Airport Artificial Intelligence Can Detect Deception – Or am I lying?

Louise Marie Jupe

Department of Psychology, University of Portsmouth

David Adam Keatley

Researchers in Behaviour Sequence Analysis (ReBSA) & School of Law, Murdoch University, Perth, Australia, 6150

Author notes

Correspondence concerning this article should be addressed to Louise Jupe, Department of Psychology, University of Portsmouth, King Henry Building, King Henry 1 Street, PO1 2DY, Hants, United Kingdom. Email: louise.jupe@port.ac.uk

Abstract

Since the 9/11 terrorist attacks, research has enveloped numerous areas within the psychological sciences as a means to increase the ability to spot potential threats. While airports took to heightened security protocols, many academics looked deeper into ways of detecting deception within international airport settings. Various verbal and nonverbal systems were intensely scrutinised under the empirical magnifying glass with the aim of creating security environments that are better able to detect potential threats. However, in 2018, a €4.5m grant from the European Union's Horizon 2020 research and innovation programme, number 700626, was awarded to further *in vivo* test the use of computational methods to detect deception from facial cues. The system is deemed a non-invasive psychological profiling system and stems from that of a system called 'Silent Talker' (Rothwell, Bandar, O'Shea, & McLean, 2006). The 'iBorderCtrl' AI system uses a variety of 'at home' pre-registration systems and real-time 'at the airport' automatic deception detection systems. Some of the critical methods used in automated deception detection is that of micro-expressions. In this opinion article, we argue that considering the state of the psychological sciences current understanding of micro-expressions and their associations with deception, such *in vivo* testing is naïve and misinformed. We consider the lack of empirical research that supports the use of micro-expressions in the detection of deception and question the current understanding of the validity of specific cues to deception. With such unclear definitive and reliable cues to deception, we question the validity of using artificial intelligence that includes cues to deception, which have no current empirical support.

Keywords: lie detection, airport security, artificial intelligence, machine learning, iBorderCtrl,

Airport Artificial Intelligence Can Detect Deception – Or am I lying?

It has been announced recently that several European Airports will begin to test the usability of Artificial Intelligence (AI) systems to detect whether travellers are making deceitful statements. The 'iBorderCtrl' AI system, which was granted €4.5m for development, will be tested in: Hungary, Latvia, and Greece, on passengers who are travelling from outside of the European Union (EU). The technology and computer programming involved does indeed appear highly technical and suggests a significant advancement in the pursuit of accurately detecting deception. The notion of pre-arrival registration, advanced biometrics and face matching all have the allure of a failsafe system designed to enhance the national and international security in areas of high risk, namely international airports. The system will be *in vivo* tested[1]. *In vivo* is a reference to when a test that involves a living organism (i.e., a human) is explored in the environment it is meant to be applied. In the current paper, this refers to the removal of testing in the laboratory to testing in the field and with members of the general public.

Popular media such as *Lie to Me* has seen an increase in characters like Dr Cal Lightman and his 'wizard' type abilities to detect deception (Levine, Serota, & Shulman, 2010; Su & Levine, 2016) and the portrayal of advanced technological systems as seen in *CSI* (Baskin & Sommers, 2010) has led many to overestimate what science can and cannot do. However, implementing an AI system based on weak theoretical science, which may appease the public, is likely to results in serious (possibly fatal) inaccuracies and reliance upon – what we will argue – is a flawed approach. The focus of this opinion piece is to provide readers with a simplified description of AI and a brief background into the history of lie detection

[1] Note, between submission of article and publication, the iBorderCtrl system has been tested, and initial anecdotal evidence suggests that it resulted in a false positive (Gallagher & Jona, 2019). We hope future developers of such technology will heed the advice in this article and/or contact the authors to discuss developing such systems.

research, to include verbal and nonverbal indicators, and micro-expressions (the main cues used in the iBorderCtrl system and that of *Lie to Me*). Finally, while we acknowledge that advancing our understanding of deception may be aided by computational methods, we feel it pertinent not to allow the public or practitioners to be blinded by the seductive technicalities of a system that could wrongly sway professional/TSA judgements about passengers' honesty and intentions, which could have dire consequences. The main argument that we will propose is that the cues that AI systems use do not yet have enough underlying diagnostic value in terms of differentiating truth tellers from liars. Finally, we discuss some of the more recent techniques currently under investigation that may be more suitable to be implemented in airport scenarios.

Nonverbal Cues to Deception

The current state of psychological science suggests that nonverbal methods for detecting deception are often limited and unreliable (DePaulo et al., 2003) and often only barely identify deception above chance levels of accuracy (Bond & DePaulo, 2006). For example, DePaulo and colleagues (2003) found that of 158 possible cues to deception, ranging from the more subtle, such as response latency and gaze aversion to the more obvious such as postural shifts and shrugs, very few were found to be significantly correlated with deception. For example, obvious stereotypical cues to deception such as gaze aversion, fidgeting, silent pauses and facial expressiveness were not commonly found amongst individuals who were being deceptive. Very few cues emerged as having a relationship with deception, and of those that did (e.g., liars are less forthcoming, provide fewer compelling tales, create a negative impression, are tenser and provide fewer unusual details than truth tellers), the statistical correlation between such cues and deceptive behaviour was very low. To this day, we are still not able to identify clear and highly significant behavioural cues when individuals are lying or telling the truth. There is no single 'tell' or Pinocchio's' nose

for deception (Albrechtsen, Meissner, & Susa, 2009; Hartwig & Bond, 2011; Vrij, Leal, Mann, Vernham, & Brankaert, 2015; Vrij, Mann, Leal, Vernham, & Vaughan, 2016). AI programmes based upon such approaches, therefore, are destined to fail by producing unacceptable levels of accuracy considering their use in security contexts.

