10.6094/behemoth.2015.8.1.852

From Detection to Surveillance: U.S. Lie Detection Regimes from the Cold War to the War on Terror

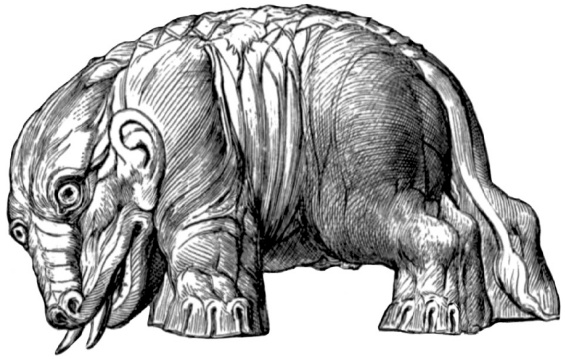
John Philipp Baesler

Abstract:

When the polygraph was developed in the early twentieth century, its creators promised a reliable security technology that would furnish mutual trust between individuals, in corporations, and between government and citizens. The history of the use of the lie detector, however, shows that it was not a reliable technology and often exacerbated distrust and conflicts due to the confrontational methodology and the unsubstantiated assumptions governing its use. This history shows that security concerns – namely, the need to uphold a posture of deterrence – and bureaucratic prerogatives of the Central Intelligence Agency made the polygraph nevertheless useful. However, a regime of security did not lead to conditions of trust. This insight is crucial for an understanding of early twenty-first century truth technologies based on surveillance that appears less intrusive than lie detection via the polygraph. Security technologies such as brain scanning or biometrics rely on similarly flawed assumptions about human physiology and the possibility of its representation through technology as well as ideological assumptions about the proper social relationships between individuals and between government and citizens, none of which tend to favor mutual trust.

Keywords: lie detector; trust; Central Intelligence Agency; national security

John Philipp Baesler is Associate Professor of History at Saginaw Valley State University. He studied modern and medieval history at the University of Heidelberg, the University of Kentucky, and Indiana University. He teaches the history of U.S. foreign relations at Saginaw Valley State University in Michigan. He has published in German and English, most recently: Die Macht des Lügendetektors im amerikanischen Sicherheitssystem. In: Greiner, B.; Müller, T.B.; Voss, K. (eds) Das Erbe des Kalten Krieges. Hamburg: Hamburger Edition, 2013: 128-137. He is currently working on a book manuscript on the history of the polygraph and the Cold War for the University of Georgia Press. **Email: jbaesler@svsu.edu**



From the trial of an alleged assassin in 1907 to the so-called War on Terror after the attacks of September 11 2001, lie detection technology has played a prominent role in U.S. national security procedures. At the beginning of the twentieth century, German psychologist Hugo Münsterberg attempted to prove with the help of scientific truth tests that the United Mine Workers had conspired to kill the governor of the state of Idaho (Lukas 1997). In the early twenty-first century, U.S. military and intelligence officials attempt to establish the bona fides of Iraqi citizens, Afghani warlords and American citizens who apply to work in the national security agencies with the help of lie detection technology (Pool 2010). Further, behavioral lie detection techniques are being developed and marketed to civilians for everyday use in the United States and elsewhere. Lastly, surveillance of individuals through cumulative analysis of behavioral data is quickly enveloping more and more aspects of everyday life. What will be the socio-political consequences of the new spread of lie detection? What does the history of the polygraph, the oldest and most common truth technology in use, suggest about projects to establish trust in modern society by means of allegedly objective security technology? Given that trust should be conceived as the end product of rules and conditions that establish reliability and security in social relations, it must be investigated whether the polygraph fulfilled its promise to forge mutual trust, rather than suspicion, within communities of security that relied on it (Hartmann 2014).

This paper will make the following arguments: First, despite hopes among scientists in the early twentieth century that a universal regime of lie detection would lead to more trusting social relations, the lie detector enhanced conflicts between notions of trust and security among citizens, among employers and employees, and in national security agencies in the United States during the Cold War and beyond. That is because the lie detector is not an objective scientific instrument, but rather an aid to interrogation. In its methodology, the polygraph is inherently confrontational and aims at deterring unwanted individuals from entering a community of trust, rather than establishing a general regime of trust. Indeed, trust still played a prominent role in security discourses, namely when it came to the broad outline of national security policies. The heads of government agencies such as the CIA or the State Department exempted themselves from mandatory lie detector exams and pleaded for the trust of skeptical citizens in the face of repeated scandals during the Cold War. Therefore, the lie detector did rely on trust, but only at the cost of establishing hierarchy.

Secondly, this paper will argue that more recent surveillance-based lie detection regimes such as

face reading, biometrics, and the collection of meta-data, are not likely to engender trust in social relations either. The *act of collecting* data through these technologies is far less intrusive than a polygraph interrogation. However, the new technologies reflect similar institutional goals as the lie detector: namely to make predictions about a person's future behavior based on a limited set of physiological and behavioral data. They are therefore just as likely to enhance distrust between citizens and government agencies or private corporations, due to the privilege that comes with interpreting these incomplete data.

