# A Mental Trespass? Unveiling Truth, Exposing Thoughts and Threatening Civil Liberties with Non-Invasive AI Lie Detection

1st Given Name Surname 2nd Given Name Surname 3rd Given Name Surname 4th Given Name Surname

***Abstract*—Imagine an app on your phone or computer that can tell if you are being dishonest, just by processing affective features of your facial expressions, body movements, and voice. People could ask about your political preferences, your sexual orientation, and immediately determine which of your responses are honest and which are not. In this paper we argue why artificial intelligence-based, non-invasive lie detection technologies are likely to experience a rapid advancement in the coming years, and that it would be irresponsible to wait any longer before discussing its implications. To understand the perspective of a "reasonable" person, we conducted a survey of 129 individuals, and identified consent as the major factor regarding the use of these technologies. In our analysis, we distinguish two types of lie detection technologies: "truth metering" and "thought exposing". We generally find that truth metering is already largely within the scope of existing US federal and state laws, albeit with some notable exceptions. In contrast, we find that current regulation of thought exposing technologies is ambiguous and inadequate to safeguard civil liberties. In order to rectify these shortcomings, we introduce the legal concept of "mental trespass" and use this concept as the basis for proposed legislation.**

***Index Terms*—Technology, Society, Affective Computing, Ethics**

## I. Introduction

The world's first real supercomputer was Control Data Corporation's CDC 6600, developed in 1964. The computer was enormous, the size of multiple people, and state of the art - miles far ahead of the competition. Three times as fast as its predecessor, it could run 3 million megaFLOPS. It cost the equivalent of $60 million in 2021. The CDC 6600 was so powerful the word "supercomputer" was coined to describe it. If someone were to tell its creator, Seymour Cray, that in 50 years' time a processor the size of his forearm would cost 50,000 times less and be 2 million times faster, he might not believe them. But the NVIDIA GeForce GTX Titan X, released in 2015, was exactly that.

One field of technology experiencing a similar rapid advancement is computer vision-based artificial intelligence (AI), and advanced noninvasive, AI-driven sensing technologies. As we experience this revolution firsthand, we benefit from ever more surprising contributions to our daily lives. AI powered thermal cameras systems are actively being used to screen passengers for fevers associated with coronavirus [84] [30] [25] [18] [50] and systems that extract heart rate from common video stream [56] [36] [54] [7] [23] are being used in health monitoring [35] [20].

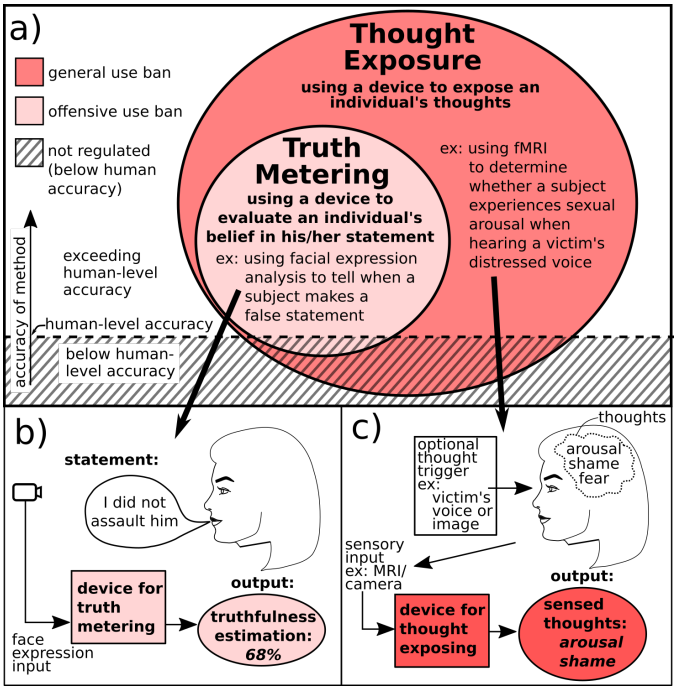


Fig. 1. **Visualization of Lie Detection Technologies** We recommend a general use ban of "accurate thought exposing" technologies and an offensive use ban of "accurate truth metering" technologies. The idea of "accuracy" (shown as the dashed bold line in part a) of the figure) must exceed average human level capabilities to fall under the proposed "Mental Trespass Act" outlined in the paper.