Notwithstanding the overall findings that nonverbal cues to deception are weak and unreliable (DePaulo et al., 2003), a recent exploratory study into publication bias, small effect sizes and underpowered studies (Luke, 2018) indicates that our current understanding of cues to deception may be deeply flawed. Luke states: "That is to say, the informational value of the present literature is so low as to make it virtually impossible to distinguish real effects from false positives" (2018, p. 2). Have we, therefore, been deceived about what deceivers do when they lie? Is there any evidence at all that we can detect deception? The answer is one that is open to much speculation and underpins why the use of AI within the current state of psychological science is potentially hazardous. If we do not know what cues we need to look for, then the notion that a programmed set of algorithms or can detect deception is misguided and destined to fail. However, many people do erroneously believe they can learn Cal Lightman's skills and spot lies; therefore, false confidence is given to systems like iBorderCtrl that do the same thing with more technologically advanced infrastructure.

What is Artificial Intelligence?

While most people understand the word artificial, what needs a clear definition is the aspect of intelligence. Despite years of research, we still have very few clear definitions of what constitutes intelligence, with many books on AI discussing how AI asks *itself* what AI is (Bringsjord & Schimanski, 2003). This alone makes the definition of AI reasonably complex. In its purest form, AI is the ability of a computer to respond, as if it were using human intelligence to particular stimuli (Poole, Mackworth, & Goebel, 1998). While writing programmes that *appear* smart may be possible, their interpretation of meaningful, junk or

noisy outcomes is often lacking. However, what AI does is learn through experience, which is called machine learning (ML). ML is defined by a computer's ability to demonstrate the *process* of learning (Samuel, 1959). To fully complete the process: useful AI is built upon ML, and most ML is built upon neural networks (NN). A NN is a computational system that mimics how human cognition is organised into networks. In the 1960s, the first NN demonstrated that digital synapses could amend themselves in line with pattern recognition was developed (Widrow & Hoff, 1960).

What is iBorderCtrl Proposing?

The iBorderCtrl system is proposing the use of an Automatic Deception Detection System (ADDS), by analysing an individual's 'nonverbal micro expressions' (iBorderCtrl, 2019, p. 2). This is the second stage of the process. The initial stages require pre-registration from the travellers' home, using the internet, much akin to online check-in. Part of the second stage also assesses biometric data, to include fingerprint and vein pattern analysis. ADDS was built upon findings from two research papers (Rothwell et al., 2006; Rothwell, Bandar, O'Shea, & McLean, 2007). The first (Rothwell et al., 2006) we refer to as part of its title, 'Silent Talker' and the second (Rothwell et al., 2007), as its full name: Charting the behavioural state of a person using a backpropagation neural network. When one reviews the article 'Silent Talker' (Rothwell et al., 2006), there are clear fundamental methodological issues with the data. There is a significant issue with the number of participants used. Ten truthful participants and seven deceptive participants formed the sample upon which accuracy of up to 79% was reported. Closer inspection of the data also shows that initial trials yielded deception accuracy rates of 54% (Rothwell et al., 2006, p. 769). Further trials also showed deception detection rates as low as 14% (Rothwell et al., 2006, p. 772). In their second paper, the numbers are even higher cause for concern. Their sample consisted of only 15 English men, to make their lying and truth telling sample. Despite their use of vectors for repeated

testing, initial accuracy for deception is 77% and truthful 72% (Rothwell et al., 2007, p 332). Some of the findings also show truth accuracy as low as 43%. This is below the odds of chance alone. Using three as the number of dependent variables, as per Rothwell et al, (2007), G*Power analyses concede that to obtain even a small effect size of .2, with a modest (arguably somewhat unacceptable) level of power of .8, a total of 60 participants (30 liars and 30 truth tellers) should be used (Faul, Erdfelder, Lang, & Buchner, 2007). Therefore, we argue that the studies upon which iBorderCtrl has been built are majorly underpowered.

Are Micro-Expressions Reliable Indicators of Deception?

Before we build a complex computer-assisted deception detector, it is important to investigate where this approach begins in the research literature. Micro-expressions are innate involuntary physical responses to emotional stimuli, typically used to indicate a mismatch/disharmony between what is being said by an individual, and what is felt (Marono, Clarke, Navarro, & Keatley, 2018; Marono, Clarke, Navarro, & Keatley, 2017). Micro-expressions typically occur as fast as 1/15 to 1/25 of a second, and are therefore imperceptible to the human eye, and cannot accurately be detected in real time; this means that we cannot observe an individual and decipher his or her micro-expressions as they occur (Honts, Hartwig, Kleinman, & Meissner, 2009). Besides, individuals rarely display micro-expressions at best (Porter & ten Brinke, 2008). Individuals who have studied the automation of detecting micro-expressions have stated that it is a very difficult cue to standardise. "Deceptive behaviour is very subtle and varies across different people. Thus, detecting these subtle micro motion patterns… is a challenging problem" (Wu, Singh, Davis, & Subrahmanian, 2017, p. 2). The level of challenges that current computational micro-expression detection systems face means that it is by no means ready for *in vivo* testing. Irrespective of the potential problems with using micro-expressions as a method to detect deception overall, micro-expressions have received minimal empirical testing. While Paul

Ekman founded the notion of micro-expressions, he has never published any of his micro-expression related research (Vrij, Hope, & Fisher, 2014). The underlying theory behind micro-expressions is that of leakage (Ekman, 1992; Ekman & Friesen, 2016), the notion that our true emotions of feelings leak from within, more often referred to as the classical theory of emotions (Nguyen et al., 2012).

