techniques from the United States Army Field Manual: Intelligence-gathering interrogation techniques. *Applied Cognitive Psychology*, *28*(6), 867–875. https://doi.org/10.1002/acp.3065.

Evans, J. R., Michael, S. W., Meissner, C. A., & Brandon, S. E. (2013). Validating a new assessment method for deception detection: Introducing a psychologically based credibility assessment tool. *Journal of Applied Research in Memory and Cognition, 2*(1), 33–41. https://doi.org/10.1016/j.jarmac.2013.02.002.

Feng, V. W., & Hirst, G. (2013). Detecting deceptive opinions with profile compatibility. In *IJCNLP* (pp. 338–346). Retrieved from ftp://128.100.3.31/dist/gh/Feng+Hirst-IJCNLP-2013.pdf.

Fenn, E., McGuire, M., Langben, S., & Blandón-Gitlin, I. (2015). A reverse order interview does not aid deception detection regarding intentions. *Frontiers in Psychology*, *6*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4553365/.

Fisher, R. P., & Geiselman, R. E. (1992). *Memory-enhancing techniques for investigative interviewing: The cognitive interview*. Springfield, IL: Thomas.

Fisher, R. P., Geiselman, R. E., & Amador, M. (1989). Field test of the cognitive interview: Enhancing the recollection of actual victims and witnesses of crime. *Journal of Applied Psychology, 74*(5), 722–727. https://doi.org/10.1037/0021-9010.74.5.722.

Fitzpatrick, E., Bachenko, J., & Fornaciari, T. (2015). *Automatic detection of verbal deception* (Vol. 8). Morgan & Claypool Publishers. Retrieved from http://www.morganclaypool.com/doi/abs/10.2200/S00656ED1V01Y201507HLT029.

Fornaciari, T., & Poesio, M. (2013). Automatic deception detection in Italian court cases. *Artificial Intelligence and Law, 21*(3), 303–340. https://doi.org/10.1007/s10506-013-9140-4.

Fornaciari, T., & Poesio, M. (2014). *Identifying fake Amazon reviews as learning from crowds*. Association for Computational Linguistics. Retrieved from http://repository.essex.ac.uk/id/eprint/14591.

Gallini, B. (2010). Police "science" in the interrogation room: Seventy years of pseudo-psychological interrogation methods to obtain inadmissible confessions. *Hastings Law Journal*, *61*, 529–577. https://scholarworks.uark.edu/lawpub/29/.

Granhag, P. A., Vrij, A., & Meissner, C. A. (2014). Information gathering in law enforcement and intelligence settings: Advancing theory and practice: Effective human intelligence gathering techniques. *Applied Cognitive Psychology, 28*(6), 815–816. https://doi.org/10.1002/acp.3093.

Harvey, A. C., Vrij, A., Nahari, G., & Ludwig, K. (2017). Applying the verifiability approach to insurance claims settings: Exploring the effect of the information protocol. *Legal and Criminological Psychology, 22*(1), 47–59.

High-Value Detainee Interrogation Group. (2016). Interrogation best practices report. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/file-repository/hig-report-august-2016.pdf/view.

Honts, C., & Hartwig, M. (2014). Credibility assessment at portals. In D. C. Raskin, C. Honts, & J. Kircher (Eds.), *Credibility assessment: Scientific research and applications* (pp. 37–62). San Diego: Academic Press.

Inbau, F. E. (Ed.). (2013). *Criminal interrogation and confessions* (5th ed.). Burlington, MA: Jones & Bartlett Learning.

Johnson, M. K., Bush, J. G., & Mitchell, K. J. (1998). Interpersonal reality monitoring: Judging the sources of other people's memories. *Social Cognition, 16*(2), 199–224.

Johnson, M. K., & Raye, C. L. (1981). Reality monitoring. *Psychological Review, 88*(1), 67–85. http://dx.doi.org/10.1037/0033-295X.88.1.67.

Jupe, L. M., Leal, S., Vrij, A., & Nahari, G. (2017). Applying the verifiability approach in an international airport setting. *Psychology, Crime & Law, 23*(8), 812–825. https://doi.org/10.1080/1068316X.2017.1327584.

Kassin, S. M., Drizin, S. A., Grisso, T., Gudjonsson, G. H., Leo, R. A., & Redlich, A. D. (2010). Police-induced confessions, risk factors, and recommendations: Looking ahead. *Law and Human Behavior, 34*(1), 49–52. https://doi.org/10.1007/s10979-010-9217-5.