Recent advances have even enabled noninvasive systems to evaluate aspects of an individual's mental state from facial expressions alone, such as whether someone is imagining vs. remembering an event [34], or whether someone is experiencing one of the common emotions [68] [26] [29]. As such systems become increasingly further developed, they will likely find even more unanticipated applications. However, not all of these applications are may be beneficial to human-kind.

With the increasing powers of noninvasive AI, also come new methods for invasion of privacy and circumvention of our rights against unreasonable searches. For example, a recent AI system purports to be able to predict one's sexual orientation from their facial features [82] [51]. It is easy to foresee the harm that can result from exposing one's private sexuality considering the case of college student Tyler Clementi. After

Tyler's roommate set up a webcam in their room and publicly broadcasted a private sexual encounter he had with another male student, Tyler, decided to take his own life and under extreme stress, died of suicide [59]. Similarly daunting is the use of AI systems in police surveillance. Allegations of Chinese government oppression against the Uyghgur minorities in the Xinjian province have been made as AI facial recognition is used with camera surveillance [64]. Chinese authorities state that use of such technologies are necessary to fight terrorism and that similar surveillance systems were instrumental in enforcing the quarantines that helped halt the progression of coronavirus COVID-19 throughout China [19]. How do we ensure that advances in AI sensing technologies are not abused?

The legal system may be in a good position to help prevent abuses while not stifling the benefits such technology brings. However, legal systems have a mixed history of being in sync with technological developments [85] [43] and the future is anything but certain regarding the interaction between technological advances and humans from an ethical perspective [42]. Specifically, the interplay between advances in lie detection technologies and the legal system has a rich history and most unpredictable future [62] [38] [74] [33] [45] [16].

### A. Summary of Paper

In this paper we examine the progression of lie detection technologies and evaluate their potential to cause societal harm through loss of privacy and circumvention of civil liberties. We then consider to what extent US law currently regulates these technologies. As illustrated in Fig. 1, we distinguish two types of lie detection technology: '*accurate truth metering*, which involves evaluating the veracity of an individual's statement (e.g., the degree of belief that an individual has in their intentionally made statement), and '*accurate thought exposing*, which involves predicting an individual's inner thoughts with superior-to-human accuracy.

In our analysis, we generally find that *truth metering* is already largely within the scope of existing US federal and state laws, albeit with some notable exceptions. In contrast, we find that current regulation of *thought exposing* technologies is ambiguous and inadequate to safeguard civil liberties. In order to rectify these shortcomings, we introduce the legal concept of "mental trespass" and use this concept as the basis for proposed legislation.

More specifically, in this paper we argue that:

- Development of noninvasive, AI-based lie detection technologies are likely to progress rapidly in the near future, and no law or government effort is likely to halt its production, distribution, and use (in many cases the government is investing heavily in the advancement of such technologies).
- Lie detection technologies carry with them much potential for individual harm in terms of loss of privacy, wrongful criminal conviction, and unfair bias.
- While the current legal environment generally already regulates *accurate truth metering* technologies, it is largely ambiguous with regards to the legality of uses of *accurate thought exposing* technologies.
- In order to mitigate the potential harms such technologies may bring, we recommend the introduction of a regulatory federal "Mental Trespass Act".

Due to the hybrid nature of this paper in considering technological, legal, and public perspectives, we use an atypical paper layout. The remainder of the paper is organized as follows. A Technology Progression section provides a background of the technologies that underlie lie detection and describes the revolutionary advances that are imminent. The Laws and Limitations section examines current US Federal and State laws relevant to the coming lie detection advances and highlights gaps in their coverage. This is followed by the Public Perspective section which provides the results of a public survey in order to motivate this paper's recommendations.

## II. Technology Progression: A Lie Detection Revolution

*"If anyone bring an accusation against a man, and the accused ... jump into the river ... if he sink in the river his accuser shall take possession of his house." - Code of Hammurabi, circa 1754 BC* The underlying technology of lie detection is comprised of several components including developments in physiological knowledge, improvements in questioning techniques, and more recently, advances in AI sensing-tools and data analysis systems. It is the exponential advances that these components have made recently that make a lie detection revolution seemingly inevitable.