Ekman based his work on the findings from a system called 'Emotion Facial Action Coding System (EMFACS)', created in the 1980s (Ekman, 2019). This system allows for the movements of the face to be tracked and inferences drawn as to the inner state of the individual. However, Ekman's theories have been heavily criticised. Lisa Feldman Barrett, a professor of psychology at Northeastern University stated that she first explored the theory as a graduate student. She came across Ekman's methods when looking for *objective* ways to measure emotion. Feldman Barrett realised that Ekman's work was limited by the participants having been provided labelled expressions to match to faces in his work. Barrett Feldman believed that Ekman 'primed' his participants. Barrett Feldman repeated the study, without labels, and found that the recognition of emotions fell dramatically (Barrett Feldman, 2014). Barret Feldman went on to develop her own theory of emotions (Barrett Feldman, 2017a). She states that there are no universal areas of the brain that are related to emotions that are activated by external stimuli. Not only do micro-expressions have little in terms of empirical evidence, but the theoretical and experiential evidence also shows severe flaws in the methodology upon which the classical theory of emotions is built.

The hype surrounding micro-expressions appears to be more related to publications in popular media than science (Adelson, 2004; Best, 2017; Henig, 2006). Micro-expressions are idiosyncratic. Individuals vary in the types of micro-expressions they exhibit, and interpretation comes down to subjective experiences. AI cannot 'unpack' the subjective meaning and nuances across different people and situations. It is objective in running

equations and programs. The fact that emotional expressions are idiosyncratic and do not respond to the same stimuli suggests that measures of micro-expressions can only lead to inaccurate readings and that its use in high-security contexts has potentially dangerous consequences. The notion that we *all* display the same small furrowing of the brows during anger (Ortony & Turner, 1990, p. 319) or pursing of the lips when we are disgusted (Rozin, Lowery, & Ebert, 1994) is, unfortunately, an unsupported assumption. There are no standard responses amongst homo sapiens to particular stimuli (Barrett Feldman, 2017b, 2017a). However, Rothwell et al., (2006) have stated that the objectivity of the system is a benefit, allowing it to override that of human error resulting from fatigue etc. Such a statement appears nonsensical given our understanding of overt human emotion.

However, What About Passports and Biometrics? Surely, They Are Reliable?

The National Crime Agency has recognised that identity crime often enables individuals to pass freely between borders because of the use of genuine identity documents (National Crime Agency, 2017). However, the use of biometric additions to passports, often seen as enhancing security, is open to spoofing (Gold, 2012; Hadid, 2014; Marcel, Nixon, & Li, 2014). Fingerprints are, unfortunately, no longer the holy grail of identification we once held them to be due to their alteration (Soweon Yoon, Jianjiang Feng, & Jain, 2012). The unique elements of our iris are easily spoofed with contact lenses (Kohli, Yadav, Vatsa, Singh, & Noore, 2016), and our gait is effortlessly changed (Gafurov, Snekkenes, & Bours, 2007). Although vein analysis may be seen as a turning point, it too is not without limitations. Researchers have shown that their efficacy is profoundly affected by factors such as wet palms (e.g., the nervous traveller), dry palms, skin conditions and scars (Nguyen et al., 2012). However, the most worrying of all is the potential spoofing of facial attributes, which again would render a system which works on the specifics of the face impractical (Hadid, 2014). However, iBorderCtrl does acknowledge such downfalls:

> Despite the extensive use of biometrics on security applications including in border control with the advent of digital passports that contain fingerprints digital images and physical characteristics of individuals, a traveller with ill intentions using own documents, biomarkers would not reveal their attempted deceit. iBorderCtrl deploys well established as well as novel technologies together to collect data that will move beyond biometrics and onto biomarkers of deceit (iBorderCtrl, 2019).

Biomarkers refer to an individual's inner state. Based on what we have discussed in the current opinion piece and that of numerous psychological studies, there are no ways of accurately assessing a human's inner state due to their idiosyncratic nature. Irrespective of whether this is carried out by a human or a machine. Using biomarkers as a method above and beyond that of biometrics is merely a complete misconception.

An Artificial Crisis

Despite the rapidly growing integration of AI and ML into our everyday lives, we are facing what many experts are referring to as a 'science crisis' (Ghosh, 2019). Allen (2019, cited in Ghosh, 2019) states that the facilitation of machine learning is leading research scientists to analyse data via computational methods that are often completely erroneous and that the flaw in analysis means there is a lack of trust in such findings. We now take a closer look at the use of AI and ML within deception research and many of the problems that systems such as the 'iBorderCtrl' need to consider, before the use of *in vivo* testing.