Polygraph tests rely on procedures that suggest scientific methodology and predictable results. During a standard polygraph test, two soft rubber belts are strapped around a subject's stomach and chest, measuring the subject's breathing. Two wires are fastened on the ends of two of the subject's fingers, measuring sweating responses. Further, a blood pressure cuff is placed around the subject's upper arm measuring pulse and variations in blood pressure. All measurements are hooked to a modest-sized box sitting on a table between examiner and subject (since the 1980s the box has been replaced by computers). During a typical exam, between nine and fifteen questions are asked in intervals of about fifteen seconds, with all physiological responses that accompany "yes" or "no" answers being recorded on a continuous roll of paper. The test is usually repeated two or three times for control. It is preceded by a pre-test interview, during which the examiner discusses the procedure and the questions with the subject. It concludes with a post-test interview, which offers the subject the chance to clear up any issues with his or her chart (Lykken 1998).

A handful of interrogative methodologies have been in use, all of which aim first to evoke emotionally charged physiological responses from the subject, and second to distinguish responses originating from generic stress from those originating from a guilty conscience that arises from telling a lie. The most popular testing procedure for screening large pools of subjects, which is my focus here, is the "Control or Diagnostic Question" test, in which the subject's responses to irrelevant yet embarrassing questions likely to create emotional turmoil (for example, "have you ever lied during a job interview?") are compared to responses to relevant questions (for example, "do you plan to steal secrets from this organization?") (Lykken 1998).

The set up of the test therefore appears objective and orderly. However, the polygraph's interrogation methodology requires the test to be confrontational toward the subject, because only when a baseline of genuine emotional distress is created through these control questions does the test

"work," even according to its supporters. In short, if the interrogation is not upsetting to the subject, it is ineffective. Further, the polygraph test is not a precise scientific procedure because there is no identifiable physiological lie response. Test results therefore have a considerable error rate, either in form of false positives when an innocent person is accused of deception, or false negatives when a lie goes undetected. Since the interrogator must always infer deception from ambiguous physical data, the technology does not produce self-explanatory results. In 2003, a comprehensive study by the U.S. National Research Council on the validity of the lie detector found the instrument of ambiguous use for specific investigations but especially problematic for use in mass screenings, for example as a precondition for employment in the Central Intelligence Agency: "[The polygraph's] accuracy in distinguishing actual or potential security violators from innocent test takers is insufficient to justify reliance on its use in employee security screening in federal agencies." (National Research Council 2003, 6) Instead, the polygraph became useful mostly as a means of preclusion and discouragement: Even if not scientifically solid, the lie detector was seen as a deterrent to enemies or unsuitable individuals, therefore resembling the principle of Cold War geopolitics after 1945, which throughout most of the conflict was based on deterrence through spectacular performances of technological prowess rather than building trust between the opponents (Alder 2007b).

Given the technocratic enthusiasm often displayed by advocates of surveillance technologies today, it is important to recall that already in the early twentieth century, the creators of lie detection promised its social utility to establish trust in modern mass society. After German psychologist Hugo Münsterberg came to Harvard in the 1890s, the practical research in developing lie detection technologies took place in the United States (Bunn, 2011). A convinced advocate of psychology as a discipline with social usefulness, Münsterberg wrote countless books and articles in popular magazines spouting the promise of technology to detect deception and its potential for law enforcement, promising to do away with unreliable witness testimony and forced confessions. After Münsterberg's death in 1916, his flamboyant student William M. Marston developed blood pressure as the most relevant indicator of deception. Marston lobbied for the lie detector as a tool of popular psychology by offering it as a remedy for the emotional distress accompanying dishonesty and playing on fantasies of a utopian society free of deception. Marston spread his liberationist agenda in magazines like *Cosmopolitan, Good Housekeeping*, or *Ladies' Home Journal*. He gave radio talks advocating the use of the lie detector in private relations, for example to solve marital problems by revealing

unresolved conflicts between spouses (Bunn 1997; Littlefield 2011). He called the lie detector "psychological medicine, if you like, which will cure crime itself when properly administered." (Marston 1938, 15) Periodic testing would establish genuine trust in the workplace as well, Marston believed: "But after all have been tested a new spirit of mutual trust and confidence always prevails [...] It is inevitable that sooner or later the Lie Detector will bring about this condition of mutual trust in all large business and financial organizations." (112) Most famously Marston developed the comic book character *Wonder Woman* in the early 1940s, swinging a lasso compelling everyone caught to tell the truth. Freedom through submission to loving authority was a major theme of *Wonder Woman's* adventures. Through this character Marston promoted non-coercive emotional and social discipline through self-knowledge, based on a commitment to unreserved honesty (Lepore 2014).

Because it was seen as cost-effective, non-coercive, as well as imbued with the authority of science, advocates of technological lie detection saw the polygraph as a quintessentially progressive machine. August Vollmer, the widely respected leader of progressive police professionalization and long-time chief of police in Berkeley, California, utilized the polygraph from 1921 on in his effort to establish a reliable police force untainted by corruption (Alder 2007). Following the Berkeley police department with its two lie detector researchers John Larson and Leonarde Keeler, many cities throughout the 1930s instituted lie detector tests together with entrance examinations for police officers, IQ tests as an aid to decide promotions, and new scientific police units such as forensic science units.

