L. Farwell, "Brain Fingerprinting: Detection of Concealed Information" in Wiley Encyclopedia of Forensic Science, eds A. Jamieson and A.A. Moenssens, John Wiley: Chichester. DOI: 10.1002/9780470061589.fsa1013. Published June 16, 2014

Brain Fingerprinting: Detection of Concealed Information

Introduction: The State of the Art Before Brain Fingerprinting

The record stored in the brains of the witness and perpetrator is often a much more comprehensive account of the crime than what can be pieced together from connecting a few specific features of the crime scene with a few specific features of the perpetrator.

This record has not been accessible to scrutiny. The stored record has the advantage of often providing by far the most comprehensive account of the crime available.

Witness testimony is a subjective report of the contents of memory. Memory is known to be limited and imperfect in a number of ways (*see* ***Eyewitness Memory Issues in Civil Litigation***). It is approximate, sometimes distorted, selective, and subject to numerous influences. It is known to be affected by mental or physical illness, injury, passage of time, drugs, and many other factors.

The two primary disadvantages of witness testimony are (i) human memory is imperfect and (ii) the witness may lie.

Investigators have developed psychophysiological methods to attempt to detect deception (*see* ***Deception: Detection of***; ***Deception Detection***). The fundamental premise of the various techniques for detection of deception is that lying produces emotional stress and other psychological effects, which in turn produce physiological arousal and other changes. These can be measured through changes in perspiration, blood pressure, breathing, and so on. The commonly used control question test in conventional detection of deception employs direct, relevant questions regarding participation in the crime, such as “Did you shoot Mr. Jones?”

Lykken [1, 2] originated a new technique for discovering more of the details of the record of the crime stored in the brain. It is known as the *guilty knowledge test* (GKT) or concealed information test [3–6].

The conventional GKT is an adjunct to interrogation and testimony (*see* ***Interrogation***). It is a method not of directly detecting evidence of a crime stored in the brain but of determining the veracity of a subject who is testifying regarding the evidence and who may be seeking to conceal his connection with it.

Methods for detection of deception or credibility assessment have met with limited success. They have been used primarily to guide investigations rather than to definitively establish the relevant facts.

Overview of Brain Fingerprinting Science and Technology

There has been no objective, scientific way to detect the record stored in the brain and thereby to connect the perpetrator with the crime scene.

Brain fingerprinting seeks to address this fundamental lack.[a] Brain fingerprinting was developed to provide an objective way to connect the established features of the crime scene with the record of the crime stored in the brain of the perpetrator [7–16]. This is accomplished by measuring the response of the subject’s brain to stimuli in the form of words or pictures presented briefly on a computer screen. During a brain fingerprinting test, electroencephalograph (EEG) signals are recorded noninvasively from the scalp. When a subject recognizes and takes note of something significant in the present context, the brain emits an “Aha!” response. This involves the firing of neurons in a specific, identifiable pattern known as *P300-MERMER* that can be detected by computer analysis of the EEG signals. When a subject recognizes a specific feature of the crime scene, such as the murder weapon, the brain fingerprinting system detects the “Aha!” response and its corresponding EEG pattern. This reveals that the subject knows the relevant information. If the subject does not possess the relevant knowledge, then this brain response is absent.

The data are then analyzed using a statistical and mathematical algorithm to determine whether the crime-relevant information is known by the subject.

Brainwave Measurements and Event-Related Brain Potentials

EEG involves the measurement of patterns of voltage changes that originate in the brain. When the brain conducts certain tasks, specific patterns of EEG (or "brainwave") activity are produced known as *event-related potentials* (ERPs).

As the brain is engaging in the information processing of interest in a scientific experiment, it is also engaging in many other activities. The result is that the brainwaves measured at any time are a mixture of the relevant (event-related) activity and other brainwave activities. In order to isolate the activity of interest, the standard procedure in ERP research is to present a stimulus many times and average the responses [17–21]. All of the brainwave activity that is not specifically related to processing this specific stimulus averages out to near-zero, because its timing is unrelated to the event of the appearance of the stimulus on the screen. What is left in the average response is the ERP: the brainwave pattern that is specifically related to the event of interest.

Each stimulus presentation and associated response is referred to as a *trial*. The larger the number of trials in each average brainwave response, the more extraneous brainwave activity is eliminated by the averaging procedure [17]. In order to obtain valid and reliable results, experience has shown that a minimum number of trials is required [12]. Experimenters usually run several tests, each containing about 100 trials. Each separate test is referred to as a *block*. Successive blocks may use the same stimuli or different stimuli relevant to the same specific event or knowledge.

The P300 is an electrically positive potential that occurs at 300 or more milliseconds after the stimulus [20, 22]. The name refers to the fact that the response is electrically positive (P) and has a latency of at least 300 ms (300). The P300 occurs when a subject recognizes a stimulus as significant in the context in which it is presented. It may be called an *Aha* response. In the early P300 research, the responses were elicited by very simple stimuli such as clicks or tones. These were made significant in context by the experimental instructions. When the stimulus and the task are simple, the P300 peak occurs at about 300 ms after the stimulus.

In the initial brain fingerprinting research, Farwell and Donchin [10, 23] used the P300 event-related brain potential. Later, it was discovered that the P300 can be considered to be a part of a larger response termed a memory and encoding related multifaceted EEG response or P300-MERMER.

The Discovery of the P300-MERMER

In dealing with real-life situations, it was found to be necessary to use longer and more complex stimuli to accurately communicate the necessary information to the subject [13]. In order to present realistic stimuli that accurately represented knowledge unique to FBI agents, researchers found it necessary to use stimuli consisting of several words, sometimes several long words. It took the subjects longer to read the words and assess their significance than in previous experiments with simpler stimuli.

To give the subjects time to process the stimuli and respond appropriately, they lengthened the interval between stimuli from 1500 to 3000 ms. They recorded a longer segment of brainwave data in each trial.

This more complex response included both the P300 and a late negative peak (LNP). This was the basis for the P300-MERMER [7, 11–13]. The P300 is maximal in the parietal area. The LNP that constitutes the latter part of the P300-MERMER is parietally maximal yet also frontally prominent [7, 9] (i.e., it is at its largest in the back area of the head).