Why Deception Detection is Not Ready For AI

Machine learning algorithms are mostly what is known as 'black boxes', as it is difficult to know how much deception they detect (Nortje & Tredoux, 2019) especially when tested *in vivo.* Unless every passenger is put through a complete security check, irrespective of the output of the systemoutput, we have no definite hit or miss rates. This is a crucial point to argue as to why AI within deception detection should be more rigorously tested within the

safe confinements of a lab until we hit accuracy rates which can be deemed acceptable within security environments. What is critical in this argument towards our concern regarding the use of AI in areas of high security is that AI and machine learning are faced with similar obstacles to that of human assessors; the 'gold standard' of known veracity (Nortje & Tredoux, 2019, p. 10). Neither AI nor a human can be sure of a veracity status or 'ground truth' without substantial evidence. This is where we hit upon a quandary. If both human and ML systems can never be sure of an individual's veracity status, then what exactly is it that the machine is looking for? What is even more worrying is that despite the €4.5m grant used to develop the system, the final decision as to a passengers flight eligibility will be made by a human. "iBorderCtrl is a human in the loop system, and the Border Guard will use his/her experience in making the final decision" (iBorderCtrl, 2019). Given our current understanding, that experts rarely exceed accuracy levels above those of lay individuals (Bogaard, Meijer, Vrij, & Merckelbach, 2016; Mann, Vrij, Bull, Vrij, & Bull, 2018; O'Sullivan, Frank, Hurley, & Tiwana, 2009; Vrij et al., 2015), relying upon a Border Guards expertise is only adding further potential error to a system, which is yet to yield accuracy rates that would be deemed acceptable within a high-security setting. This seems like a 'failsafe' approach to not relying on technology; however, if humans are to make the final choice, then why not use the €4.5 in further interpersonal deception detection research?

What would be more logical, based upon the meager number of participants used to explore the automation of the detection of micro-expressions (Rothwell et al., 2006), would be to use Monte Carlo simulations. Doing so allows for a better understanding of the potential risk of a system). Alternatively, cross-validation is also recommended, a method which allows the simulation of an infinite number of participants (Kleinberg, Arntz, & Verschuere, 2019). Both systems can be completed in rapid time using specific programmes. By doing so, not

only is there less of a burden on public expenditure, but potential errors can be identified (e.g., if the system will fail, it will be known almost immediately, and changes can be made).

Is *In Vivo* Testing A Waste of Time?

We answer the above: Is *in vivo* testing a waste of time? Absolutely not. *In vivo* testing allows research scientists to overcome many aspects of experimental testing that are associated with laboratory research. Many studies have had to defend their lack of mundane realism, replicability and participant motivation (Marono et al., 2017a, 2017b; Keatley, 2018). How do psychologists get individuals who are clearly taking part in a scientific experiment to behave as if they would if they were really lying? How can we compare a student attempting to gain negligible participant allowance with an airline passenger attempting to transfer location for terrorist activity? The majority of research in deception detection is conducted on student, WEIRD (western, educated, industrialised, rich, and democratic cultures [Henrich, Heine, & Norenzayan, 2010]) samples, which in essence creates a false representation of overall human behaviour (Jones, 2010). This provides limited ecological validity. This points towards the use of *in vivo* testing; however, there should be an apparent gap between ‘testing' and ‘proving'. We are not suggesting that iBrderCtrl should not be tested, merely that the system should not be relied upon without stringent testing – a hurdle we feel it is unable to overcome, given the limited theoretical foundations upon which it is based.

In addition, with *in vivo* testing comes media interest, a clear public presence and a misunderstanding of what the results are telling us (Lovell-Badge, 2013). As an exemplifier, iBorderCtrl has been reported in many mainstream media outlets, such as the BBC (Woollacott, 2017), the Telegraph (Bernal, 2018) and the Express (McGrath, 2018). Online platforms have not only been quick to support the movement but have suggested human rights violations (EDRi, 2019) and the fact that iBorderCtrl has dangerously understood the

concept of AI (ActuIA, 2019). Petitions have been sent to the Greek Government calling for its removal from *in vivo* testing (Homo Digitalis, 2019) and have further suggested that it is impossible to check whether such a system is permittable under European Law and that "its credibility and validity can not be proven" (Homo Digitalis, 2019, our translation).

Implementing *in vivo* testing of an automated system, based upon methods which have already been shown to be an ineffective method for differentiating between honest and dishonest individuals, is not only an argument against the use of poor public spending but makes little, if any, methodological sense. While the argument may posit that an automated system can detect micro-expressions, their detection has no direct causal relationship with an individual's inner state. Moreover, for those individuals who do not display micro-expressions (Porter & Brinke, 2008), there is little use of an automated system to detect them. The use of AI to detect deceptive cues which are unlikely to exist is one that is a counter-intuitive advancement in lie detection. In essence, AI will currently work with weak theoretical understandings of deception and a great deal of human (error-prone) input (Nortje & Tredoux, 2019).

A Possible Future For AI?

What should be made clear is that we are not dismissing the use of AI in future deception detection research. Potentially, AI has many advantages over the standard computational power of humans, irrespective of expertise or intelligence. We suggest one potential area where AI experts could assist deception researchers. Current research suggests that verbal indicators to deception are currently showing to be the most discriminative between liars and truth tellers. After the seminal findings of the meta-analysis into nonverbal cues by DePaulo et al. (2003), researchers in deception moved their focus to verbal cues, in particular methods which would exploit differences between liars and truth tellers by eliciting more cues to deceit (Vrij & Granhag, 2012). Such verbal veracity tools tend to work on the

premise of encouraging an interviewee to say more (Vrij, Fisher, Blank, Leal, & Mann, 2016), increasing cognitive load such that lying becomes more difficult (Debey, Verschuere, & Crombez, 2012) and providing a model statement so that individuals know the amount and type of detail they should be able to provide (Sartori, Tasios, Vrij, Leal, & Fisher, 2018). Such methods allow analysts to identify particular traits in the individual's speech patterns, from detecting consistency, inaccuracies, core versus peripheral details or statement length, to name only but a few. The idea behind these methods is that they should make recall taxing for a liar whilst benefiting the truth teller (for more examples see the Strategic Use of Evidence [Granhag & Hartwig, 2015], Cognitive Credibility Assessment [Vrij, Fisher, & Blank, 2017], Assessment Criteria Indicative of Deception [ACID] [Colwell, Hiscock-Anisman, Memon, Taylor, & Prewett, 2007] and the Verifiability Approach [Nahari, 2018]).