However, the stated goals of lie detection as a trust-builder, either between individuals, in the workplace, or between law enforcement and citizens, were based on unquestioned assumptions about the predictive value of the technology. When science failed to deliver this authority, the coercive aspects of the test became increasingly prominent. Authority for the test was therefore created in other ways. In his 1930 article, "A Method for Detecting Deception," Leonarde Keeler suggested that each test should be initiated by a preamble read to the subject. The preamble read that the machine "so far has proved a very reliable means of detecting the innocence or guilt of man, and I'm sure we will not fail in your case." Keeler then noted that "75% of the guilty suspects confess" without the necessity for analyzing the physiological measures (Keeler 1930, 48). As Keeler's own 1939 survey of thirteen police polygraph units revealed, a stunning 60% of suspects judged deceptive after having been given the test subsequently confessed to some crime (Alder 2002, 14-17). Therefore, despite being barred from the courts and the skepticism of academic psychologists, the polygraph

chart established its usefulness as a tool to *extract confessions after being read*, rather than acting as a witness itself. Getting results with the lie detector now meant getting confessions, and the lie detector test became a heavy-handed exercise of power, not a friendly scientific aid. Instead of fulfilling its early utopian promise of enlightened psychological guidance and fair-minded progressive administration of justice, the lie detector by 1945 had become a widely used yet controversial technology. If nothing else, lie detector tests could pressure subjects to confess to something.

The use of the polygraph by the U.S. federal government since the 1940s also underlines the confrontational effects of the technology. William Moulton Marston first attempted to make the lie detector useful for national security purposes during World War I, when Harvard psychologist Robert Yerkes – the driving force behind the development of the IQ test in the United States in 1917-1918 – allowed Marston to conduct experiments with recruits at Fort Greenleaf in Georgia. (Alder 2007a, 50ff.) At the time Marston advertised the procedure as a promising way to flush out "slackers" – draft dodgers – and German spies, but the war ended before he found an opportunity to do so. Between the wars, the lie detector became widespread in American policing, but during and especially after World War II it entered national security procedures as a way to protect against communist subversion from within and without.

In his 1947 address known as the Truman Doctrine, president Harry Truman famously divided the world into the U.S.-led "free world" and the Soviet-led "slave world" and therefore employed the rhetoric of a strict ideological binary to explain the geo-strategic conflict between the United States and the Soviet Union (Fousek 2000). As part of this trope of an ideological binary, Americans came to understand the Cold War also as a conflict between American idealism and Soviet utilitarianism, between western sincerity and eastern duplicity. As for example diplomat George Kennan wrote, "the very disrespect of Russians for objective truth – indeed, their disbelief in its existence – leads them to view all stated facts as instruments for furtherance of one ulterior purpose or another." (Kennan 1967, 555) Catching liars therefore became an issue of national security. However, given that the Cold War clash between the United States and the Soviet Union was about ideologies and interests, the term "national security" came to include more than simple issues of protecting the border against invasion or espionage. Put differently, national security always had a physical and a psychological connotation. As Melvyn Leffler succinctly states, "The national security approach demands that as much attention be focused on how the American government determines its core

values as on how it perceives external dangers. Core values are the objectives that merge ideological precepts and cultural symbols like democracy, self-determination, and race consciousness with concrete interests like access to markets and raw materials and the defense of territory." (Leffler 2004, 126)

However, the relation between truthfulness and "national security" was put in very different terms in the secret 1954 "Doolittle Report" on CIA activities prepared on request for president Eisenhower. To fulfill its mission, the CIA had to accept that in the Cold War "[h]itherto acceptable norms of human conduct do not apply. [...] Long-standing American concepts of 'fair play' must be reconsidered. We must develop an aggressive covert psychological, political and paramilitary organization more effective, more unique and, if necessary, more ruthless than that employed by the enemy. No one should be permitted to stand in the way of the prompt, efficient and secure accomplishment of this mission." (Doolittle 1954, 2f.) The lie detector was meant to solve the dilemma of U.S. national security policy, which meant to preserve core values through policies that potentially violated those values. The polygraph promised hard truth delivered objectively and with precision and can therefore be interpreted as a technology meant to square the circle of containment as a policy meant to protect freedom by coercive means.

U.S. possession of nuclear weapons and the threat of Soviet espionage made use of lie detectors part of a new risk assessment that favored a "better save than sorry" attitude. The leaders of the Manhattan District facility in Oak Ridge used the polygraph on selected personnel at Oak Ridge in early 1946. Eleven examiners would periodically test over 50,000 workers. Only when nuclear scientists began taking employment in less restrictive private settings did the AEC abandon the tests in 1953 (Alder 2007a, 204ff). Nevertheless, atomic energy and nuclear weapons continued to be a major impetus to create a new regime of security measures by the federal government that now had found a place for the lie detector.

The Central Intelligence Agency was one of the heaviest users of the lie detector, partly because its core mission was to identify treason and espionage, but also because as a new bureaucracy it had to establish its reputation and place in the pecking order of the American national security state. Its Office of Security was responsible both for "approv[ing] or disapprov[ing], from a security standpoint, the employment or utilization of individuals by the Agency" (with the exception of covert personnel abroad) and "develop[ing] and conduct[ing] counterintelligence programs for the Agency

security procedures." (Central Intelligence Agency 1957, 1, 21) In CIA these two functions merged into one: Each employee was treated as a potential "mole." Security procedures, including lie detector tests, therefore served a double function: they had to be thorough enough to catch potential spies, and "routine" enough to handle everyone else. In this context, institutional pressure on the polygraph test to identify sufficient numbers of liars grew.