The classical P300 is also known by various other names, including the P3, N2–P3 complex, P3a and P3b, late positive complex, and late positive component. There has been considerable discussion as to whether the P300 is a unitary response or in fact a constellation of several responses [12, 24]. There has also been discussion over whether the various names refer to the same or slightly different phenomena [12, 24].

No doubt there will be considerable discussion as to whether the MERMER or P300-MERMER is a unitary phenomenon inclusive of the P300 and the LNP or whether the LNP is a separate component from the component or components that make up the P300 [12–14]. The answers to these questions are empirical, to be settled by further research.

Differences in nomenclature also exist. Over a thousand published studies have associated the name "P300" with a positive peak. The first report of the P300-MERMER, including the positive peak of the P300 and the LNP, was in 1994 [7]. By 2001, almost all researchers in detection of concealed information were using the full P300-MERMER in data analysis. Some authors [25, 26], however, have used the name “P300” to refer to the entire P300-MERMER response, including not only the traditional P300 peak but also the LNP of the P300-MERMER.

Additional facets in the P300-MERMER waveform that occur simultaneously with the positive and negative peaks have been reported [7, 9, 11–13, 27]. The nature of these additional facets and their relationship to the more readily visible positive and negative peaks is also an empirical question to be resolved by further research.

In all brain fingerprinting research using either the P300-MERMER or the P300 alone, there have been no false negatives and no false positives. These results are summarized in Tables 1 and 2, further discussed later. When the full P300-MERMER is included in the data analysis algorithm, there have also been no indeterminates. In brain fingerprinting research using the P300 alone, results have been indeterminate in 3% of cases overall, consisting of 12.5% in one study. As discussed later, an indeterminate response is not an incorrect response but rather the determination that insufficient data are available to make a determination in either direction with high statistical confidence. The acceptance of the accuracy of these techniques is not universal [26, 28, 29]. However, proponents suggest that this is because of the failure of some authors to properly adhere to the necessary protocols described here and elsewhere [12–14, 30, 31].

Different commentators have summarized the published results differently, depending on which distinctions they make or do not make with respect to methods practiced in different studies. Some authors distinguish between studies that meet the brain fingerprinting standards and studies that do not, and consequently they conclude correctly that the former consistently report no errors (which is generally characterized as “less than 1% error rate”) and the latter report much higher and highly variable error rates [12–14, 30, 31]. Authors who do not make such a distinction, and thus do not consider the differences in results produced by fundamentally different methods, correctly report that error rates are highly variable for studies in the detection of concealed information with ERPs taken as a whole [26, 28, 29].

Brain Fingerprinting Scientific Protocol

Experimental Design

Brain fingerprinting tests should be conducted according to set protocols. “Reference” stimuli, including targets (information on the crime that the subject knows whether he or she committed it or not), irrelevants (inaccurate information about the crime), and probes (information about the crime known only to the perpetrator and the investigators) are presented to the subject in order to create the background signal for known data [10–13, 23].

For example, if a subject claims not to have been at the murder scene and not to know what the murder weapon was, a probe stimulus could be the murder weapon, such as a knife. Irrelevant stimuli could be other plausible (but incorrect) murder weapons such as a pistol, a rifle, and a baseball bat.

Brain fingerprinting data analysis comprises a mathematical and statistical algorithm that computes a determination of “information present” or “information absent”. The information that is either present or absent in the brain of the subject is the information contained in the probes. The brain fingerprinting method also computes a statistical confidence for each individual determination, for example, “information present, 99.9% confidence”. If the statistical algorithm does not return either an “information present” or an “information absent” determination with a high statistical confidence, the outcome is classified as “indeterminate”.

An indeterminate result is not an error. It is a determination that the data analysis algorithm has insufficient data to make a determination of either information present or information absent with a high statistical confidence.

Things are significant to a person in context. The context of the probe stimuli in relation to the crime or other investigated situation is established in the interview before the brain fingerprinting test. Immediately before the test, the experimenter describes the significance of each probe in the context of the investigated situation. Before the test, the subject has explicitly stated that he does not know which stimulus is the probe containing the correct information.

Under these circumstances, a large P300-MERMER in response to the probes provides evidence that the subject recognizes the probes as significant in the context of the investigated situation. If the experimenter has followed the proper protocols, the subject has eliminated all plausible nonincriminating explanations for this knowledge by his own account before the test. Therefore, an information-present response can provide evidence regarding the subject's involvement in the investigated situation.

Data Analysis

The purpose of data analysis in brain fingerprinting studies is to determine whether the probe responses are more similar to the target responses or to the irrelevant responses and to provide a statistical confidence for this determination. The determination and statistical confidence must be computed for each individual subject.

To be valid, the statistical confidence for an individual determination of "information present" or "information absent" must take into account the level of variability in the individual brain responses that are aggregated in the average response. Bootstrapping was introduced to compute a statistical confidence for each individual determination that takes this variability into account [10, 12, 13, 32, 33].

If the bootstrapping procedure produces a high statistical confidence that the probe response is more similar to the target response than to the irrelevant response, then the determination is "information present". If the bootstrapping procedure produces a high statistical confidence that the probe response is more similar to the irrelevant response, then the determination is "information absent".

If neither the statistical confidence for "information present" nor the confidence for "information absent" is high enough to meet the established criteria, then the result is "indeterminate". Typically, a confidence of 90% is required for an "information present" determination. A lower criterion, typically 70%, is generally required for an "information absent" determination.

Before applying the bootstrapping technique on correlations between waveforms, noise in the form of high-frequency activity is eliminated by the use of digital filters. Specific types of filters known as *optimal digital filters* are highly effective for eliminating this high-frequency noise while preserving the brainwave pattern of interest in event-related brain potential research [34].

Brain Fingerprinting and Other Techniques

Brain fingerprinting and the conventional GKT are concerned with the relevant features of the crime that are known to the perpetrator and not to an innocent suspect.

An "information present" or "information absent" determination is entirely independent of whether the subject tells the truth or lies about this information or anything else.

Brain fingerprinting is fundamentally different from attempts to detect deception by the polygraph and similar instruments. It detects knowledge, not lies [3, 7, 9–13, 15, 35].

