

Detecting Deception



Deception detection technologies such as polygraphs have been available for decades, although their use is controversial. Newer techniques are being developed that aim to detect deception based on facial imaging or brain activity. This briefing outlines the scientific basis for deception detection technology and considers the implications of its use in different contexts.

Deception detection uses questioning techniques in conjunction with technologies to monitor a range of physiological functions. Newer technologies are exploring the potential uses of brain or facial imaging as the basis for monitoring responses. This POSTnote looks at the:

- different types of questioning and tests;
- different technologies that can be used to monitor physiological responses;
- accuracy of the various different approaches;
- use of deception detection in different settings.

Deception Detection

Questioning and Tests

The questions used fall into three categories:

- **Irrelevant** questions are used to establish a baseline for truthful answers (Is today Tuesday?).
- **Comparison** questions are indirectly related to the event under investigation, but do not directly refer to it (As a young person did you ever physically hurt someone?). They are designed and delivered so as to encourage the subject to lie when answering. They are used to establish a baseline for untruthful answers.
- **Relevant** questions address issues related to the investigatory process (Did you shoot John Smith?).

Overview

- A wide range of technologies is available to detect deliberate deception. Their greater use within the UK would raise both regulatory and ethical issues.
- Polygraph testing is the most long-standing technique although research suggests that it is of variable reliability.
- A polygraph pilot is being conducted in the UK to test its usefulness as part of supervision for convicted sex offenders.
- Voice analysis has been used in the banking and insurance sectors and piloted by the government for detecting benefit fraud. However, peer-reviewed journals have questioned the reliability of this approach.
- There is interest in using newer techniques such as brain imaging and face recognition for surveillance/security. The reliability of such methods has yet to be established.

These questions can form the basis of different types of tests. Two of the most commonly used types are the comparison question test (CQT) and the guilty knowledge test (GKT). In a CQT, responses to relevant questions are compared with responses to comparison questions. Deceptive individuals are expected to show more pronounced responses to relevant questions, whereas truthful individuals are expected to show the opposite pattern of response. A GKT is designed to examine whether a subject possesses knowledge about a particular event. It uses indirect multiple-choice questions, each having one relevant, and several comparison, alternatives. In such tests it is assumed that the possession of relevant knowledge will affect the recorded response from a guilty subject to the relevant alternative.

Technologies

Polygraphs

Polygraphs record physical parameters governed by the part of the nervous system that is largely not under conscious control. Among the parameters a polygraph may record are heart and respiration rate, relative blood pressure, skin conductance, vasomotor (capillary dilation) responses¹ and muscular movement.

Polygraphs are assumed to indicate a short-term stress response associated either with lying or with information items that are of particular significance to the examinee. However, changes in these responses are not unique to deception; for instance they are also linked to mental effort as well as to emotional states such as fear, anger and surprise. Changes in these responses are recorded while a subject is asked a series of questions. Polygraphs can be used in conjunction with both CQTs and GKTs.

Voice Analysis

Speech pattern and language analysis have been used since the 1960s to attempt to detect deception. Modern approaches use computers to model aspects of speech such as pitch, frequency, intensity and micro tremors and to detect minute variations in the voice thought to signal lying. One feature of voice analysis is that it can be done over the telephone and thus may be used covertly. The technology is used in the banking and insurance industries to assess the likelihood that customers are telling the truth. Computer programmes record responses to control questions, look for variations in speech when operators probe claims with relevant questions to detect possible deception, and assign the caller a risk profile. The operator can then take further action if necessary.

Electroencephalography (EEG)

EEG uses electrodes placed on the scalp to measure patterns of brain activity triggered when meaningful information is recognised. Operators show relevant images or objects to subjects combined with specific questioning techniques to assess whether they recognise them. For instance, a suspected criminal may be shown a series of photographs of a crime scene, one of which investigators want to know whether the suspect recognises.

Newer Technologies

In addition to the longer-standing approaches outlined above, there is also interest in using newer technologies as the basis for deception detection techniques. Two of the technologies currently under development have shown some promise. These are novel brain imaging techniques (Box 1) and face recognition technology (Box 2). However, neither approach has yet been shown to be reliably useful.