After J. Edgar Hoover in early 1948 ordered the FBI to abandon security screenings on behalf of its new bureaucratic competitor CIA, the U.S. Army recommended it to the agency (Jeffreys-Jones 2007, 141ff.). Polygraph exams became part of clearance procedures for Special Intelligence beginning in 1948, and then, according to Director of Security Sheffield Edwards, spread to "routine screening of employees prior to departure for overseas assignments, as well as employees returning from extended periods of overseas duty. In the fall of 1951, a procedure was initiated whereby all applicants, as a part of their entry on duty processing, were given polygraph examinations on a voluntary basis. This program has continued without interruption. [...] Considering the results of the polygraph program and its benefits from a security standpoint, I am convinced that its use since 1948 has immeasurably increased the security of this Agency." (Edwards 1953)

The agency subsequently developed a carefully managed lie detector program, which included a short consent form to establish voluntarism as a key to the practice. By 1970, the CIA had developed its philosophy for the polygraph, which was encoded in the definition of its purpose by Director Richard Helms in a memorandum:

> "The polygraph will be used in the Central Intelligence Agency as an aid to investigation for determining the security eligibility of persons for employment by or assignment to the Agency; security clearance by the Agency; staff-like access to sensitive Agency installations; utilization in operational situations; or continued access to classified information where implications of a security nature or investigative information require clarifying security interviews." (Helms 1970)

The agency valued the technology enough that when challenged by Congress it would defend the polygraph aggressively.

By the 1970s, the blunt anti-communism of the early Cold War had lost much of its appeal. However, the responsibility to protect intelligence "sources and methods" according to Section 102 (d) (3) of the National Security Act provided a strong legal and institutional argument for continued

polygraph use. In a 1975 letter to Congresswoman Bella Abzug, who at the time was Chair of the House Subcommittee on Government Information and Individual Rights, DCI George Bush charged that a complete prohibition of polygraph use in the federal government would "seriously impair" him "from complying with his statutory responsibility under the National Security Act." Bush justified the polygraph not only because it uncovered security-relevant information and had "proven reliability," but also because it was "a useful and comforting confirmation of other screening procedures." (Bush 1976) This was, of course, circular logic: If the lie detector found something other screening procedures had missed, it proved an essential additional tool of security. However, if it found nothing, it was a welcome affirmation of the reliability of the rest of the security program. Either way, the polygraph was central to the CIA's mission to protect sources and methods of intelligence.

By the early 1980s, experience was one of the strongest arguments for the polygraph. In 1980, the DCI's Security Committee stated, "the utility of the polygraph interview as part of security processing has been demonstrated by empirical means. [...] These practical results, plus more than thirty years experience, make the use of the polygraph in security screening truly unique and indispensable. Indeed, the available evidence shows conclusively that the most revealing source of adverse information is a polygraph examination. [...] Favorable polygraph test results afford an important extra measure of security assurance." (Central Intelligence Agency 1980)

Official documents do not reveal the power the polygraph amassed. As polygraph examiner John Sullivan points out in his memoirs, failure to submit to the test or a "failed" test meant no employment with CIA. While the CIA's screening process includes a background investigation, a medical exam, psychological tests, and personal interviews,

> "[...] a polygraph subject's admission of serious wrongdoing has more impact on a decision to disapprove an applicant than all other parts of the process combined. When a polygraph subject admits ongoing felonious activity, recent use of illegal drugs, or other disqualifying information, an adjudicator's decision is objective and easy to defend. All other parts of the clearance/adjudication process [...] are much more open to interpretation and challenge. [...] In trying to recall instances in which applicants who passed their polygraph tests were subsequently denied employment, I can only recall two." (Sullivan 2007, 5)

The lie detector did not catch one major spy during the Cold War yet was considered by CIA leadership as an irreplaceable part of "national security." Instead, it did people in for minor transgressions, but especially homosexuality. Confusion over the benefits of lie detector tests was entangled with confusion over the purpose of security procedures in general. An internal history of 1973 admitted that despite considerable experience with security procedures, "the precise yardstick for the measuring of security reliability of an individual continued to be elusive." (Central Intelligence Agency 1973, 31f.) In a 1974 analysis, the Interrogation Research Branch concluded that, "analysis fails to justify use of the polygraph in terms of uncovering penetration attempts or developing serious security information. Not one of the [redacted] repolygraph cases surfaced as a counterintelligence case or case with CI overtones." Instead, the report fell back on "intangible advantages" of the polygraph as deterrence of wrongdoing or infiltration, or "peace of mind available to employees who recognize that their peers have also gone through and face again the possibility of polygraph." (Central Intelligence Agency 1974)

The intangible benefits of the lie detector as a deterrent and tool to extract confessions withstood repeated political attacks by privacy advocates. Congress specified regulations for use of lie detectors in the federal government after an investigation in 1964, came close to outlawing the practice in 1976, and finally passed the Polygraph Protection Act of 1988, which banned the practice for commercial purposes but left a loophole for security-related use. This act therefore cemented "national security" not as the foundation to create trust in social relations, but rather as a separate sphere of governmental authority in which separate rules of security applied. After the attacks of September 11 2001, lie detector use has increased in national-security agencies. For example the FBI since 2002 demands random lie detector exams (Federal Bureau of Investigation 2002). The boundary between the sphere of "national security" and the rest of social relations in the United States therefore proved to be permeable.

The polygraph caused conflict between branches of government and between citizens and that government. For once, the polygraph implemented U.S. national security policy, but those policies themselves remained a matter of trust in leadership. Once "security reliability" was defined, the Lie Detector could be used for interrogation, but what exactly are the personal features of an individual that makes him or her loyal and reliable? And would an honest person not be a lot more nervous during the procedure than an experienced liar? In short, employment of supposedly objective scientific/

technological measures such as the polygraph tends to protect U.S. government agencies from challenges from bureaucratic competitors and congressional attempts at oversight (Porter 1995). But the history of lie detectors does not suggest them as an objective, neutral way to define the meaning of national security, not only because of the unreliable methodology of the test, but also because there is no objective, neutral way to define an ideologically-charged term such as "national security."