Principles of Applying Brain Fingerprinting in the Laboratory and the Field

Brain fingerprinting does not evaluate whether the investigator's account of the crime is accurate or whether the relevant knowledge embodied in the probe stimuli actually correctly represents the crime.

It only detects whether the subject has the relevant knowledge. The prosecution may argue that the best explanation for an "information present" determination is that the subject learned the relevant knowledge while committing the crime. (In a properly executed brain fingerprinting test, plausible alternative hypotheses will have been eliminated before the test.) The defense may argue that an "information absent" determination introduces a reasonable doubt that the subject is guilty and provides support for his or her claims of innocence.

Brain Fingerprinting in Criminal Cases

Three cases describe the application of brain fingerprinting in criminal cases. They are the James B. Grinder case, the Terry Harrington case, (*see* ***Daubert v. Merrell Dow Pharmaceuticals***; ***Evidence: Rules of***) and the Jimmy Ray Slaughter case. Details of the relevant circumstances and results are detailed in [12, 13, 36]. See also [35, 37–40] (Figures 1–3).

Standards for Brain Fingerprinting Tests

Procedures for brain fingerprinting have been proposed to maximize the reliability of the technique

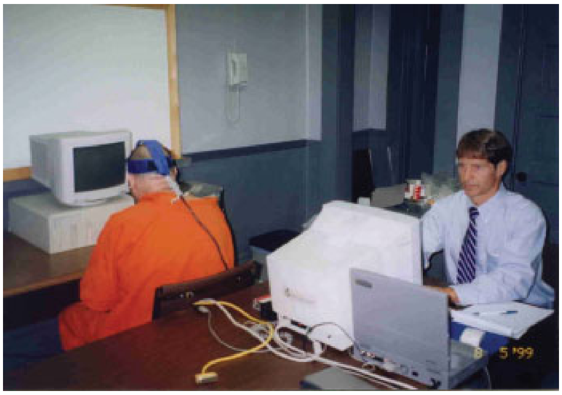

Figure 1 Dr. Larry Farwell conducts a brain fingerprinting test on serial killer J.B. Grinder, then a suspect in the murder of Julie Helton. The test showed that Grinder's brain contained a record of certain salient features of the crime. He pled guilty and was sentenced to life in prison. [Reproduced with permission from Ref. 12. © L.A. Farwell, 2012.]

[7–14]. These include restricting scientific conclusions to a determination as to whether a subject has the specific crime-relevant knowledge embodied in the probes stored in his or her brain [11–13, 35, 37].

Published Research on Brain Fingerprinting

Overview of Research

While casework is not technically considered scientific testing, brain fingerprinting technology has been used in casework.

The studies conducted on brain fingerprinting testing have included field/real-life and laboratory studies.

Brain fingerprinting testing has been used to detect information stored in the brain regarding two different types of activities.

1. Specific issue tests detect information regarding a specific incident or a particular crime.
2. Specific screening or focused screening tests detect information relevant to a specific type of training or inside knowledge of a specific field, such as FBI agent training or knowledge of bomb making.

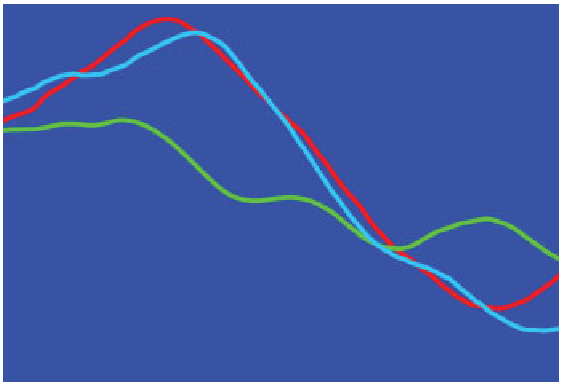

Figure 2 Brain response of serial killer J.B. Grinder to information relevant to the murder of Julie Helton. Voltage at the parietal midline area (range: −2 to 5 μV), average of all responses for the time range from 0.35 to 1.20 s after the stimulus. There is a clear P300-MERMER in response to the known targets (red line). The P300 is the positive voltage peak at the upper left. The P300-MERMER contains both the positive peak and the LNP at the lower right. There is no P300-MERMER in response to the irrelevants (green line). The probes (blue line) contain specific details about the crime that the criminal investigators believe the perpetrator experienced in committing the crime. Grinder's response to the probes, like his response to the targets, clearly contains a P300-MERMER. Mathematical data analysis yielded a determination of "information present" with a statistical confidence of 99%. This shows that the record in the brain of J.B. Grinder contains salient details of the murder. [Reproduced with permission from Ref. 12. © L.A. Farwell, 2012.]

Brain fingerprinting testing is not applicable for general screening applications, that is, interrogation where the investigators do not know what specific information they seek to detect.

Summary of Results of Research and Field Applications

For all brain fingerprinting studies by Farwell and colleagues, Grier A' [41] values are 1.0.

Table 1 [42] outlines the laboratory studies on brain fingerprinting testing conducted by Farwell and colleagues.

Table 2 [43, 44] outlines the field/real-life studies on brain fingerprinting testing conducted by Farwell and colleagues.

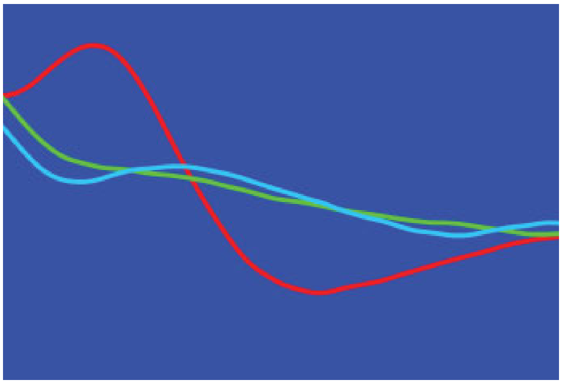

Figure 3 Brain response of innocent convict Terry Harrington to information relevant to the murder of which he had been convicted. Voltage at the parietal midline area (range: −2 to 15 μV), average of all responses for the time window from 0.5 to 1.5 s after the stimulus. The red line is the response to targets – items he knows. As he recognizes them, he gets a specific brain response. The P300 is the positive peak in the upper left. The P300-MERMER is the P300 and the negative peak in the lower right. The green line is the response to irrelevant stimuli, wherein the P300-MERMER is lacking. The blue line is the response to the probes, which are items relevant to the crime. Note that there is no P300-MERMER in response to the probes. Mathematical data analysis yielded a determination of "information absent" with a statistical confidence of 99%. This shows that Harrington's brain does not have a record of these specific crime-relevant details. [Reproduced with permission from Ref. 12. © L.A. Farwell, 2012.]