Kassin, S. M., & Gudjonsson, G. H. (2004). The psychology of confessions: A review of the literature and issues. *Psychological Science in the Public Interest, 5*(2), 33–67. https://doi.org/10.1111/j.1529-1006.2004.00016.x.

Kleinberg, B., Mozes, M., Arntz, A., & Verschuere, B. (2018). Using named entities for computer-automated verbal deception detection. *Journal of Forensic Sciences, 63*(3), 714–723. https://doi.org/10.1111/1556-4029.13645.

Kleinberg, B., Nahari, G., Arntz, A., & Verschuere, B. (2017). An investigation on the detectability of deceptive intent about flying through verbal deception detection. *Collabra: Psychology*. https://doi.org/10.1525/collabra.80.

Kleinberg, B., Nahari, G., & Verschuere, B. (2016). Using the verifiability of details as a test of deception: A conceptual framework for the automation of the verifiability approach. In *Proceedings of NAACL-HLT* (pp. 18–25). Retrieved from http://www.anthology.aclweb.org/W/W16/W16-0803.pdf.

Leal, S., Vrij, A., Warmelink, L., Vernham, Z., & Fisher, R. P. (2015). You cannot hide your telephone lies: Providing a model statement as an aid to detect deception in insurance telephone calls. *Legal and Criminological Psychology, 20*(1), 129–146.

Levine, T. R., Blair, J. P., & Carpenter, C. J. (2018). A critical look at meta-analytic evidence for the cognitive approach to lie detection: A re-examination of Vrij, Fisher, and Blank (2017). *Legal and Criminological Psychology, 23*(1), 7–19. https://doi.org/10.1111/lcrp.12115.

Loney, D. M., & Cutler, B. L. (2016). Coercive interrogation of eyewitnesses can produce false accusations. *Journal of Police and Criminal Psychology, 31*(1), 29–36. https://doi.org/10.1007/s11896-015-9165-6.

Luyckx, K., & Daelemans, W. (2008). Authorship attribution and verification with many authors and limited data. In *Proceedings of the 22nd International Conference on Computational Linguistics* (Vol. 1, pp. 513–520). Stroudsburg, PA: Association for Computational Linguistics.

Mac Giolla, E., Granhag, P. A., & Vrij, A. (2014). Discriminating between true and false intentions. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Detecting deception* (pp. 155–173). Chichester, UK: Wiley. https://doi.org/10.1002/9781118510001.ch7.

Masip, J., Sporer, S. L., Garrido, E., & Herrero, C. (2005). The detection of deception with the reality monitoring approach: A review of the empirical evidence. *Psychology, Crime & Law, 11*(1), 99–122. https://doi.org/10.1080/10683160410001726356.

Meijer, E. H., & Verschuere, B. (2010). The polygraph and the detection of deception. *Journal of Forensic Psychology Practice, 10*(4), 325–338. https://doi.org/10.1080/15228932.2010.481237.

Meissner, C. A., Redlich, A. D., Michael, S. W., Evans, J. R., Camilletti, C. R., Bhatt, S., et al. (2014). Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review. *Journal of Experimental Criminology, 10*(4), 459–486. https://doi.org/10.1007/s11292-014-9207-6.

Memon, A., Meissner, C. A., & Fraser, J. (2010). The cognitive interview: A meta-analytic review and study space analysis of the past 25 years. *Psychology, Public Policy, and Law, 16*(4), 340–372. https://doi.org/10.1037/a0020518.

Mihalcea, R., & Strapparava, C. (2009). The lie detector: Explorations in the automatic recognition of deceptive language. In *Proceedings of the ACL-IJCNLP 2009 Conference Short Papers* (pp. 309–312). Association for Computational Linguistics. Retrieved from http://dl.acm.org/citation.cfm?id=1667679.

Morris, S., Jones, M., & Booth, R. (2013). The "magic" bomb detector that endangered lives all over the world. *The Guardian*. Retrieved from https://www.theguardian.com/uk/2013/apr/23/magic-bomb-detector-lives-risk.

Nahari, G., Leal, S., Vrij, A., Warmelink, L., & Vernham, Z. (2014). Did somebody see it? Applying the verifiability approach to insurance claim interviews: The verifiability approach in insurance interviews. *Journal of Investigative Psychology and Offender Profiling, 11*(3), 237–243. https://doi.org/10.1002/jip.1417.