However, over time, language changes (Freeborn, 2006). The intricacies of modern language do not represent the same verbal prose documented 100 years ago. Language also changes across the lifespan (McLennan, 2006; Wang, 1979). Working on this premise, the language we use in 20 years will change as we age and as a society, 100 additional years are likely to amend the same linguistic traits we use today. AI has the potential to predict such changes in language. Due to the computational power of AI, ML and NN, if AI specialists were to integrate data from many years previous on the way that human language has developed, then predictions about how it may change in the future should be able to be made. Such predictions will allow deception researchers the ability to stay 'one step ahead', designing verbal veracity tools which will be ready before such changes in language even appear.

Current Alternatives to iBorderCtrl

Assessing individuals in an airport scenario requires rapid evaluation. We appreciate that verbal veracity tools (those which encourage the interviewee to say more, allowing for

their responses to be scrutinised) is not necessarily the most viable method under the circumstances. One method proposed where AI or automation may be useful is by using The Rigidity Effect (RE [Burgoon, 2018]). The RE postulates that when an individual is faced with deception under high stake situations, there is an initial freeze response (see Jansen, Nguyen, Karpitskiy, Mettenleiter, & Loewy, 1995 for an overview of autonomic responses to threat). Research has shown that individuals manage their nonverbal behaviour and overall impression so that they appear credible (Burgoon, Buller, Ebesu, White, & Rockwell, 1996). Working on the theoretical basis of rigidity, studies have shown that blinking reduces during deception (Leal & Vrij, 2008) and the suppression of one facial expression led to the suppression of all facial expressions (Hurley & Frank, 2011). However, despite being told to suppress rigidity, countermeasure studies have shown that this is a challenging endeavour (Twyman, Proudfoot, Schuetzler, Elkins, & Derrick, 2015).

Using a theoretical framework of probabilistic functionalism proposed by Brunswik (1952), Hartwig and Bond (2011) found that we may not be as weakly attuned to deceptive cues as the literature would suggest, but that the issue is inherent that the behavioural differences between liars and truth tellers are weak at best. Hartwig and Bond (2011) suggest that the elicitation of more explicit cues is needed, i.e., we need to evoke much stronger behavioural differences between liars and truth tellers. This in part can be achieved by increasing the cognitive load placed upon liars (see Vrij, Fisher, Mann, & Leal, 2006; Vrij, Fisher, & Blank, 2017; Vrij & Ganis, 2014). If we are still unable to elicit clearer more identifiable cues – even if AI were to be able to detect them – it also means we still currently do not know what these cues are.

An Intelligent Honest Future? Perhaps Not Quite Yet

Although we question the suitability of iBorderCtrl to be used in security settings *in vivo* currently, there is no doubt that AI will have a part to play in the future of deception

detection. The hour's researchers spend coding will no doubt soon be completed by an *intelligent* system which can understand the intricacies of human language. The current criticism falls on a severe misunderstanding of an anxiety heuristic, in which liars show fear and truth tellers do not, which manifests in their behaviour (Jupe & Hartwig, 2019), specifically, their micro-expressions. In addition, we believe iBorderCtrl is not designed upon theoretical underpinning and uses indices which do not have a direct correlation with deception.

AI researchers must consider the complexity of lies, in which all are not equal in terms of moral, meaning, and potential outcomes. The father who lies to his child about the existence of Santa Claus is a far cry from the same man lying to his wife about a prolonged affair with her best friend. Even so, these lies are leagues away from a psychopathic, emotionless serial killer, who denies his wrongdoing despite the devastation he or she causes to the lives of many. A serial killers' lies will no doubt differ greatly from the suicide bomber who believes that the explosive device he will detonate mid-air is all for his greater calling in the name of religion. The refugee attempting to gain asylum to escape the horrors of their country is likely to show very different nonverbal behaviours than the terrorist attempting to enter the country for nefarious reasons. When we apply this to deception, denying that one was involved in a crime that they did commit, the evidence is unequivocal. Some liars feel guilt, others feel anxious, and others feel excitement (also known as the emotional approach to deception [(Vrij, 2000)]). If liars all feel different emotions and their emotions manifest differently in their overt behaviour, then why is there an assumption that we can interpret these to a level deemed acceptable in areas such as international airports? Until we fully understand and integrate the differences between liars and truth tellers, attempting to create a 'one-rule-fits-all' algorithm is destined to fail. Dr Cal Lightman should, therefore, remain a fictional television character, if only for the time being.

References

ActuIA. (2019). iBorderCtrl : a dangerous misunderstanding of what AI really is - Actu IA. Retrieved March 5, 2019, from https://www.actuia.com/english/iborderctrl-a-dangerous-misunderstanding-of-what-ai-really-is/

Adelson, R. (2004). Detecting deception. *Monitor on Psychology*, *35*(7).