Laboratory tests have been conducted on mock crimes/espionage scenarios with stimuli consisting of both words and phrases [10] and pictures [42].

Specific issue field tests have applied brain fingerprinting to detect, among other things, real-life events including felony crimes in CIA and FBI studies [11, 13] and real crimes with substantial consequences (either a judicial outcome, i.e., evidence admitted in court, or a $100 000 reward for beating the test) [12, 13, 37].

Specific screening field tests have applied brain fingerprinting to detect, among other things, knowledge unique to FBI agents [12, 13] and to bomb makers (explosives/EOD/IED experts) [12, 13]. Four studies of specific issue and specific screening field tests compared results using the P300-MERMER in data analysis with results using the P300 alone [13]. Error rate was 0% with both analysis methods. Statistical confidence for "information present" or "information absent" determinations was higher with the P300-MERMER for most subjects. Median statistical confidence for individual determinations with the P300-MERMER was 99.9% [13]. The P300-MERMER produced a statistically significant improvement over the P300 alone in each of the four studies.

Replications of brain fingerprinting science in other laboratories

Others have published results of similar accuracy. Iacono and colleagues [45] used P300 ERPs to detect learned information in a three-stimulus experimental design. The authors achieved 6% error rate in detecting learned material as learned and 4% error rate in identifying unknown material as unknown. They used a Bayesian algorithm for computing a determination and statistical confidence for each individual subject. Although the mathematical algorithm was not identical to the bootstrapping algorithm used

Table 1 Brain fingerprinting laboratory, specific issue studies by Farwell and colleagues

Study name [publication references]	Type of information detected	Number of subject tests	Error rate (%)[a]	Indeterminates[b]
Mock Espionage Study "Experiment 1" [10, 23]	Mock crime/espionage; word stimuli	40[c]	0	5
CIA Picture Study [42][d]	Mock crime/espionage; picture stimuli	28	0	0

[a] Percentage of determinations made that were errors: false positives and false negatives.

[b] Number of cases where no determination was made. In all indeterminate cases, analysis was with P300 alone, not P300-MERMER. Analysis with P300-MERMER yielded no indeterminates, no false negatives, and no false positives.

[c] Each individual in Mock Espionage Experiment 1 was tested once as an "information present" subject and once on different information as an "information absent" subject: 40 subject tests were conducted on 20 individuals.

[d] Results reported in a conference abstract.

Table 2 Brain fingerprinting field/real-life studies by Farwell and colleagues

Study name [publication references]	Type of information detected	Subject tests	Error rate[a] (%)	Indeterminates[b]
Specific issue tests				
Real-life "Experiment 2" [10, 23]	Real-life minor crimes	8[c]	0	1
CIA Real-life study [13]	Real-life events (some crimes)	20	0	0
Real Crimes Real Consequences $100 000 Reward Study [13]	Knowledge of actual crimes; judicial outcome or $100 000 reward for beating test	14	0	0
FBI Real-life Events Study [11]	Real-life events in FBI agents' lives	6	0	0
Specific Screening Tests				
FBI Agents Study [13]	FBI-relevant knowledge, FBI agents	21	0	0
Bomb Maker Study [13]	Bomb-making knowledge	21	0	0
CIA/US Navy Study [43][d]	Expertise in military medicine	30	0	0
Occupation Study [44][d]	Occupation-specific knowledge	4	0	0

[a] Percentage of determinations made that were errors: false positives and false negatives.
[b] Number of cases where no determination was made. In all indeterminate cases, analysis was with P300 alone, not P300-MERMER. Analysis with P300-MERMER yielded no indeterminates, no false negatives, and no false positives.
[c] Each individual in Real-life Experiment 2 was tested once as an "information present" subject and once on different information as an "information absent" subject: eight subject tests were conducted on four individuals.
[d] Results reported in a conference abstract.

by Farwell and colleagues, the results showed a similar level of accuracy.

In another study, the authors [46] compared their Bayesian algorithm with the bootstrapping of the brain fingerprinting technique and with a simplified application of bootstrapping. They replicated the high accuracy of the brain fingerprinting technique. They reported no false positives using this method and that increased motivation to beat the test increased the accuracy of the brain fingerprinting technique. This may be one of the reasons for the extremely high accuracy achieved using brain fingerprinting in field situations [12, 13]. The authors theorized that the basis of this difference was cognitive rather than emotional: that the difference resulted from increased cognitive salience of stimuli in the more motivated condition.

Limitations of Brain Fingerprinting

Like all sciences, brain fingerprinting cannot be correctly described as "100% accurate". However, the limited data available suggest a very high degree of accuracy.

Limits to the Applicability of Brain Fingerprinting Testing

Brain fingerprinting is not applicable in every case for every suspect. The investigator must have some knowledge about the crime. When no knowledge about what was involved in the crime is available, then a brain fingerprinting test cannot be conducted.

Similarly, a brain fingerprinting test is not applicable when the subject knows absolutely everything about the crime that investigators know because he or she has been told this information after the crime.

In some cases, however, such as the Terry Harrington case [37], it is possible to find salient features of the crime to which the subject was never exposed, and which he or she claims not to know. Under these circumstances, a brain fingerprinting test can be conducted using these salient features of the crime as probe stimuli.

Brain Fingerprinting and the Limitations of Human Memory

Human memory is not perfect. It is affected by myriad factors, including mental and physical illness, trauma, injury, drugs, aging, passage of time, and many other well-known factors.

Brain fingerprinting does not indicate directly what took place at the crime scene. The value of brain fingerprinting is that it can provide evidence that the triers of fact use in their decisions regarding what took place. Brain fingerprinting does not determine what the facts are, other than the one fact of presence or absence of specific information stored in a specific brain.