Nahari, G., & Vrij, A. (2014). Are you as good as me at telling a story? Individual differences in interpersonal reality monitoring. *Psychology, Crime & Law, 20*(6), 573–583.

Nahari, G., Vrij, A., & Fisher, R. P. (2014a). Exploiting liars' verbal strategies by examining the verifiability of details. *Legal and Criminological Psychology, 19*(2), 227–239. https://doi.org/10.1111/j.2044-8333.2012.02069.x.

Nahari, G., Vrij, A., & Fisher, R. P. (2014b). The verifiability approach: Countermeasures Facilitate its ability to discriminate between truths and lies: The verifiability approach and countermeasures. *Applied Cognitive Psychology, 28*(1), 122–128. https://doi.org/10.1002/acp.2974.

Oberlader, V. A., Naefgen, C., Koppehele-Goseel, J., Quinten, L., Banse, R., & Schmidt, A. F. (2016). Validity of content-based techniques to distinguish true and fabricated statements: A meta-analysis. *Law and Human Behavior, 40*(4), 440–457.

Ormerod, T. C., & Dando, C. J. (2015). Finding a needle in a haystack: Toward a psychologically informed method for aviation security screening. *Journal of Experimental Psychology: General, 144*(1), 76–84. https://doi.org/10.1037/xge0000030.

Ott, M., Cardie, C., & Hancock, J. T. (2013). Negative deceptive opinion spam. In *HLT-NAACL* (pp. 497–501). Retrieved from http://www.aclweb.org/website/old_anthology/N/N13/N13-1.pdf#page=535.

Ott, M., Choi, Y., Cardie, C., & Hancock, J. T. (2011). Finding deceptive opinion spam by any stretch of the imagination. In *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies—Volume 1* (pp. 309–319). Association for Computational Linguistics. Retrieved from http://dl.acm.org/citation.cfm?id=2002512.

Panasiti, M. S., Cardone, D., Pavone, E. F., Mancini, A., Merla, A., & Aglioti, S. M. (2016). Thermal signatures of voluntary deception in ecological conditions. *Scientific Reports, 6*(1). https://doi.org/10.1038/srep35174.

Pennebaker, J. W., Boyd, R. L., Jordan, K., & Blackburn, K. (2015). *The development and psychometric properties of LIWC2015*. Retrieved from https://repositories.lib.utexas.edu/handle/2152/31333.

Perry, M., & Gilbey, A. (2011). The screening of passengers by observation techniques programme. *Aviation Security International, 17*(3), 12.

Schler, J., Koppel, M., Argamon, S., & Pennebaker, J. W. (2006). Effects of age and gender on blogging. In *AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs* (Vol. 6, pp. 199–205).

Schubert, S. (2006). A look tells all. *Scientific American*. Retrieved from http://www.scientificamerican.com/article.cfm?id=a-look-tells-all.

Shaw, D. J., Vrij, A., Leal, S., Mann, S., Hillman, J., Granhag, P. A., et al. (2013). Expect the unexpected? Variations in question type elicit cues to deception in joint interviewer contexts. *Applied Cognitive Psychology, 27*(3), 336–343.

Sooniste, T., Granhag, P. A., Knieps, M., & Vrij, A. (2013). True and false intentions: Asking about the past to detect lies about the future. *Psychology, Crime & Law, 19*(8), 673–685. https://doi.org/10.1080/1068316X.2013.793333.

Sooniste, T., Granhag, P. A., Strömwall, L. A., & Vrij, A. (2015). Statements about true and false intentions: Using the cognitive interview to magnify the differences. *Scandinavian Journal of Psychology, 56*(4), 371–378. https://doi.org/10.1111/sjop.12216.

Soukara, S., Bull, R., Vrij, A., Turner, M., & Cherryman, J. (2009). What really happens in police interviews of suspects? Tactics and confessions. *Psychology, Crime & Law, 15*(6), 493–506. https://doi.org/10.1080/10683160802201827.

Swanner, J. K., Meissner, C. A., Atkinson, D. J., & Dianiska, R. E. (2016). Developing diagnostic, evidence-based approaches to interrogation. *Journal of Applied Research in Memory and Cognition, 5*(3), 295–301. https://doi.org/10.1016/j.jarmac.2016.07.001.

Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and opportunities* (2nd ed.). New York: John Wiley & Sons Ltd.