Another trust-related issue is the secrecy surrounding national security agencies. In the wake of the numerous scandals involving the CIA, its leaders always appealed to the trust that average citizens should have in the patriotism of the leadership of the intelligence services. For example, in 1971, shortly before the Watergate scandal led to revelations about a number of U.S. covert activities, CIA director Richard Helms famously called himself and his colleagues "honorable men" whose devotion to protecting American democracy had to be taken on faith. (Helms 1971, 25) The implication here was clearly that citizens could trust in the patriotism of their clandestine services. In 1983, when the Reagan administration initiated stricter polygraph rules against leakers of government secrets, Secretary of State George Shultz was quoted in the press as responding to the question whether he would ever submit to a polygraph test, "[t]he minute, in this government, I am told that I'm not trusted is the day that I leave." (Oberdorfer 1988) He was quickly assured that high-ranking officials would, of course, never be asked to submit to the test. Lowly applicants for federal employment, on the other hand, often did not have the luxury of declining an otherwise appealing job.

The idea that policy makers could be held responsible for public statements through polygraph tests seems unthinkable. This illustrates the hierarchical power of the procedure. However, it bears emphasizing that some scientists envisioned lie detector tests for world leaders to prevent nuclear catastrophe and initiate nuclear disarmament during the Cold War. In 1961, at the height of global anxiety over the possibility of nuclear war, University of Michigan neurophysiologist Ralph Gerard proposed an idea to break the deadlock in disarmament negotiations using the insights of the behavioral science. Maybe the vicious cycle of mutual distrust and rapidly evolving nuclear capabilities could be broken if world leaders could be made to rely on each other's truthfulness. Gerard thus made the following proposal:

> "The argument is simple: given matched power [...] opposing nations will resort to actual warfare overwhelmingly as a result of mistrust of the other or of misunderstanding resulting from false information – either suspected or actual. My solution is to insure

> that public or other official statements made by key figures are indeed true. This can be done with available lie detection techniques if national leaders will submit to them. [...] The proposal is simply this: all key men, speaking officially for their country in private negotiations or public addresses, subject themselves to lie, or better, truth detection procedures administered by technicians from an opposing country or from the UN. More positively, when a statesman wished to convince the world that he was making a true statement he would subject himself to truth detection." (Gerard 1961, 212, 216)

Based on such unassailable implementation of the polygraph, world leaders would soon learn to trust each other: "Since each antagonist would be able to tell very soon when his own lies were caught, he would soon develop confidence in the technique that revealed them. With growing conviction that false statements would be caught up, spokesmen would tell the truth publicly and their hearers would come to have some trust in the truth of these statements." (Gerard 1961, 216) The confrontational, scientifically uncertain nature of the polygraph made this rather utopian proposal unlikely to succeed. Further, since President Truman killed off the Acheson-Lilienthal Plan in 1946, the United States government had never seriously considered sharing nuclear technology with the Soviet Union. Joseph Stalin, on the other hand, found the prospect of permanent military inferiority vis-à-vis the United States unacceptable (Craig/Radchenko 2008). Gerard's proposal also risked becoming paradoxical: Would such an agreement on a lie detection protocol not already assume the kind of trust that lie detectors were supposed to establish in the first place? Once one could retrieve truth, why limit it to arms control? The more weight one would give the lie detectors, the more trust both sides would have to invest in the procedures of its application. Lastly, it should be noted that in international relations, leaders probably assume an opponent's truthfulness much less than we do in daily social interactions or in domestic politics. The role of lies in international politics has not been thoroughly researched, but political scientist John Mearsheimer argues that outright lies are rare in diplomacy due to the fact that in high-stakes matters trust among nations is already low. It seems that political leaders mostly lie to their own populations, who are more inclined to trust them (Mearsheimer 2011).

In the early twenty-first century, new versions of the polygraph continue to appear periodically. In 2008, the U.S. military introduced a hand-held lie detector, the so-called Preliminary Credibility Assessment Screening System. It was introduced for use in Afghanistan and Iraq as well as in

counter-narcotics operations in Colombia without prior testing in field studies (Pool 2010). However, the polygraph is currently being supplemented by new technologies of truth, most prominently technologies that promise visual access to the human brain, most prominently in the form of brain "imaging" or "scanning." As literary scholar Melissa Littlefield has pointed out, these new "mind reading" machines continue to make promises, and base their findings, on assumptions about the nature of mind and body that they directly inherited from the polygraph. As the polygraph did in the mid-twentieth century, "Brain Fingerprinting" or its current competitor, functional magnetic resonance imaging (fMRI), promise that *finally* a scientifically sound way to identify liars has been discovered. Both methodologies utilize a questioning technique directly drawn from the Guilty Knowledge Test developed by David Lykken for the polygraph. The fMRI and Brain Fingerprinting also assume that lies can be localized in the body, only now through sequences of three-dimensional images of the brain, which means that the measurement takes place directly at the central, not the peripheral, nervous system. In this endeavor, Littlefield shows, the new techniques continue to encounter the same methodological problems the polygraph did: first, intentionality cannot be localized through a specific physical manifestation because of the logical problem that one cannot unambiguously infer a cause from its consequence and because deception is not a physical phenomenon but a discursive construct the content of which depends on the experimental design one chooses. Second, all bodily activity takes place within an organism, where all activity occurs in an interdependent system that needs to be evaluated as a whole. In addition, truth technology makes a fundamental supposition about lying as an activity of the brain. All such technologies therefore presume that truthfulness results in lack of activity. This presumption has not been proven and could easily be challenged on evolutionary grounds. Lastly, image-based lie detection is open to the same potential countermeasures as the polygraph (Littlefield 2011).