Non-Brain Fingerprinting Research on Brainwave-Based Detection of Concealed Information

Common Errors in Research on Brainwave-Based Detection of Concealed Information

The brain fingerprinting three-stimulus paradigm was introduced in 1986 [10, 23]. The authors coined the term *probe* to refer to the crime-relevant stimuli known only to the perpetrator and investigators and *target* to refer to the known stimuli. Many of the subsequent experimenters, however, did not follow the standards for brain fingerprinting cited earlier. For a comprehensive review of all relevant publications, see [12].

So far, all of the alternative methods that have failed to meet these standards have produced higher error rates than those reported by Farwell and others whose research has met the brain fingerprinting standards, generally about 10–20 times more errors (see [12] and [13]; ***Deception, Detection of, P300 Event-Related Potential (ERP)***). Some specific methods have produced error/accuracy rates as low as chance. [26, 30, 31, 47–51]. Moreover, statistical confidences produced by these methods have been substantially lower than those of brain fingerprinting.

The following is a summary of the most common errors and the errors that have produced the greatest increases in error rates and decrements in statistical confidence and/or validity. For a detailed discussion of how the failure to meet specific brain fingerprinting standards results in higher error rates and lower statistical confidences, see [12].

1. Failure to recognize that brain fingerprinting detects only the presence or absence of certain specific knowledge stored in the brain [47, 52, 53] and not how the knowledge was obtained or what the subject has done or not done.
2. Failure to establish separate determinations and reasonable statistical confidence criteria for both information-present and information-absent results. Failure to include an indeterminate category [12, 13, 26, 54–60].
3. Failure to apply a mathematical classification algorithm. Failure to record and analyze a subject's responses to known, relevant information (target stimuli) as well as to irrelevant information (irrelevant stimuli) and to classify the subject's responses to the stimuli being tested (probes) as being more similar to one or the other of these templates. Methods that fail to meet this standard, ignore the target stimuli in data analysis, and merely compare the amplitude of the probe and irrelevant responses consistently produce higher error rates, as well as statistical confidences averaging 50% (chance) for information-absent determinations in all published studies to date [12, 13, 26, 54–60].
4. Confounding "lying" with knowing the relevant information [26, 55, 56, 61]. For a discussion see [62].
5. Failure to inform subjects of the significance of the probes and to describe the significance of the probes and targets that will appear in each block immediately before the block [47, 63].
6. Measuring P300 from the wrong scalp location [55, 60].
7. Failure to run a sufficient number of trials for adequate signal-to-noise enhancement or failure

to apply adequate signal-processing and noise-reduction techniques such as digital filters and artifact detection algorithms [26, 28, 47, 52, 60].

8. Failure to require an overt behavioral task that requires the subject to recognize and process every stimulus, specifically including the probe stimuli [48–51, 64–66].

Other Non-Brain Fingerprinting Studies

Other experimenters have attempted to detect concealed information with event-related brain potentials by applying methods that are different from brain fingerprinting in various ways [12, 67]. Some studies have used mock crimes or virtual mock crimes [68, 69]. Some have applied various other knowledge-imparting procedures [70–73]. Some have detected recognition of well-known personal information such as pictures of known individuals [63, 73]. These studies have met some but not all of the brain fingerprinting scientific standards. Accuracy rates have varied considerably based on the methods used.

A number of researchers in Japan [60, 74, 75] used a variety of procedures applying event-related brain potentials in the detection of concealed information. Results varied considerably according to the methods applied.

Some studies were designed to detect simulated malingering (*see* ***Malingering: Forensic Evaluations***) relevant to brain injury and memory loss [76–83]. These studies are not directly comparable to brain fingerprinting.

Countermeasures

Brain fingerprinting has proven to be highly resistant to countermeasures. In a series of brain fingerprinting tests on actual crimes, in which some of the experiments offered a $100 000 reward for beating a brain fingerprinting test, countermeasures had no effect on the results of brain fingerprinting [12, 13] (see also [84]).

Endnotes

[a] The term "brain fingerprinting" is derived from the following analogy. Fingerprinting matches prints at the crime scene with prints on the fingers of the subject (*see* ***Friction Ridge Examination (Fingerprints): Interpretation of***), DNA "fingerprinting" matches biological samples from the crime scene with biological samples from the suspect (*see* ***DNA***). Similarly, brain fingerprinting matches information from the crime scene with information stored in the brain of the subject. Like fingerprinting, brain fingerprinting analyzes multiple facets of the evidence to detect a match.

References

[1] Lykken, D.T. (1959). The GSR in the detection of guilt, *Journal of Applied Psychology* **43**, 385–388.

[2] Lykken, D.T. (1960). The validity of the guilty knowledge technique: the effects of faking, *Journal of Applied Psychology* **44**, 258–262.

[3] Iacono, W.G. (2008). The forensic application of "Brain Fingerprinting": why scientists should encourage the use of P300 memory detection methods, *The American Journal of Bioethics* **8**(1), 30–32.

[4] Iacono, W.G. (2007). Detection of deception, in *Handbook of Psychophysiology*, J. Cacioppo, L. Tassinary & G. Berntson, eds, Cambridge University Press, New York, pp. 688–703.

[5] Iacono, W.G. & Patrick, C.J. (2006). Polygraph ("lie detector") testing: current status and emerging trends, in *The Handbook of Forensic Psychology*, I.B. Weiner & A.K. Hess, eds, John Wiley & Sons, Inc., Hoboken, NJ, pp. 552–588.

[6] Iacono, W.G. & Lykken, D.T. (1997). The validity of the lie detector: two surveys of scientific opinion, *Journal of Applied Psychology* **82**, 426–433.

[7] Farwell, L.A. (1994). Method and Apparatus for Multifaceted Electroencephalographic Response Analysis (MERA), U.S. Patent #5,363,858.

[8] Farwell, L.A. (1995). Method and Apparatus for Truth Detection, U.S. Patent #5,406,956.

[9] Farwell, L.A. (1995). Method for Electroencephalographic Information Detection, U.S. Patent #5,467,777.

[10] Farwell, L.A. & Donchin, E. (1991). The truth will out: interrogative polygraphy ("lie detection") with event-related potentials, *Psychophysiology* **28**(5), 531–547. www.larryfarwell.com/pdf/Farwell-Donchin-1991-Psychophysiology-Brain-Fingerprinting-the-Truth-Will-Out-dr-larry-farwell-dr-lawrence-farwell.pdf.