Vrij, A. (2016). Baselining as a lie detection method: Baselining. *Applied Cognitive Psychology, 30*(6), 1112–1119. https://doi.org/10.1002/acp.3288.

Vrij, A., Blank, H., & Fisher, R. P. (2018). A re-analysis that supports our main results: A reply to Levine et al. *Legal and Criminological Psychology*, *23*(1), 20–23. https://doi.org/10.1111/lcrp.12121.

Vrij, A., & Fisher, R. P. (2016). Which lie detection tools are ready for use in the criminal justice system? *Journal of Applied Research in Memory and Cognition, 5*(3), 302–307. https://doi.org/10.1016/j.jarmac.2016.06.014.

Vrij, A., Fisher, R. P., & Blank, H. (2017). A cognitive approach to lie detection: A meta-analysis. *Legal and Criminological Psychology, 22*(1), 1–21. https://doi.org/10.1111/lcrp.12088.

Vrij, A., & Granhag, P. A. (2012). Eliciting cues to deception and truth: What matters are the questions asked. *Journal of Applied Research in Memory and Cognition, 1*(2), 110–117. https://doi.org/10.1016/j.jarmac.2012.02.004.

Vrij, A., Granhag, P. A., Mann, S., & Leal, S. (2011). Lying about flying: The first experiment to detect false intent. *Psychology, Crime & Law, 17*(7), 611–620. https://doi.org/10.1080/10683160903418213.

Vrij, A., Granhag, P. A., & Porter, S. (2010). Pitfalls and opportunities in nonverbal and verbal lie detection. *Psychological Science in the Public Interest, 11*(3), 89–121. https://doi.org/10.1177/1529100610390861.

Vrij, A., Leal, S., Granhag, P. A., Mann, S., Fisher, R. P., Hillman, J., et al. (2009). Outsmarting the liars: The benefit of asking unanticipated questions. *Law and Human Behavior, 33*(2), 159–166.

Vrij, A., Leal, S., Mann, S. A., & Granhag, P. A. (2011). A comparison between lying about intentions and past activities: Verbal cues and detection accuracy. *Applied Cognitive Psychology, 25*(2), 212–218.

Vrij, A., Mann, S. A., Fisher, R. P., Leal, S., Milne, R., & Bull, R. (2008). Increasing cognitive load to facilitate lie detection: The benefit of recalling an event in reverse order. *Law and Human Behavior, 32*(3), 253–265. https://doi.org/10.1007/s10979-007-9103-y.

Warmelink, L., Vrij, A., Mann, S., & Granhag, P. A. (2013a). Spatial and temporal details in intentions: A cue to detecting deception. *Applied Cognitive Psychology, 27*(1), 101–106. https://doi.org/10.1002/acp.2878.

Warmelink, L., Vrij, A., Mann, S., & Granhag, P. A. (2013b). Spatial and temporal details in intentions: A cue to detecting deception: Spatial and temporal details in lie detection. *Applied Cognitive Psychology, 27*(1), 101–106. https://doi.org/10.1002/acp.2878.

Warmelink, L., Vrij, A., Mann, S., Jundi, S., & Granhag, P. A. (2012). The effect of question expectedness and experience on lying about intentions. *Acta Psychologica, 141*(2), 178–183.

Warmelink, L., Vrij, A., Mann, S., Leal, S., Forrester, D., & Fisher, R. P. (2011). Thermal imaging as a lie detection tool at airports. *Law and Human Behavior, 35*(1), 40–48. https://doi.org/10.1007/s10979-010-9251-3.

Warmelink, L., Vrij, A., Mann, S., Leal, S., & Poletiek, F. H. (2013). The effects of unexpected questions on detecting familiar and unfamiliar lies. *Psychiatry, Psychology and Law, 20*(1), 29–35. https://doi.org/10.1080/13218719.2011.619058.

Wilgoren, J., & Wong, E. (2001). After the attacks: United flight 93; On doomed flight, passengers vowed to perish fighting. *New York Times.* Retrieved from http://www.nytimes.com/2001/09/13/us/after-attacks-united-flight-93-doomed-flight-passengers-vowed-perish-fighting.html.

Yarkoni, T., & Westfall, J. (2017). Choosing prediction over explanation in psychology: Lessons from machine learning. *Perspectives on Psychological Science, 12*(6), 1100–1122. https://doi.org/10.1177/1745691617693393.

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