Albrechtsen, J. S., Meissner, C. A., & Susa, K. J. (2009). Can intuition improve deception detection performance? *Journal of Experimental Social Psychology*. https://doi.org/10.1016/j.jesp.2009.05.017

Barrett Feldman, L. (2014). Opinion | What Faces Can't Tell Us. Retrieved March 8, 2019, from https://www.nytimes.com/2014/03/02/opinion/sunday/what-faces-cant-tell-us.html

Barrett Feldman, L. (2017a). *How Emotions are Made:The Secret Life of the Brain*. Boston, MA: Houghton Mifflin Harcourt.

Barrett Feldman, L. (2017b). Why our emotions are cultural – not built in at birth. Retrieved March 8, 2019, from https://www.theguardian.com/lifeandstyle/2017/mar/26/why-our-emotions-are-cultural-not-hardwired-at-birth

Baskin, D. R., & Sommers, I. B. (2010). Crime-Show-Viewing Habits and Public Attitudes Toward Forensic Evidence: The "CSI Effect" Revisited. *The Justice System Journal*. Taylor & Francis, Ltd. https://doi.org/10.2307/27977480

Bernal, N. (2018). AI lie detectors to be tested by the EU at border points. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/technology/2018/11/01/ai-lie-detectors-tested-eu-border-points/

Best, S. (2017). The robot that knows when you're lying: Scientists create an AI that can detect deception in the courtroom (and it's already "significantly better" than humans). Retrieved August 12, 2018, from http://www.dailymail.co.uk/sciencetech/article-

5197747/AI-detects-expressions-tell-people-lie-court.html

Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Strong, but wrong: Lay people's and police officers' beliefs about verbal and nonverbal cues to deception. *PLoS ONE*, *11*(6). https://doi.org/10.1371/journal.pone.0156615

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of Deception Judgments. *Personality and Social Psychology Review*, *10*(3), 214–234. https://doi.org/10.1207/s15327957pspr1003_2

Bringsjord, S., & Schimanski, B. (2003). What is artificial intelligence? Psychometric AI as an answer. In *IJCAI International Joint Conference on Artificial Intelligence* (pp. 887–893). Retrieved from http://www.cyc.com

Brunswik, E. (1952). The conceptual framework of psychology. *Psychological Bulletin*, *49*(6), 654–656. Retrieved from https://insights.ovid.com/psychological-bulletin/plbul/1952/11/000/conceptual-framework-psychology/14/00006823

Burgoon, J. K. (2018). Microexpressions Are Not the Best Way to Catch a Liar. *Frontiers in Psychology*, *9*, 1672. https://doi.org/10.3389/fpsyg.2018.01672

Burgoon, J. K., Buller, D. B., Ebesu, A. S., White, C. H., & Rockwell, P. A. (1996). Testing interpersonal deception theory: Effects of suspicion on communication behaviors and perceptions. *Communication Theory*, *6*(3), 243–267. https://doi.org/10.1111/j.1468-2885.1996.tb00128.x

Colwell, K., Hiscock-Anisman, C. K., Memon, A., Taylor, L., & Prewett, J. (2007). Assessment Criteria Indicative of Deception (ACID): an integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling*, *4*(3), 167–180. https://doi.org/10.1002/jip.73

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., … Cooper, H. (2003). Cues to deception. *Psychological Bulletin*, *129*(1), 74–118. https://doi.org/10.1037//0033-2909.129.1.74

EDRi. (2019). Greece: Clarifications sought on human rights impacts of iBorderCtrl - EDRi. Retrieved March 8, 2019, from https://edri.org/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/

Ekman, P. (1992). *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. *Design* (Vol. Paperback,). https://doi.org/152.384 E45t

Ekman, P. (2019). Facial Action Coding System | Micro Expressions. Retrieved March 8, 2019, from https://www.paulekman.com/product-category/facs/

Ekman, P., & Friesen, W. V. (2016). Nonverbal Leakage and Clues to Deception†. *Http://Dx.Doi.Org/10.1080/00332747.1969.11023575*, *32*(1), 88–106. https://doi.org/10.1080/00332747.1969.11023575

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/BF03193146

Freeborn, D. (2006). *From Old English to standard English : a course book in language variation across time*. *Studies in English language series*. Retrieved from http://hotfile.com/dl/83728759/def5fc0/From.old.english.to.standard.english.rar.

Gafurov, D., Snekkenes, E., & Bours, P. (2007). Spoof Attacks on Gait Authentication System. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, *2*(3). https://doi.org/10.1109/TIFS.2007.902030

Gallagher, R., & Jona, L. (2019). We Tested Europe's New Digital Lie Detector. It Failed. Retrieved August 27, 2019, from https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

Ghosh, P. (2019). AAAS: Machine learning "causing science crisis" - BBC News. Retrieved March 5, 2019, from https://www.bbc.co.uk/news/science-environment-47267081

Gold, S. (2012). Border control biometrics and surveillance. *Biometric Technology Today*, *2012*(7), 9–11. https://doi.org/10.1016/S0969-4765(12)70149-2

Granhag, P. A., & Hartwig, M. (2015). The strategic use of evidence technique: A conceptual overview. In *Detecting deception: Current challenges and cognitive approaches.* (pp. 231–251). Wiley-Blackwell.