[11] Farwell, L.A. & Smith, S.S. (2001). Using brain MERMER testing to detect concealed knowledge despite efforts to conceal, *Journal of Forensic Sciences* **46**(1), 135–143. www.larryfarwell.com/pdf/Farwell-Smith-Journal-of-Forensic-Sciences-Brain-Fingerprinting-P300-MERMER-dr-larry-farwell-dr-lawrence-farwell.pdf.

[12] Farwell, L.A. (2012). Brain fingerprinting: a comprehensive tutorial review of detection of concealed

information with event-related brain potentials, *Cognitive Neurodynamics* **6**, 115–154. www.larryfarwell.com/pdf/Dr-Lawrence-Farwell-Brain-Fingerprinting-P300-MERMER-Review-Cognitive-Neurodynamics-Dr-Larry-Farwell.pdf. DOI: 10.1007/s11571-012-9192-2

[13] Farwell, L.A., Richardson, D.C. & Richardson, G.M. (2013). Brain fingerprinting field studies comparing P300-MERMER and P300 brainwave responses in the detection of concealed information, *Cognitive Neurodynamics* **7**(4), 263–299. www.larryfarwell.com/pdf/Dr-Lawrence-Farwell-Brain-Fingerprinting-P300-MERMER-Review-Cognitive-Neurodynamics-Dr-Larry-Farwell.pdf, DOI: 10.1007/s11571-012-9230-0

[14] Farwell, L.A. & Richardson, D.C. (2013). Brain fingerprinting: let's focus on the science – a reply to Meijer, Ben-Shakhar, Verschuere, and Donchin. *Cognitive Neurodynamics* **7**(2), 159–166. 10.1007/s11571-012-9238-5. http://link.springer.com/article/10.1007%2Fs11571-012-9238-5.

[15] Farwell, L.A. (2013). Lie detection, in *Encyclopedia of Forensic Sciences*, 2nd Edition, Elsevier, Oxford. DOI: 10.1016/B978-0-12-382165-2.00025-8

[16] Farwell L.A. (2010). Method and Apparatus for Brain Fingerprinting, Measurement, Assessment and Analysis of Brain Function. U.S. Patent # 7,689,272.

[17] Farwell, L.A. & Donchin, E. (1988). Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials, *Electroencephalography and Clinical Neurophysiology* **70**, 510–523. http://www.larryfarwell.com/pdf/Farwell-Donchin-1988-Talking-Off-the-Top-of-Your-Head-BCI-brain-computer-interface.pdf.

[18] Donchin, E., Miller, G.A. & Farwell, L.A. (1986). The endogenous components of the event-related potential - a diagnostic tool?, in *Progress in Brain Research*, D.F. Swaab, E. Fliers, M. Mirmiran, W.A. Van Gool & F. Van Haaren, eds, Elsevier Vol. 70 *Aging of the Brain and Alzheimer's Disease*, Amsterdam, pp. 87–102.

[19] Bashore, T.R., Miller, G.A., Farwell, L.A. & Donchin, E. (1987). Research in Geriatric Psychophysiology in *Annual Review of Gerontology and Geriatrics*, Vol. 7, Springer, New York, 1–27.

[20] Donchin, E., Ritter, W. & McCallum, W.C. (1978). Cognitive psychophysiology: the endogenous components of the ERP, in *Brain Event-related Potentials in Man*, E. Callaway, P. Teuting & S. Koslow, eds, Academic Press, New York, pp. 349–441.

[21] Picton, T.W. (1988). *Handbook of Electroencephalography and Clinical Neurophysiology: Human Event-related Potentials*, Vol. 3, Elsevier, Amsterdam.

[22] Sutton, S., Braren, M., Zubin, J. & John, E.R. (1965). Evoked potential correlates of stimulus uncertainty, *Science* **150**, 1187–1188.

[23] Farwell, L.A. & Donchin, E. (1986). The "brain detector": P300 in the detection of deception, *Psychophysiology* **23**(4), 434 (abstract).

[24] Spencer, K.M., Dien, J. & Donchin, E. (2001). Spatiotemporal analysis of the late ERP responses to deviant stimuli, *Psychophysiology* **38**, 343–358.

[25] Soskins, M., Rosenfeld, J.P. & Niendam, T. (2001). The case for peak to peak measurement of P300 recorded at .3 Hz high pass filter settings in detection of deception, *International Journal of Psychophysiology* **40**, 173–180.

[26] Rosenfeld, J.P., Soskins, M., Bosh, G. & Ryan, A. (2004). Simple effective countermeasures to P300-based tests of detection of concealed information, *Psychophysiology* **41**(2), 205–219.

[27] Rapp, P.E., Albano, A.M., Schmah, T.I. & Farwell, L.A. (1993). Filtered noise can mimic low dimensional chaotic attractors, *Physical Review E* **47**(4), 2289–2297.

[28] Mertens, R. & Allen, J.J.B. (2008). The role of psychophysiology in forensic assessments: deception detection, ERPs, and virtual reality mock crime scenarios, *Psychophysiology* **45**(2), 286–298.

[29] Meijer, E.H., Ben-Shakhar, G., Verschuere, B. & Donchin, E. (2012). A comment on Farwell (2012): Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials, *Cognitive Neurodynamics* **7**(2), 155–158. DOI: 10.1007/ s11571-012-9217-x

[30] Farwell, L.A. (2011). Brain fingerprinting: corrections to Rosenfeld. *Scientific Review of Mental Health Practice*, **8**(2), 56–68. www.larryfarwell.com/pdf/Farwell-Brain-Fingerprinting-Corrections-to-Rosenfeld-Scientific-Review-of-Mental-Health-Practice-dr-larry-farwell-dr-lawrence-farwell.pdf.

[31] Farwell, L.A. (2011). Brain fingerprinting: comprehensive corrections to Rosenfeld in *Scientific Review of Mental Health Practice*. Seattle: Excalibur Scientific Press. www.larryfarwell.com/pdf/Scientific-Review-of-Mental-Health-Practice-Farwell-Brain-Fingerprinting-Comprehensive-Corrections-to-Rosenfeld-dr-larry-farwell-dr-lawrence-farwell.pdf.