Accuracy and Limitations

Experts agree that the previously described approaches cannot be relied upon in isolation, but may be useful as part of a range of techniques to probe deception. However there may be confounding effects that need to be taken into account when interpreting a result. For instance:

- where subjects are aware that they are being tested, this may cause anxiety and influence the result;
- people with certain psychiatric disorders may lie without intent deliberately to mislead by filling gaps in memories with fabrications they believe to be true;
- biases introduced by testers may affect the outcome.

Box 1. Novel Brain Imaging Techniques

Developments in brain imaging have provided new tools to study brain structure and function in real time. Imaging techniques measure different aspects of brain activity and may be able to link these to the cognitive states (behaviours, thoughts, emotions and intentions) that they produce. There are two main approaches:

- **Functional magnetic resonance imaging (fMRI)** detects the use of oxygen by brain tissue while a person performs specific tasks (identifying colours or recalling memories). It is also used in drug development, research and as a diagnostic tool.
- **Functional Near Infrared Spectroscopy (fNIRS)** can be used to assess various aspects of brain activity, but is most commonly used to look at blood oxygen levels. It is a lower resolution imaging tool than fMRI but may be used as a portable, field-based, system.

Research combining such techniques with existing methods might lead to more accurate deception detection tests. Neuro-imaging techniques might also provide indirect evidence of deception. For example, a subject could be shown a series of pictures from a crime scene and fMRI could be used to assess recognition of the object. There is speculation that further advances may enable 'mind-reading' – to ascertain what a person is thinking or feeling. However, the complexity of the human brain poses a barrier to developing this technology. Determining the psychological state of a person may be a more realistic goal.

Brain imaging is in its infancy - the equipment is very expensive, requires skilled operators and fMRI is unlikely to be available in a portable format in the near future. Critics have argued that reliable results from functional brain imaging are based on group averages rather than individuals. Newer studies suggest deception detection can reach 80% accuracy when analysed at the individual level.

Polygraphs

A review of the scientific evidence by the US National Academies of Science (NAS) concluded that polygraph accuracy depends on a number of factors. These include:

- **the purpose of use** - there is more evidence that the tests can give accurate results when they are used in relation to specific events (like a crime) than when applied to screen populations for employment purposes;
- **the type of test used** – CQTs are more prone to false positives (truth tellers assessed as liars) than GKTs;
- **the availability of counter-measures training** - for instance, false negatives might arise if subjects simulate anxiety when answering comparison questions;
- **the manner in which the test is conducted** – including the competency and ethics of the polygraph user.

The accuracy of polygraph testing is therefore a matter of some debate. A key problem is that the polygraph does not directly measure deception; it measures physiological variables to assess the relative psychological significance that the examinee places on the relevant questions.

Voice Analysis

Estimates of accuracy differ between academic papers based on peer review and the non-peer reviewed marketing material used by companies selling the technology. Peer reviewed papers estimate accuracy in separating truth-tellers from liars using voice analysis to be no better than chance and much less reliable than a well conducted polygraph test. For instance one such paper states that

Box 2. Novel Facial Imaging Analysis Techniques

Computers can detect minute changes in facial expressions, eye movement patterns, pupil dilation, sweating and blood flow, using visual and thermal detection tools. Researchers believe that these measurements can be linked to emotions and other cognitive processes including deception. The Engineering and Physical Sciences Research Council is funding research at the universities of Aberystwyth and Bradford to develop facial analysis technology. Early data from controlled testing in the laboratory indicate reliability at 67%. Researchers are liaising with several agencies on practical uses, including the Home Office, HM Revenue and Customs and the defence technology company QinetiQ. Possible uses of this tool include interrogations and interviews. An operational trial in collaboration with the UK Border Agency is planned for 2011 to test stress, anxiety and deception at the immigration desk.

“these machines perform at chance level”² and the NAS report noted “empirical research on the validity of the technique has been far from encouraging”¹. There are also concerns about their use with disadvantaged groups. For instance, a UK voice analysis trial reported difficulties in applying the tool to people whose first language is not English, or who have mental health problems or hearing difficulties. Nevertheless voice analysis is used by some companies.

EEG

While some studies have claimed up to 85% accuracy for EEG in deception detection trials¹, the availability of objects or images that would be recognised only by the individual who committed the crime is one factor that may limit its use. Another is that it requires complex equipment and skilled operators to collect and interpret data, and so is not well suited to applications requiring portable equipment.