### A. Ancient history Timeline of Deception Technology

*"If anyone bring an accusation against a man, and the accused ... jump into the river ... if he sink in the river his accuser shall take possession of his house." - Code of Hammurabi, circa 1754 BC*

What started out as mere random chance or religious belief, the art of lie detection has progressed to include increasingly powerful scientific techniques including advanced sensing tools and more refined questioning techniques (See Fig. 2). As demonstrated in the above quotation, lie detection was essential enough to human civilizations that it appears in the Code of Hammurabi, one of the very first instances of written law from circa 1754 BC [65]. Translations of preserved tablets of the Code state that questions of honesty were to be resolved through what has been termed *trial by ordeal*. It took approximately 800 more years before the first glimmer of scientific legitimacy in lie detection to appear, which was found in the ancient Hindu text; the Vedas. Loosely based on the involuntary fight or flight response (which causes individuals to go white as blood is diverted from body extremities to the heart and lungs) The Vedas describes how to spot a poisoner, *"[The poisoner] ... does not answer questions, or they are evasive answers; he speaks nonsense . . . his face is discolored ..."* [80]. The scientific progression of lie detection continued in the 3rd century BC, as renowned physician Erasistratus used pulse, skin temperature, and skin pallor, to correctly detect the

lies of Prince Antiochus, as the prince tried to conceal his passionate love for his father's new wife [79] [10].

An underlying premise regarding lie detection began to be recognized. Charles Darwin wrote in his 1872 book, *The Expression of Emotions in Man and Animals*, that "...actions become habitual in association with certain states of the mind, and are performed whether or not of service in each particular case..." [22]. We more formally term *The Fundamental Premise of Lie Detection* as the notion that We recognize a fundamental premise of lie detection in that: *a person's internal state of mind uncontrollably leaks out into the externally observable world when appropriately probed*. Indeed, this premise must hold for a given lie detection technique to work. Through *appropriately probed* we recognize that specialized questioning techniques may be necessary to cause honest and dishonest subjects to elicit detectable differences in observable behavior. This definition additionally brings attention that advanced tools may be useful in observing these subtle differences.

*"Beyond my expectation, thru uncontrollable factors, this scientific investigation became for practical purposes a Frankenstein's monster, which I have spent over 40 years in combating." John Larson, inventor of the common polygraph*

The use of tools and specialized questioning techniques in lie detection is demonstrated with the perhaps most well-known and widely used lie detection device, the contemporary polygraph. Like Erasistratus's technique, the common polygraph tracks the subject's heart rate and respiration. The modern polygraph, however, has two notable improvements over Erastratus including: 1) additional sensors for blood pressure, skin conductivity, and respiration rate; and 2) a formal questioning technique, known as the *control question test*. The polygraph sensors collectively provide a measure of the subject's physiological arousal. Crucially, the control question test begins with questions unrelated to the matter for which the lie detector is being applied, including *baseline questions* and *control questions*. Baseline questions are trivial questions used to indicate the subject's arousal at rest. Alternatively, control questions are designed to create a strong physiological response in most people, for example *Have you ever stolen office supplies from work? Have you ever cheated on your taxes?*. The unrelated questions are followed with *relevant questions*, which are questions pertinent to whatever is being investigated (i.e. the alleged crime). The underling theory of the control question test is that someone who is lying is more likely to be nervous during the relevant questions than during the control questions, compared to an honest subject who is expected to have a stronger level of arousal during a similar or reduced response during the relevant questions compared to the control questions [63] [15]. Other questioning techniques such as the guilty knowledge test (GKT), which relies on strategic use of information only a guilty person would have, have been developed and compared with the control question test [57]. Depending on the context and person that is being interrogated, one questioning technique may be preferred and more effective than the other.