It might very well be its aesthetic fit with the authority of photographic realism, that is: a widespread belief in the early twenty-first century that images contain a special authority due to their allegedly unconstructed and self-evident nature, that makes lie detection through brain-imaging so attractive (Paul/Egbert, 2014). Yet it needs to be emphasized that the hyperrealism of the brain scan hides its constructed nature. *All* lie detection technologies are based on highly problematic methodological assumptions that are disguised through representational compression into a simple curve or a colorful image.

The larger governmental project of gaining access to the thoughts and intentions of citizens through traces of bodily activity continues as well, in the United States and elsewhere. Governmental power appears to be less centralized in comparison to the twentieth century, with Big Business as an equal partner to Big Government. Less visibly, observers such as political theorist Sheldon Wolin see a gradual shift toward "inverted" totalitarian government that is creeping up on citizens through the guise of benevolent empire rather than overt counter-revolutionary activity. In an echo of C. Wright Mills's demand that the intellectual class should devote itself to truth rather than power, Wolin insists that democracy requires truth-telling and that "inverted totalitarianism" is based on secrecy and propaganda (Mills 2008; Wolin 2008). Here the contrast of new surveillance technology to the polygraph is most startling. Rather than confronting individuals in a heighted state of alert during a test that requires definite "yes" or "no" answers, technologies such as data mining of online activity or tracking of cell phone use simply follow individuals in their private and professional consumption of technology. By intimately connecting technology with our own sense of self, we assume that smart phones and other devices simply become extensions of ourselves rather than tools that can be used for different purposes. As writer Charles Howarth puts it,

> "[…] we now view technology not just as empowering but as self-actualizing as well. Because it's positioned as key to our authentic selves, we are newly intimate with it. This sounds utopian. It seems as if technology is finally reaching its potential: It is no longer the threat to human freedom, but its driving force. […] The result is that we become blind to technology's dark side – its potential to be misused in ways that encroach on our privacy. How can we see the privacy implications of our smartphones when we see them first as the key to the authentic self, or the Google Car when it looks so cute, or Google Glass when we believe that it will allow us to transcend our bodies to allow a new mastery of the world." (Howarth 2014)

Yet surveillance technologies do have governmental agendas, the purposes for which they were created. From a Foucaultian perspective surveillance technologies are more than a reflection of economics or ideology. Rather, performative technologies shape the subjective experience of individuals and make them productive. As Peter Miller and Nikolas Rose argue, the dominant aspect of western liberalism since the 1970s has been the ideal of the self-governing individual who pursues his/her authentic self and therefore must be made self-governing through risk management,

audits, budgeting and other governmental techniques. In this sense, government in the early twenty-first century centers on a particular notion of freedom, namely "a type of regulated freedom that encourage[s] or require[s] individuals to compare what they did, what they achieved, and what they were with what they could or should be." (Miller/Rose 2009, 9) Such a notion of freedom is based on the assumption of competition among individuals as the constitutive principle of society (Dardot/Laval 2014). In this sense, governmental power animates individuals to "freely" explore their true selves and does not inflict direct violence on individuals unless they become targets of investigation. Linked technologies such as databases of biometric data, therefore, grant individuals the subjective experience of freedom through effortless travel or enjoyment of social benefits. Yet it is wise to consider, as David Lyon does, that identification based on such technological forms of surveillance can be used to limit individual freedom as well. After all, slaves were the first individuals in the United States whom the government attempted to authenticate through ID (Parenti 2004) .Therefore, creating categories for inclusion and exclusion, rather than trust, should be seen as among the goals pursued through ID technologies based on surveillance.

Further, identification through methods such as iris scans, electronic fingerprints, voice pattern analysis etc. separates physiological information from the body and is based on parameters that are chosen, just as with the polygraph, with an eye toward sensitivity and specificity, that is: the ability to correctly identify culprits and innocents. As with the lie detector, choice of parameters can lead to mis-identification. Government by identification through disembodied aggregates of data is therefore based on constant surveillance, assessment, and classification of bodies, all of which include possibilities for error and open avenues of punishment if the citizen refuses cooperation or deviates from a certain governmental ideal (Lyon 2009).

The analysis of facial expression is also part of the larger project of defining parameters of normal vs. abnormal bodies. In this case, it is the body in its expression of affect, as when psychologist Paul Ekman's Automated Facial Expression Analysis is being used to develop face reading software for uses in human-computer interaction, psychological therapy, but also forensic investigations (Gates 2011). Ekman researches non-verbal communication of emotions. He argues that expression of emotions is determined by evolution and therefore universal among humans. His book *Telling Lie*s and his cooperation with the U.S. TV series *Lie To Me* made Ekman the most prominent proponent of using facial expressions (especially easily-missed micro-expressions such as pursing of the lips)

to identify emotions, but also intent to deceive (Weinberger 2011). Ekman's ongoing project is to create a comprehensive map of emotions as expressed by the human face through his Facial Action Coding System. Ekman's work in combining analysis of facial expression with other nonverbal clues has been incorporated by the Transportation Security Administration (TSA) into their Screening Passengers by Observation Technique (SPOT), which began in 2006 and has been criticized – ironically also by proponents of the polygraph such as David Raskin, a retired professor of psychology at the University of Utah – for being unconfirmed by peer-reviewed research and untested in the field (Weinberger 2011). Lie detection techniques based on nonverbal clues and other behavioral science techniques are increasingly marketed as how-to guides for the average citizen or business owner. Former CIA or FBI officers often write these guides (Meyer 2012; Houston/Floyd et al 2012; Navarro/Sciarra Poynter 2014).