Hadid, A. (2014). Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops* (pp. 113–118). https://doi.org/10.1109/CVPRW.2014.22

Hartwig, M., & Bond, C. F. (2011). Why Do Lie-Catchers Fail? A Lens Model Meta-Analysis of Human Lie Judgments. *Psychological Bulletin*, *137*(4), 643–659. https://doi.org/10.1037/a0023589

Henig, R. B. (2006). Looking for the Lie. Retrieved August 12, 2018, from https://www.nytimes.com/2006/02/05/magazine/looking-for-the-lie.html?_r=1

Homo Digitalis. (2019). Homo Digitalis Reporting to the Hellenic Parliament on the use of the IBORDERCTRL system at the Greek border. Retrieved March 8, 2019, from https://www.homodigitalis.gr/posts/2771

Honts, C. R., Hartwig, M., Kleinman, S. M., & Meissner, C. A. (2009). *Credibility assessment at portals: Portals committee report. Final Report of the Portals Committee to the Defense Academy for Credibility Assessment.*

Hurley, C. M., & Frank, M. G. (2011). Executing Facial Control During Deception Situations. *Journal of Nonverbal Behavior*, *35*(2), 119–131. https://doi.org/10.1007/s10919-010-0102-1

iBorderCtrl. (2019). Technical Framework. Retrieved February 27, 2019, from https://www.iborderctrl.eu/Technical-Framework

Jansen, A. S. P., Nguyen, X. V., Karpitskiy, V., Mettenleiter, T. C., & Loewy, A. D. (1995). Central Command Neurons of the Sympathetic Nervous System: Basis of the Fight-or-Flight Response. *Science*, *270*(5236), 644–646. https://doi.org/10.1126/science.270.5236.644

Jupe, L. M., & Hartwig, M. (2019). Deception, anxiety and folk beliefs: An examination of the asymmetrical anxiety heuristic. *Manuscript in Preperation*.

Keatley, D. (2018). *Pathways in crime: an introduction to Behaviour Sequence Analysis*. Springer.

Kleinberg, B., Arntz, A., & Verschuere, B. (2019). Being accurate about verbal credibility assessment. https://doi.org/10.31234/OSF.IO/H6PXT

Kohli, N., Yadav, D., Vatsa, M., Singh, R., & Noore, A. (2016). Detecting medley of iris spoofing attacks using DESIST. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*. https://doi.org/10.1109/BTAS.2016.7791168

Leal, S., & Vrij, A. (2008). Blinking During and After Lying. *Journal of Nonverbal Behavior*, *32*(4), 187–194. https://doi.org/10.1007/s10919-008-0051-0

Levine, T. R., Serota, K. B., & Shulman, H. C. (2010). The Impact of *Lie to Me* on Viewers' Actual Ability to Detect Deception. *Communication Research*, *37*(6), 847–856. https://doi.org/10.1177/0093650210362686

Lovell-Badge, R. (2013). Nine out of ten statistics are taken out of context | Understanding

Animal Research | Understanding Animal Research. Retrieved March 5, 2019, from http://www.understandinganimalresearch.org.uk/news/communications-media/nine-out-of-ten-statistics-are-taken-out-of-context/

Luke, T. J. (2018). Lessons from Pinocchio: Cues to deception may be highly exaggerated. https://doi.org/10.31219/OSF.IO/XT8FQ

Mann, S., Vrij, A., Bull, R., Vrij, A., & Bull, R. (2018). True lies: police officers' ability to detect suspects' lies, 147–172. https://doi.org/10.4324/9781315169910-10

Marcel, S., Nixon, M., & Li, S. (2014). *Handbook of Biometric Anti-Spoofing*. Retrieved from http://link.springer.com/content/pdf/10.1007/978-1-4471-6524-8.pdf

Marono, A., Clarke, D. D., Navarro, J., & Keatley, D. A. (2017). A Behaviour Sequence Analysis of Nonverbal Communication and Deceit in Different Personality Clusters. *Psychiatry, Psychology and Law*, 1–15. https://doi.org/10.1080/13218719.2017.1308783

Marono, A., Clarke, D., Navarro, J., & Keatley, D. (2018). A Sequence Analysis of Nonverbal Behaviour and Deception. *Journal of Police and Criminal Psychology*, *33*(2), 109–117. https://doi.org/10.1007/s11896-017-9238-9

McGrath, C. (2018, November 2). Lie detector scheme to boost fight against "terror threats" trialled at EU borders. *The Express*. Retrieved from https://www.express.co.uk/news/world/1040150/eu-news-lie-detector-scheme-fight-terror-threats-trialled-borders-hungary

McLennan, C. T. (2006). The time course of variability effects in the perception of spoken language: Changes across the lifespan. In *Language and Speech* (Vol. 49, pp. 113–125). https://doi.org/10.1177/00238309060490010701

Nahari, G. (2018). The Applicability of the Verifiability Approach to the Real World. In P. R. J (Ed.), *Detecting Concealed Information and Deception: Recent Developments* (pp. 329–349). https://doi.org/10.1016/B978-0-12-812729-2.00014-8

National Crime Agency. (2017). Identity Crime. Retrieved December 14, 2017, from http://www.nationalcrimeagency.gov.uk/crime-threats/identity-crime

Nguyen, D. T., Park, Y. H., Lee, H. C., Shin, K. Y., Kang, B. J., & Park, K. R. (2012). Combining Touched Fingerprint and Finger-vein of a Finger, and Its Usability Evaluation. *Advanced Science Letters*, *5*(1), 85–95. https://doi.org/10.1166/asl.2012.2177