[32] Wasserman, S. & Bockenholt, U. (1989). Bootstrapping: applications to psychophysiology, *Psychophysiology* **26**, 208–221.

[33] Farwell, L.A. & Donchin, E. (1988). Event-related brain potentials in interrogative polygraphy: analysis using bootstrapping, *Psychophysiology* **25**(4), 445 (abstract).

[34] Farwell, L.A., Martinerie, J.M., Bashore, T.R., Rapp, P.E. & Goddard, P.H. (1993). Optimal digital filters for long-latency components of the event-related brain potential, *Psychophysiology* **30**(3), 306–315.

[35] Farwell, L.A. & Makeig, T.H. (2005). Farwell brain fingerprinting in the case of Harrington v. State, *Open Court* **X** [**10**]:3, 7-10. Indiana State Bar Assoc. http://www.larryfarwell.com/pdf/OpenCourtFarwell Makeig-dr-larry-farwell-brain-fingerprinting-dr-lawrence-farwell.pdf.

[36] Farwell, L.A. (2013). Dr. Larry Farwell – Brain Fingerprinting. http://www.larryfarwell.com/.

[37] *Harrington v. State*, Case No. PCCV 073247 (Iowa District Court for Pottawattamie County, March 5, 2001).

[38] Roberts, A.J. (2006). Everything new is old again: brain fingerprinting and evidentiary analogy, *Yale Journal of Law and Technology* **9**, 234–270. http://yjolt.research.yale.edu/files/roberts-9-YJOLT-234.pdf/http://www.larryfarwell.com/pdf/roberts-9-YJOLT-234.

[39] Erickson, M.J. (2007). Daubert's bipolar treatment of scientific expert testimony – from Frye's polygraph to Farwell's brain fingerprinting, *Drake Law Review* **55**, 763–812.

[40] Moenssens, A.A. (2002). Brain fingerprinting – can it be used to detect the innocence of persons charged with a crime?, *UMKC Law Review* **70**, 891–920.

[41] Grier, J.B. (1971). Non-parametric indexes for sensitivity and bias: computing formulas, *Psychology Bulletin* **75**, 424–429.

[42] Farwell, L. A. (2012) Brain fingerprinting with pictorial stimuli: comparing P300 and P300-MERMER ERPs in the detection of concealed information. *Psychophysiology* **49**, S1, S114 (abstract).

[43] Farwell, LA, Richardson, D.C. (2006) Brain fingerprinting in field conditions. *Psychophysiology* **43**(s1), S38 (abstract).

[44] Farwell, L.A. (1992). Two new twists on the truth detector: brain-wave detection of occupational information, *Psychophysiology* **29**(s4A), S3(abstract).

[45] Allen, J., Iacono, W.G. & Danielson, K.D. (1992). The identification of concealed memories using the event-related potential and implicit behavioral measures: a methodology for prediction in the face of individual differences, *Psychophysiology* **29**, 504–522.

[46] Allen, J. & Iacono, W.G. (1997). A comparison of methods for the analysis of event-related potentials in deception detection, *Psychophysiology* **34**, 234–240.

[47] Rosenfeld, J.P., Shue, E. & Singer, E. (2007). Single versus multiple probe blocks of P300-based concealed information tests for autobiographical versus incidentally learned information, *Biological Psychology* **74**, 396–404.

[48] Rosenfeld, J.P., Labkovsky, E., Lui, M.A., Winograd, M., Vandenboom, C. & Chedid, K. (2008). The Complex Trial Protocol (CTP): a new, countermeasure-resistant, accurate P300-based method for detection of concealed information, *Psychophysiology* **45**, 906–919.

[49] Meixner, J.B., Haynes, A., Winograd, M.R., Brown, J. & Rosenfeld, P.J. (2009). Assigned versus random, countermeasure-like responses in the P300 based complex trial protocol for detection of deception: task demand effects, *Applied Psychophysiology and Biofeedback* **34**(3), 209–220.

[50] Rosenfeld, J.P., Tang, M., Meixner, J.B., Winograd, M. & Labkovsky, E. (2009). The effects of asymmetric vs. symmetric probability of targets following probe and irrelevant stimuli in the complex trial protocol for detection of concealed information with P300, *Physiology and Behavior* **98**(1–2), 10–16.

[51] Rosenfeld, J.P. & Labkovsky, E. (2010). New P300-based protocol to detect concealed information: resistance to mental countermeasures against only half the irrelevant stimuli and a possible ERP indicator of countermeasures, *Psychophysiology* **47**(6), 1002–1010.

[52] Mertens, R., Allen, J., Culp, N. & Crawford, L. (2003). The detection of deception using event-related potentials in a highly realistic mock crime scenario, *Psychophysiology* **40**, S60.

[53] Allen, J.J. & Mertens, R. (2009). Limitations to the detection of deception: true and false recollections are poorly distinguished using an event-related potential procedure, *Social Neuroscience* **4**(6), 473–90.

[54] Farwell LA (2007) Apparatus for a classification guilty knowledge test and integrated system for detection of deception and information. U.K. Patent # GB2421329.

[55] Rosenfeld, J.P., Nasman, V.T., Whalen, R., Cantwell, B. & Mazzeri, L. (1987). Late vertex positivity in event-related potentials as a guilty knowledge indicator: a new method of lie detection, *International Journal of Neuroscience* **34**, 125–129.

[56] Rosenfeld, J.P., Cantwell, G., Nasman, V.T., Wojdac, V., Ivanov, S. & Mazzeri, L. (1988). A modified, event-related potential-based guilty knowledge test, *International Journal of Neuroscience* **42**, 157–161.

[57] Rosenfeld, J.P., Angell, A., Johnson, M. & Qian, J. (1991). An ERP-based, control-question lie detector analog: algorithms for discriminating effects within individuals' average waveforms, *Psychophysiology* **28**, 319–335.

[58] Johnson, M.M. & Rosenfeld, J.P. (1992). Oddball-evoked P300-based method of deception detection in the laboratory II: utilization of non-selective activation of relevant knowledge, *International Journal of Psychophysiology* **12**(3), 289–306.