The value of imbuing everyday life with intelligence techniques remains questionable and may be seen as part of the larger culture of security that developed in the wake of the 9/11 attacks. We are increasingly asked not to look away when our fellow citizens involuntarily reveal private information about themselves. Such inquisitiveness violates what sociologist Erwing Goffman defined as the essence of civilized behavior (Goffman 1959). Surveillance society therefore combines the demands of loyalty and trust associated with smaller communities with the power of the state that rules modern society. As such it threatens the artifice of social form that protects individuals from ridicule and allows them to interact in a rule-based public sphere (Plessner 1999). While the U.S. government and U.S. technology firms have been at the forefront of developing surveillance technologies, books directed at a general audience encourage citizens to apply surveillance techniques on each by studying the other person's body language and/or facial expressions in Germany as well (Nasher 2012; Standop 2014). Identifying the historical origin of such techniques in the intelligence world allows us to track the transmission of surveillance from specific "national security" functions into society as a whole. What kind of society we create when we hover like drones over our fellow citizens as if they were enemies remains to be seen (Rafael 2013).

The project of finding ways to identify citizens and making them "legible" (in James Scott's phrase) can be traced at least back to the beginning of the modern nation state and high imperialism in the 19th century (Scott 1999). In the early 21st century it seems that U.S. national security agencies take an "all of the above" approach, meaning that the polygraph at the moment is not being superseded,

but rather complemented, by newer technologies of lie detection and identification, both of which aim at predicting future behavior on the basis of selected physiological data and assumptions about the predictability of human behavior. However, there is a perceptible shift in truth technologies from detection to surveillance underway. This shift suggests at least three consequences for the role of trust in societies under surveillance: First, surveillance technology is becoming universal. While the polygraph is a truth technology largely confined to the United States and its intelligence agencies, biometric passports and metadata are being shared across borders and between private entities and governments. As a result, societies under surveillance are becoming increasingly global and interconnected. Second, societies under surveillance will not confine the testing of individual truthfulness to occasional testing situations such as a polygraph exam; rather, an increasing amount of routine interactions between individuals and testing institutions will include such tests as part of the process of granting access to privileges such as free travel or use of credit cards. As a result, truth technologies will not serve as a gateway into a community of trust, but will rather create concentric circles of access to privileges, each dependent on a different technological entry ticket with an expiration date. That is because, third, since technologies of surveillance require constant updating and upgrading, trust will never be final and unreserved but rather temporary and conditional. Especially surveillance based on metadata is based on a constant yet inherently incomplete flux of data. While the logic of the lie detector requires a definite judgment (deception indicated/no deception indicated) based on a limited set of data, surveillance will require just-in-time collection and interpretation of limitless data. As a consequence, clearance will always be conditional in such a global surveillance society. Likely all individuals will experience the limits of trust extended to them when access to a circle of access is denied to them at some point. In surveillance societies, then, there might be a tendency to interpret simple compliance – playing along with the rules set by testing institutions – as genuine honesty and trust. Security as a value will therefore not necessarily function as a foundation for trusting social relations. Ignoring this shortcoming is a serious danger inherent in technocratic solutions to problems of trust among individuals in society.

References

Alder, K. (2007a) *The Lie Detectors: The History of an American Obsession*. New York: Free Press.

Alder, K. (2007b) America's Two Gadgets: Of Bombs and Polygraphs. In: *Isis* 98(1): 124-137.

Alder, K. (2002) A Social History of Untruth: Lie Detection and Trust in Twentieth-Century America. In: *Representations* 80(3): 1-33.

Bunn, G.C. (2011) *The Truth Machine: A Social History of the Lie Detector*. Baltimore: Johns Hopkins University Press.

Bunn, G.C. (1997) The Lie Detector, Wonder Woman, and Liberty: The Life and Work of William Moulton Marston. In: *History of the Human Sciences* 10 (1): 91-119.

George H. W. Bush [Director of Central Intelligence] to Bella Abzug, Feb. 25, 1976, CREST.

Central Intelligence Agency, "Office of Security: Statement of Mission and Functions," Sept. 2, 1957, p. 1, 21, CIA Records Search Tool (CREST), National Archives and Records Administrations (NARA), College Park, Md.

[Redacted], *Security Program of the Central Intelligence Agency 1941-1968: Vol. II, Personnel Security*, May 1973, 31-32, CREST.

Central Intelligence Agency, [Redacted], [Chief, Interrogation Branch], "Memorandum for Director of Security, Subject: Role of Polygraph in the Reinvestigation Program," April 12, 1974, CREST

Central Intelligence Agency, [Redacted], [Executive Secretary, Security Committee], "Response to Certain Recommendations Made in a House Subcommittee Staff Report Entitled 'Security Clearance Procedures in the Intelligence Agencies,'" Jan. 16, 1980, p. 4, CREST.

Craig, C.; Radchenko, S. (2008) *The Atomic Bomb and the Origins of the Cold War*. New Haven: Yale University Press.

Dardot, P.; Laval, C. (2014) *The New Way of the World: On Neoliberal Society*. New York: Verso.

Doolittle, J. "Report on the Covert Activities of the Central Intelligence Agency," submitted 30 Sept. 1954, 2–3. CIA Electronic Research Tool (CREST), National Archives and Records Administration (NARA), College Park, Md.