Nortje, A., & Tredoux, C. (2019). How good are we at detecting deception? A review of current techniques and theories. *South African Journal of Psychology*, 008124631882295. https://doi.org/10.1177/0081246318822953

O'Sullivan, M., Frank, M. G., Hurley, C. M., & Tiwana, J. (2009). Police lie detection accuracy: The effect of lie scenario. *Law and Human Behavior*. https://doi.org/10.1007/s10979-008-9166-4

Ortony, A., & Turner, T. J. (1990). *What's Basic About Basic Emotions? Psychological Review* (Vol. 97). Retrieved from https://pdfs.semanticscholar.org/df84/be52a5c0a51db7e9545a0bdd2ab3c389cc3b.pdf

Poole, D. L., Mackworth, A. K., & Goebel, R. (1998). *Computational intelligence: a logical approach* (1st ed.). New York: omputational intelligence: a logical approach.

Porter, S., & Brinke, L. Ten. (2008). Reading between the lies: Identifying concealed and falsified emotions in universal facial expressions. *Psychological Science*, *19*(5), 508–514. https://doi.org/10.1111/j.1467-9280.2008.02116.x

Rothwell, J., Bandar, Z., O'Shea, J., & McLean, D. (2006). Silent talker: A new computer-based system for the analysis of facial cues to deception. *Applied Cognitive Psychology*, *20*(6), 757–777. https://doi.org/10.1002/acp.1204

Rothwell, J., Bandar, Z., O'Shea, J., & McLean, D. (2007). Charting the behavioural state of a person using a backpropagation neural network. *Neural Computing and Applications*,

16(4–5), 327–339. https://doi.org/10.1007/s00521-006-0055-9

Rozin, P., Lowery, L., & Ebert, R. (1994). *Varieties of Disgust Faces and the Structure of Disgust*. *Journal of Personality and Social Psychology* (Vol. 66). Retrieved from https://pdfs.semanticscholar.org/123b/28a4b062a73daa4abef15e91e23b49382bf4.pdf

Samuel, A. L. (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development*, *3*(3), 210–229. https://doi.org/10.1147/rd.33.0210

Sartori, G., Tasios, K., Vrij, A., Leal, S., & Fisher, R. P. (2018). Verbal Deception and the Model Statement as a Lie Detection Tool. *Frontiers in Psychiatry | Www.Frontiersin.Org*, *9*, 492. https://doi.org/10.3389/fpsyt.2018.00492

Soweon Yoon, Jianjiang Feng, & Jain, A. K. (2012). Altered Fingerprints: Analysis and Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *34*(3), 451–464. https://doi.org/10.1109/TPAMI.2011.161

Su, L., & Levine, M. (2016). Does "lie to me" lie to you? An evaluation of facial clues to high-stakes deception. *Computer Vision and Image Understanding*, *147*. https://doi.org/10.1016/j.cviu.2016.01.009

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. https://doi.org/10.1080/07421222.2015.1138569

Vrij, A. (2000). *Detecting lies and deciet: the psychology of lying and the implications for professional practice*. Chichester: Wiley.

Vrij, A., Fisher, R., Mann, S., & Leal, S. (2006). Detecting deception by manipulating cognitive load. *Trends in Cognitive Sciences*, *10*(4), 141–142. https://doi.org/10.1016/j.tics.2006.02.001

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., Fisher, R. P., Blank, H., Leal, S., & Mann, S. (2016). A cognitive approach to elicit verbal and nonverbal cues to deceit. *Cheating, Corruption, and Concealment: The Roots of Dishonesty*, 284–302. https://doi.org/10.1017/CBO9781316225608.017

Vrij, A., & Ganis, G. (2014). Theories in Deception and Lie Detection. In *Credibility Assessment: Scientific Research and Applications*. https://doi.org/10.1016/B978-0-12-394433-7.00007-5

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., Hope, L., & Fisher, R. P. (2014). Eliciting Reliable Information in Investigative Interviews. *Policy Insights from the Behavioral and Brain Sciences*, *1*(1), 129–136. https://doi.org/10.1177/2372732214548592

Vrij, A., Leal, S., Mann, S., Vernham, Z., & Brankaert, F. (2015). Translating theory into practice: Evaluating a cognitive lie detection training workshop. *Journal of Applied Research in Memory and Cognition*, *4*(2), 110–120. https://doi.org/10.1016/j.jarmac.2015.02.002

Vrij, A., Mann, S., Leal, S., Vernham, Z., & Vaughan, M. (2016). Train the Trainers: A First Step towards a Science-Based Cognitive Lie Detection Training Workshop Delivered by a Practitioner. *Journal of Investigative Psychology and Offender Profiling*, *13*(2), 110–130. https://doi.org/10.1002/jip.1443

Wang, W. S. Y. (1979). Language Change A Lexical Perspective. *Annual Review of Anthropology*, *8*(1), 353–371. https://doi.org/10.1146/annurev.an.08.100179.002033

Widrow, B., & Hoff, M. (1960). Adaptive switching circuits. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/241531.pdf

Woollacott, E. (2017, August 1). Better drugs, faster: The potential of AI-powered humans. *BBC News*. Retrieved from https://www.bbc.co.uk/news/business-40708043

Wu, Z., Singh, B., Davis, L. S., & Subrahmanian, V. S. (2017). Deception Detection in Videos. Retrieved from http://arxiv.org/abs/1712.04415