Use of Deception Detection Technologies**Private Sector**

Polygraphs are widely used for pre-employment screening and in criminal investigations in over 80 countries. While their use is not common in the UK, several companies do offer polygraph services. There is no mandatory UK requirement for polygraph operators to be trained or professionally accredited, although the British Polygraph Association has a voluntary registration scheme. In practice, anyone can set up in business as a polygrapher. Those who practice polygraphy – particularly in academic settings – would welcome a mandatory training/accreditation scheme. They suggest it would ensure that polygraphs are used in conjunction with well structured interviews and questions and prevent their use in inappropriate settings. For instance, some TV shows use polygraphs for entertainment purposes to look for marital infidelity or other suspected untruths.

Insurance Sector

The insurance industry has used voice analysis technology for several years in an attempt to identify motor and household insurance fraud, which costs in excess of £1 billion a year. Customers may be unaware that calls are being monitored; companies may announce a disclaimer, “this call may be recorded for training or monitoring purposes” but do not have to specify the use of the data

collected. The Association of British Insurers (ABI) as a trade body does not regulate how many companies use the technology. Some of the bigger insurers such as Allianz and Zurich are yet to be convinced of its effectiveness. Allianz has looked at using voice analysis for motoring claims (thefts and road accidents) and decided that it was not cost-effective compared with more conventional methods of detecting fraud. The company is also concerned that using the technology might give customers the impression that they are automatically under suspicion. Zurich does not use voice analysis for similar reasons.

Public Sector: Social Welfare Fraud

The government pays £190 billion in benefits, tax credits and child benefit every year, administered by HM Revenue and Customs (HMRC) and the Department for Work and Pensions (DWP). The most recent figures available suggest that in 2008/09 deliberate fraud cost:

- around £1 billion in benefits, accounting for one third of all overpayments and ~0.7% of DWP expenditure;
- an estimated £462 million in tax credits accounting for 22% of losses on this benefit.³

The National Audit Office considers the level of fraud in the benefits and tax credits systems too high.⁴ As part of a wider fraud and error programme to reduce losses, the DWP ran a pilot programme using voice analysis technology to analyse claims for housing and council tax benefit, income support and jobseekers’ allowance. The trial involved 24 local authorities, cost £2.2 million, and the results were published in 2010.⁵ Overall, the DWP was not able to conclude that the technology worked effectively and consistently in a benefits environment. DWP plans for universal credit and a move towards dealing with claimants online makes it unlikely that it will adopt telephone technologies. The project was criticised by civil liberty groups and others who doubted the scientific validity of the technique. The voice technology company involved argued that the system works when correctly implemented and managed, but that lack of consistency in operational performance impacted upon the outcomes in some of the pilot studies.

Criminal Justice: Managing Sex Offenders

The Labour Party’s 2005 manifesto committed to piloting mandatory post-conviction polygraph testing of sex offenders. This required new legislation, introduced in England and Wales in 2009 to add extra conditions to an offender’s release licence to include mandatory participation in pilot polygraph testing.⁶ Following a successful initial pilot of voluntary testing, the Ministry of Justice is running a three year mandatory pilot in the East and West Midlands (Box 3).

Advocates argue that this permits staff managing offenders released on licence to target interventions, controls and behaviour change programmes more effectively. Critics claim there is insufficient evidence to support polygraph testing. They refer to a lack of comparative research which separates out the effectiveness of polygraph testing from confounding factors, such as the treatment provided to

offenders on release.⁷ A comparative evaluation, is being carried out on the mandatory testing pilot programme to answer these criticisms. To date, two offenders have sought judicial review of their mandatory inclusion in the pilot; neither found in favour of the offenders.

Criminal Justice: Forensic Evidence

In June 2008, a judge presiding over a murder trial in India ruled that a brain scan (Box 1) of the defendant could be submitted as evidence. Expert witnesses involved in the case claimed that the defendant's pattern of brain activity during questioning indicated knowledge of facts that could be known only to the murderer. The case triggered concerns that imaging or deception detection technologies might:

- be used in ways that infringe rights to privacy; or,
- before they have been shown to be reliable.

The current consensus is that there is insufficient evidence of reliability to support the use of brain imaging in legal cases. There is a need for more research into these techniques as well as for careful consideration of the social and ethical implications of their use in forensic settings. While such scans have not been used as forensic evidence in the UK, the Association of Chief Police Officers is monitoring the progress of the technology.