[59] Lui, M. & Rosenfeld, J.P. (2008). Detection of deception about multiple, concealed, mock crime items, based on a spatial-temporal analysis of ERP amplitude and scalp distribution, *Psychophysiology* **45**(5), 721–730.

[60] Miyake, Y., Mizutanti, M. & Yamahura, T. (1993). Event related potentials as an indicator of detecting information in field polygraph examinations, *Polygraph* **22**, 131–149.

[61] Verschuere, B., Rosenfeld, J.P., Winograd, M., Labkovksy, E. & Wiersema, J.R. (2009). The role of deception in P300 memory detection, *Legal and Criminal Psychology* **14**(2), 253–262.

[62] Kubo, K. & Nittono, H. (2009). The role of intention to conceal in the P300-based concealed information test, *Applied Psychophysiology and Biofeedback* **34**(3), 227–235.

[63] Meijer, E.H., Smulders, F.T.Y. & Wolf, A. (2009). The contribution of mere recognition to the P300 effect in a concealed information test, *Applied Psychophysiology and Biofeedback* **34**(3), 221–226.

[64] Meixner, J.B. & Rosenfeld, P.J. (2010). Countermeasure mechanisms in a P300-based concealed information test, *Psychophysiology* **47**(1), 57–65.

[65] Meixner, J.B. & Rosenfeld, P.J. (2011). A mock terrorism application of the P300-based concealed information test, *Psychophysiology* **48**(2), 149–154.

[66] Winograd, M.R. & Rosenfeld, P. (2011). Mock crime application of the Complex Trial Protocol (CTP) P300-based concealed information test, *Psychophysiology* **48**(2), 155–161.

[67] Rosenfeld, J.P., Biroschak, J.R. & Furedy, J.J. (2006). P-300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms, *International Journal of Psychophysiology* **60**(3), 251–259.

[68] Abootalebi, V., Moradi, M.H. & Khalilzadeh, M.A. (2006). A comparison of methods for ERP assessment in a P300-based GKT, *International Journal of Psychophysiology* **62**(2), 309–320.

[69] Hahm, J., Ji, H.K., Jeong, J.Y., Oh, D.H., Kim, S.H., Sim, K.B. & Lee, J.H. (2009). Detection of concealed information: combining a virtual mock crime with a P300-based Guilty Knowledge Test, *Cyberpsychology and Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* **12**(3), 269–275.

[70] Lefebvre, C.D., Marchand, Y., Smith, S.M. & Connolly, J.F. (2007). Determining eyewitness identification accuracy using event-related brain potentials (ERPs), *Psychophysiology* **44**(6), 894–904.

[71] Lefebvre, C.D., Marchand, Y., Smith, S.M. & Connolly, J.F. (2009). Use of event-related brain potentials (ERPs) to assess eyewitness accuracy and deception, *International Journal of Psychophysiology* **73**(3), 218–225.

[72] Gamer, M. & Berti, S. (2009). Task relevance and recognition of concealed information have different influences on electrodermal activity and event-related brain potentials, *Psychophysiology* **47**(2), 355–364.

[73] Meijer, E.H., Smulders, F.T.Y., Merckelbach, H.L.G.J. & Wolf, A.G. (2007). The P300 is sensitive to face recognition, *International Journal of Psychophysiology* **66**(3), 231–237.

[74] Neshige, R., Kuroda, Y., Kakigi, R., Fujiyama, F., Matoba, R., Yarita, M., Luders, H. & Shibasaki, H. (1991). Event-related brain potentials as indicators of visual recognition and detection of criminals by their use, *Forensic Science International* **51**(1), 95–103.

[75] Hira, S. & Furumitsu, I. (2002). Polygraphic examinations in Japan: applications of the guilty knowledge test in forensic investigations, *International Journal of Police Science and Management* **4**, 16–27.

[76] Miller, A.R. & Rosenfeld, J.P. (2004). Response-specific scalp distributions in deception detection and ERP correlates of psychopathic personality traits, *Journal of Psychophysiology* **18**, 13–26.

[77] Rosenfeld, J.P., Rao, A., Soskins, M. & Miller, A. (2003). Scaled P300 scalp distribution correlates of verbal deception in an autobiographical oddball paradigm: control for task demand, *Journal of Psychophysiology* **17**, 14–22.

[78] Ellwanger, J., Rosenfeld, J.P., Sweet, J.J. & Bhatt, M. (1996). Detecting simulated amnesia for autobiographical and recently learned information using the P300 event-related potential, *International Journal of Psychophysiology* **23**, 9–23.

[79] Rosenfeld, J.P., Ellwanger, J.W., Nolan, K., Wu, S. & Bermann, R. (1999). P300 scalp amplitude distribution as an index of deception in a simulated cognitive deficit model, *International Journal of Psychophysiology* **33**(1), 3–20.

[80] Ellwanger, J., Rosenfeld, J.P., Hannkin, L.B. & Sweet, J.J. (1999). P300 as an index of recognition in a standard and difficult match-to-sample test: a model of amnesia in normal adults, *The Clinical Neuropsychologist* **13**, 100–108.

[81] Rosenfeld, J.P., Sweet, J.J., Chuang, J., Ellwanger, J. & Song, L. (1996). Detection of simulated malingering using forced choice recognition enhanced with event-related potential recording, *The Clinical Neuropsychologist* **10**(2), 163–173.

[82] Rosenfeld, J.P., Reinhart, A.M., Bhatt, M., Ellwanger, J., Gora, K., Sekera, M. & Sweet, J. (1998). P300 correlates of simulated malingered amnesia in a matching-to-sample task: topographic analyses of deception versus truthtelling responses, *International Journal of Psychophysiology* **28**(3), 233–249.

[83] Rosenfeld, J.P. & Ellwanger, J.W. (1999). Cognitive psychophysiology in detection of malingered cognitive deficit, in *Forensic Neuropsychology: Fundamentals and Practice*, J.J. Sweet, ed, Swets and Zerlanger, Lisse, Netherlands.

[84] Sasaki, M., Hira, H. & Matsuda, T. (2002). Effects of a mental countermeasure on the physiological detection of deception using P3, *Studies in the Humanities and Sciences* **42**, 73–84.

Lawrence A. Farwell