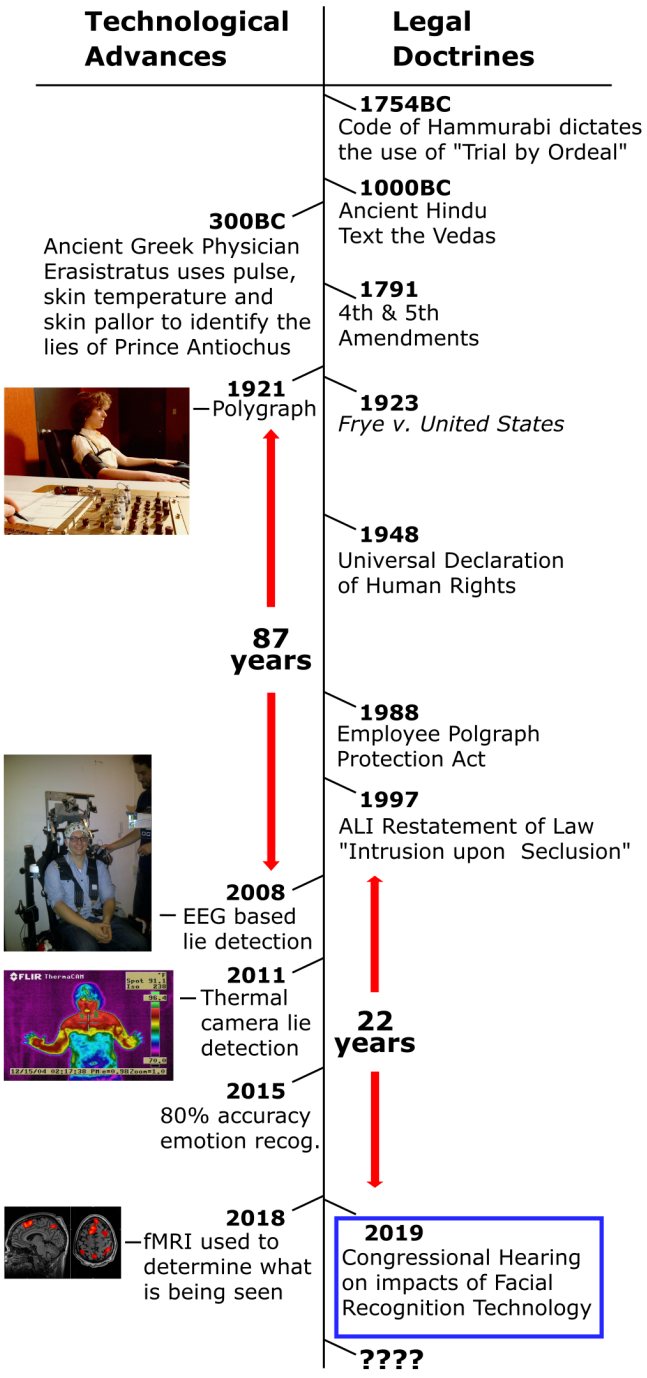


Fig. 2. **Side by Side Timeline of Technological Advances and Legal Doctrines** (Note: not to true exponential scale)

While there are many earlier references to the use of blood pressure in lie detection, John Larson, the first U.S. police officer with a PhD, is credited as the inventor of the modern polygraph in 1921. [6], [75].

Despite being grounded in scientific principles, many, including John Larson himself, questioned the merit of polygraph in measuring honesty. John Larson stated: *"Beyond my expectation, thru uncontrollable factors, this scientific investigation became for practical purposes a Frankenstein's monster, which I have spent over 40 years in combating."* Just two years after the common polygraph saw its first practical use in a criminal investigation in 1921, the American judicial system developed the legal doctrine that would almost completely bar the polygraph from ever entering the courtroom again. The *Frye test*, as it has become to be known, prevents evidence from being presented unless it is generally accepted as reliable in the relevant scientific community [73] [12]. While the polygraph has been almost completely kept out of criminal trials since its early inception due to its shaky scientific grounding, it was widely used for many years in the employment setting [76]. It was not until the 1988 Employee Polygraph Protection Act, that it was generally banned from the workplace (with notable exceptions for national security). For many years, failed lie detector tests resulted in employees losing their jobs as well as interviewees being denied employment in the first place.

Beyond the basic sensors used in the common polygraph, numerous technologies have been used for lie detection. Most notable among these is the rapid development of computer hardware as well as the analysis software which runs on it. Similar to the rapid advances in computer hardware described in the introduction, the field of computer vision has seen remarkable growth and new development in the past few decades, especially in the last several years decade. In 2012, "AlexNet" astounded researchers with its accuracy in image classification and demonstrated the power of convolutional neural networks for the task [48]. In 2014, the invention of generative adversarial networks utilized deep learning to generate realistic images [32], which recently became embroiled in controversy with their application in deepfakes. Researchers and software engineers working with computer vision have an incredible array of tools with which to develop new technologies in the coming years. We highlight the progress in computer vision specifically because these advances enable lie detection to be performed at a distance due to their inherent noninvasiveness.