Security and Counter-Terrorism

In the US, defence agencies are developing new deception detection tools for use in criminal/terrorist investigations. A portable polygraph has been used by US military personnel in Afghanistan. Field trials have been conducted in several theatres of war but information on performance and reliability is not publicly available. In the UK, the Defence Science and Technology Laboratory (DSTL) considers that there is a lack of consistent evidence to support use of polygraph tests. Instead the UK focus has been on interview skills, interviewer selection and training. The DSTL is currently assessing the applicability of an fNIRS based system to military operations. Although fNIRS lacks the resolution of fMRI, it is portable and less invasive (Box 1).

Regulation

UK regulation of deception detection technologies varies depending on the setting. In the criminal justice system, polygraph tests are not acceptable as evidence in UK or most other European courts of law in criminal cases. However, such tests are being piloted in the UK for the management of sex offenders (Box 3). Their use for such purposes is regulated by the Polygraph Rules 2009, which came into force in April 2009⁶. They allow the Secretary of State to require certain offenders released on licence to undergo polygraph testing to monitor compliance with the terms of a licence and to improve offender management. However they prohibit the use of polygraph evidence in any proceedings taken against a released offender.

In academic research, the use of deception detection technologies must meet the criteria laid down by research ethics committees. Those conducting the tests are also bound by codes of conduct specified by professional bodies

Box 3. Polygraph Testing of Sex Offenders

Initial pilot research was conducted by forensic psychiatrists at the University of Newcastle on polygraph testing of sex offenders who volunteered to be tested. It suggested that these offenders:

- disclose more reliable information about the nature of their sexual history and deviant acts;
- gave fuller accounts of offences with fewer instances of denials;
- were more likely to disclose behaviours considered high-risk by probation staff (thus leading to treatment or sanctions).

Overall, polygraph-tested offenders disclosed information relevant to supervision more readily (70%) than those who were not tested (14%). It is not known whether false disclosures were made.

Following the outcome of the research pilot, the National Offender Management Service, part of the Ministry of Justice (MoJ), is running a three year mandatory polygraph pilot to test whether use of polygraphs increases the disclosure offenders make under supervision and therefore improves how offenders are managed when they have no choice but to be tested. Mandatory testing began in April 2009 for sex offenders released on licence who live in the East and West Midlands. A failed test will not result in recall to prison, but an admission after a failed test, or a refusal to be tested, may result in an amendment to the management of the offender and potentially some form of enforcement action.

Over 400 testing sessions on 300 offenders were carried out in the first year of the pilot. A polygraph examiner conducts the test on the offender designed to find out if the offender is complying with the licence conditions then meets with the probation officer and the offender to share the results. Actions to make sure the licence is adhered to are then planned. The MoJ is running a comparison study in 2 other probation regions with which to compare results. Researchers are collecting information about the behaviour of offenders who are being supervised and who would have been referred for testing if they had lived in the pilot areas. Research thus far shows that offenders in the polygraph pilot areas are making more disclosures than those in the comparison regions. Full results will be with ministers by summer 2012 and will be subsequently published.

like the British Psychological Society. However, there is little formal regulation of the use of deception detection technologies in other settings, such as employment or security screening. The NAS report pointed out that even tests with an 80% or higher accuracy rate would generate unacceptably high numbers of 'false alarms' if used to screen large populations for rare transgressions such as terrorism. The development of new deception detection technologies raises the question of whether a more formal regulatory framework is required to ensure that:

- those taking a test have given their fully informed consent and that there is no coercion involved;
- tests are conducted in an appropriate manner without bias or duress;
- those conducting the tests have the appropriate qualifications;
- test results are not misused and privacy is safeguarded.

Endnotes

- 1 The vasomotor centre is the part of the brain that controls body temperature
- 2 Eriksson and Lacerda, *Journal of Speech, Language and the Law*, **14** (2) 169-193, 2007
- 3 *Fraud and Error in the Benefit System – October 2008-September 2009*, DWP
- 4 *Tackling External Fraud*, National Audit Office, HM Treasury, 2008
- 5 www.dwp.gov.uk/docs/vra-evaluation.pdf
- 6 Statutory Instrument No. 619, 2009
- 7 Ben-Shakhar, *Legal and Criminological Psychology*, **13** (2) 191-207, 2008