Sheffield Edwards [Director of Security], "Memorandum for Director of Central Intelligence," April 13, 1953, CREST.

Federal Bureau of Investigation (2002) *The Personnel Security Polygraph Program*. Washington: Govern-

ment Printing Press.

Fousek, J. (2000) *To Lead the Free World: American Nationalism and the Cultural Roots of the Cold War*. Chapel Hill: University of North Carolina Press.

Gates, K.A. (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press.

Gerard, R.W. (1961) To Prevent Another World War: Truth Detection. In: *Journal of Conflict Resolution* 5(2): 212-218.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Edinburgh: The University of Edinburgh Social Sciences Research Centre.

Hale, M. Jr. (1980) *Human Science and Social Order: Hugo Munsterberg and the Origins of Applied Psychology*. Philadelphia: Temple University Press.

Hartmann, M: Basic Trust, Security, and Terror: Questioning the Paradigm. Presented June 5 2014 at Conference Trust in Times of (In-)Security: Trier.

Helms, R. [Director of Central Intelligence], "Memorandum for Director of Security, Subject: Polygraph Program," Feb. 21, 1970, CREST.

Helms, R. "Global Intelligence and the Democratic Society," speech to the American Society of Newspaper Editors, 14 April 1971, p. 25, DCI Files, Job 80R01284R, box 1, folder 6.

Howarth, C. (2014) Technology Is Making Us Blind: The Dangerous Complacency of the iPhone Era. In: *Salon*. http://www.salon.com/2014/11/29/technology_is_making_us_blind_the_dangerous_complacency_of_the_iphone_era/ (29/11/2014).

Houston, P.; Floyd, M.; Carnicero, S.;Tennant, D. (2012) *Spy the Lie: Former CIA Officers Teach You How to Detect Deception*. New York: St. Martin's.

Jeffreys-Jones, R. (2007) *The FBI: A History*. New Haven: Yale University Press.

Keeler, L. (1930) A Method for Detecting Deception. In: *American Journal of Police Science* 1(1): 38-52.

Kennan, G.F. (1967) *Memoirs: 1925–1950*. Boston: Little, Brown.

Leffler, M.P. (2004) National Security. In: Hogan, M.J.; Paterson, T.G. (eds) *Explaining the History of American Foreign Relations*. New York: Cambridge University Press.

Lepore, J. (2014) *The Secret History of Wonder Woman*. New York: Knopf.

Littlefield, M. M. (2011) *The Lying Brain: Lie Detection in Science and Science Fiction*. Ann Arbor: University of Michigan Press.

Lukas, J.A. (1997) *Big Trouble: A Murder in a Small Western Town Sets Off a Struggle for the Soul of America*. New York: Simon & Schuster.

Lykken, D.T. (1998) *A Tremor in the Blood: Uses and Abuses of the Lie Detector*. New York: Basic Books.

Mearsheimer, J. J. (2011) *Why Leaders Lie: The Truth about Lying in International Politics*. New York: Oxford University Press.

Meyer, P. (2012) *Liespotting: Proven Techniques to Detect Deception*. New York: St. Martin's Griffin.

Miller, P.; Rose, N. (2008) *Governing the Present: Administering Economic, Social and Personal Life*. Malden: Polity.

Nasher, J. (2012) *Durchschaut: Das Geheimnis, kleine und grosse Lügen zu entlarven*. München: Heyne Verlag.

National Research Council: Committee to Review the Scientific Evidence on the Polygraph. Division of Behavioral and Social Sciences and Education (2003) *The Polygraph and Lie Detection*. Washington, D.C.: National Academies Press.

Navarro, J.; Sciarra Poynter, T. (2014) *Dangerous Personalities: An FBI Profiler Shows You How to Identify and Protect Yourself from Harmful People*. New York: Rodale Books.

Oberdorfer, D. (1988) Shultz Backs 'Voluntary' Polygraph Tests at State. In: *Washington Post*, April 29, 1988, A4.

Parenti, C. (2004) *The Soft Cage: Surveillance in America From Slavery to the War on Terror*. New York: Basic Books.

Paul, B.; Egbert, S. (2014) Lügendetektion per Neuroimaging. In: *Krim J: Kriminologisches Journal* 46 (3): 153-167.

Plessner, H (1999) T*he Limits of Community: A Critique of Social Radicalism*. Amherst: Humanity Books.

Pool, R. (2010) *Planning Committee on Field Evaluation of Behavioral and Cognitive Sciences-Based Methods and Tools for Intelligence and Counterintelligence; National Research Council: Field Evaluation in the Intelligence and Counterintelligence Context: Workshop Summary*. Washington, D.C.: National Academies Press.

Porter, T. (1995) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton: Princeton University Press.

Rafael, V.L. (2013) Trayvon Martin and Edward Snowden. In: *Historynewsnetwork*. http://historynewsnetwork.org/article/152783 (28/7/2013).

Scott, J.C. (1999) *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Standop, E. (2014) *Lügen: Erkennen, entdecken, entlarven*. Darmstadt: Schirner Verlag.

Sullivan, J. F. (2007) *Gatekeeper: Memoirs of a CIA Polygraph Examiner*. Dulles: Potomac Books.

Summers, J. H. (ed.) (2008) *The Politics of Truth: Selected Writings of C. Wright Mills*. New York: Oxford University Press.

Weinberger, S. (2010) Airport Security: Intent to Deceive? In: *Nature* 465: 412-415.

Wolin, S. S. (2008) *Democracy Inc.: Managed Democracy and the Specter of Inverted Totalitarianism*. Princeton: Princeton University Press.