Regardless of how sophisticated these deep learning algorithms have become, their effectiveness fundamentally relies on good data. And lots of it. It thus comes as no surprise that one of the major factors limiting progress in noninvasive deception detection is has been the lack of good data. However, with recent advances in Internet technologies, techniques are becoming available to scalably gather data on deception. For example, Sen et al. developed a system for gathering video deception data via crowdsourced individuals [70]. In addition, US government entities have very recently expressed desire to gather data sets on "credibility assessment", which could be used to develop deception detection technologies. In fact, during 2019, the Intelligence Advanced Research Project Association (IARPA) put out a grand challenge concerning the collection of deception data. The Credibility Assessments Standardized Evaluation (CASE) Challenge formally called for a protocol to standardize this procedure in regards to how these datasets are gathered and accessed. Additionally, Governments have started pouring vast amounts of funding into projects which expand their powers of surveillance. Backed by the Chinese and Russian governments, AI startup Megvii raised $460 million for the development of facial recognition technology [41].

We emphasize these specific examples to illustrate the non-invasive nature of these developing technologies, advancements in data collection procedures/capabilities and Government vested interest. Because of these qualities, it seems inevitable that accurate AI-based lie detection will soon be upon us.

## III. Laws and Limitations: Current US Federal and State Laws

In this section, we discuss various legal issues with the public use of non-invasive deception detection technology without an observed party's consent. The 1948 Universal Declaration of Human Rights has explicit language regarding human rights to"privacy", with Article 12 of the declaration stating "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence..." [58].

While it is noteworthy that any notion of such a privacy right was considered so important as to be codified in the Universal Declaration, such declarations are left largely impotent with the interpretation of what constitutes "arbitrary interference" and "privacy" left undefined. An examination of international law is further limited by the fact that individual protections depend entirely upon a state's willingness to comply with international law [39]. Different international jurisdictions have approached privacy rights in widely differing ways, with the EU seen as having strong protections based in protections of human dignity compared to minimalist protections in the US based on liberty protection from the government [52].

In this section we focus on United States Law as the basis of our analysis. In addition to the minimal privacy protections offered under US law, focus on the US is particularly suited given the recent revelations of the extent of US government and US industry intrusion upon privacy as demonstrated through the 2013 Snowden and 2018 Cambridge Analytica scandals [39].

While the interpretation of what constitutes "arbitrary interference" and "privacy" are left undefined, it is noteworthy that any notion of such a privacy right was considered so important as to be codified in the Universal Declaration.

While our focus is on U.S. law, it is worth noting that

### A. *Fourth 4th Amendment*

In the United States, perhaps the most relevant legal issue with regards to public deception detection is raised with re-

gards to the fourth 4th amendment. The fourth 4th amendment establishes the "right of the people to be secure in their persons...against unreasonable searches" and has been interpreted to prohibit searches when there is a reasonable expectation of privacy [8]. Several cases have established that in general there is no reasonable expectation of privacy for things which are in plain view in a public area. For example, the U.S. Supreme Court held that garbage that is left out on the curb can be searched without a warrant in California v. Greenwood [37] [72] [21]. This has been extended to include use of some specialized equipment, particularly the use of a plane for aerial observation of someone's backyard in California v. Ciraolo [27], and observation of an open field in an industrial complex with a high definition camera in Dow Chemical Co. v. United States [44] [67]. The court seemed to indicate the relevance of whether the equipment was available to the public, in one case finding that the EPA did not violate the fourth 4th amendment when it "was not employing some unique sensory device not available to the public". An analysis of the smells during a routine traffic stop with a specialized drug-sniffing dog was also found to not constitute an unreasonable search in Illinois v. Caballes [24] [71] [11]. However, the ability to observe someone from a public area is not absolute. The Supreme Court found in Kyllo v. United States [69] [4] [31] that viewing a person's home from outside with a thermal imaging camera (to determine if high temperature drug growing lights were used) was indeed a violation of one's "reasonable expectation of privacy". In light of these Supreme Court cases regarding fourth 4th amendment rights, how would we expect the use of a video-based lie detection apparatus to play out? One perspective is that an individual's facial expressions are in plain view and thus do not carry a reasonable expectation of privacy, as in California v. Ciraolo regarding a person's backyard, or someone's garbage on the curb in California v. Greenwood. It is likely that the camera used for deception detection need not be more advanced than the high resolution camera deemed to be acceptable in Dow Chemical v. United States. However, lie detection does involve use of state of the art AI-driven algorithms and computer vision techniques. It seems conceivable that a court could find such algorithms invasive in how they uncovering someone's internal state in an invasive way. Additionally, we may expect a court to consider, as it did in Dow Chemical Co. v. United States, whether the equipment used is publicly accessible. Thus, whether such lie detection technology is made public or not will possibly affect whether its use constitutes a fourth 4th amendment search (e.g., if it is made available to the public, the Government would not be using "specialized technology"). However, it should also be noted that fourth 4th amendment issues are limited to the government (or people working on behalf of the government) and does not apply to public at large.

### B. *Fifth 5th Amendment*

In addition to the potential fourth 4th amendment issues, the use of lie detection technology in a court of law by the prosecution may bring up Constitutional Law issues with regards to the fifth 5th amendment protection against self-incrimination. The fifth 5th amendment provides that "[n]o person shall be ... compelled ... to be a witness against himself" [9] [66]. We foresee that use of a lie detection technology without a subject's consent may be interpreted as compelled testimony. However, the courts have interpreted the fifth 5th amendment narrowly, giving the prosecution the right to compel the accused to provide a password to encrypted computer data [81] [17]. Additionally, the courts have determined that a suspect may be compelled to produce fingerprints, blood, and fingernail scrapings without violating the fifth 5th amendment [40] [40]. Further, courts have even found that compelling a witness to provide a voice sample for identification does not trigger fifth 5th amendment protections [83]. Thus, we believe that it is unlikely that a court would find use of an AI-driven lie detection technology to be a violation of one's fifth 5th amendment rights. However, in certain contexts perhaps this is not the case. For example, Thompson argues that highly invasive lie detection technology, such as unconsented application of the fMRI, is likely to violate the fifth 5th amendment due process law as it "shocks the conscience" [78]. Therefore, we take the stance that the degree of invasiveness is what fundamentally defines this question of violating the fifth 5th amendment. We bring to light in this paper that highly accurate non-invasive lie detection technologies are not only imminent, but their risk for infringing upon our civil liberties is much greater. This is due to the fact that non-invasive lie detection devices are able to lie detect non-consenting individuals from a distance. Furthermore, it is not clear whether these noninvasive methods would "shock one's conscience" enough to violate the fifth 5th using Thompson's methodology terminology.

### C. *Employee Polygraph Protection Act*

The Employee Polygraph Protection Act (EPPA) prevents private employers from requiring job applicants or current employees to submit to a lie detector of any kind, but allows polygraphs to be used by certain sectors, namely government and security positions. However, according to its website, the fMRI based lie detection company No Lie MRI "measures the central nervous system directly and such is not subject to restriction by these laws". As noted by Greely and Illes, the language used in the provision of the legislation is broad enough that loopholes like this are possible [33]. Without an explicit amendment or judicial review, No Lie MRI could continue to offer its services to employers, violating the intention of the EPPA, but not the text of the law. The EPPA is limited to employer-employee relationships, and is silent with regards to public use.

### D. *Invasion of Privacy Laws*

The strongest limitations on the public use of a non-invasive lie detection technology arise from state law. While it is difficult to analyze each state's laws individually, a concise restatement of the preferred rules used by a majority of the states is available in the "Restatement of Law", written by

the American Law Institute (ALI). The Restatement provides the law of Intrusion Upon Seclusion, commonly referred to as "invasion of privacy", which makes liable one who "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person". This liability extends even when there is no publication or use of the information obtained in violation. In general, surveillance from a public place is not intrusion upon seclusion, however, exceptions to this rule exist. In summary, it is unclear if when accurate noninvasive lie detection arrives, it will be legal to use on non-consenting individuals caught unawares.

### *E. Court System*

In the federal court system, it is unclear whether even a highly accurate lie detector would be admitted as evidence. Currently, polygraph tests and their results are almost entirely inadmissible in a federal court under evidentiary rules. Polygraph results are what is known as "highly prejudicial," meaning that regardless of the test's accuracy or even its relevance to the case at hand, hearing about it will bias the jury. If the polygraph indicates that the defendant has lied, despite its questionable accuracy, a jury may treat that as definitive proof that the defendant lied. Additionally, if they believe the defendant lied about material facts related to the case, that may indicate proof of guilt to a jury, no matter how relevant or irrelevant those facts are to the defendant's guilt or innocence. For these reasons, it is possible that even a 99% accurate lie detector could be excluded from evidence, due to a judge fearing the jury will treat it as 100% accurate.

There are currently two standards by which scientific evidence can gain admission into the courtroom depending upon jurisdiction, known as the Frye standard and the Daubert standard. The Frye standard provides that in order to be admitted, the scientific basis for the evidence "must be sufficiently established to have gained *general acceptance* in the particular field in which it belongs". Per this standard, computer AI-based lie detection would likely not be admitted in its current state, as the underlying technology is still developing and the accuracy of this method of lie detection has not been well established.

The Daubert standard, which has largely superseded the Frye standard in both federal court and most state courts, sets stricter guidelines for evidence being admitted. In addition to *general acceptance*, the Daubert standard also considers whether the scientific evidence has been tested, whether it has been peer reviewed, and whether it has a high rate of error. , but leaves the decision up to the court rather than the scientific community. This includes the Frye standard of general acceptance as well as AI-based lie detection would also likely be kept out of courtrooms according to Daubert this standard due to its current lack of widespread testing and peer review. These two standards ensure that the courts are well equipped to keep potentially inaccurate scientific evidence out of the courtroom.

Whether or not a technology is admitted into the courtroom is of the utmost importance for the following reason. Historical review shows that once a technology is deemed as legitimate (e.g. fingerprint analysis) or as questionable (such as the polygraph), such characterizations are unlikely to be changed [78]. Even though both fingerprint and polygraph analysis has questionable scientific basis, fingerprinting, which was originally admitted into the court in 1911, before the Frye or Daubert evidentiary standards were established, spent a long time being generally admissible in court [3]. A major issue with the polygraph was raised in case law, with the Oregon Supreme Ct. finding "the use of the polygraph ha[s] the potential to dehumanize parties and witnesses, treating them or as 'electrochemical systems to be certified as truthful or mendacious by a machine.'" [61]. The Daubert standard has prevented polygraph admissibility for that reason amongst the others mentioned [53]. Given that recent legal analyses argue that fMRI should not be allowed at this time [49], [46] [86] [55], it is likely the Daubert standard will keep these technologies out of the courtrooms as well for the time being. Scholars have gone on to argue for the urgent need to regulate developing lie detection technologies, such as the neuroscience-based technologies upon which fMRI lie detection is one flavor [33] [55]. Prior analysis has come to the conclusion that looking at technologies like fMRI through analogy with blood test and/or forced testimony is inappropriate, arguing that "the implicit assumption of mind-body dualism, which underlies this thinking, is dated and, most likely, no longer tenable" [78]. Scholars have argued the importance of considering legal implications of an advancing technology before it becomes ubiquitous, Thompson stating "if the existing scientific literature is indeed a harbinger of an important new technology, it will be to society's benefit that some thought have been put into its implications before its wide scale deployment." [78] . All in all, The topic of advanced lie detection has received recent attention in ethical and legal contexts [49] [28] [33] [77] [55], however, precise definitions of the technologies in question and proposed legal doctrines offering a solution have yet to be fleshed with enough granularity. With the legal doctrine and case history being classified as ambiguous at best, there is a clearly a strong societal need to formally define what should be allowed regarding these evolving technologies.

## IV. Public Perspective

### *A. Crowd Sourced Survey Responses*

To understand public opinion on the usage of these lie detection technologies, we sampled the population by conducting a survey using the crowdsourcing platform Amazon Mechanical Turk. We included demographic information on the survey and based on the responses, launched multiple surveys with participation requirements to ensure that the demographic distribution of our respondents resembled the demographic distribution of the United States. We believe matching the distribution is essential for obtaining not only a reliable sample, but one where we can reasonably extrapolate to claim

any kind of generalizable opinion. We monitored the quality of the survey responses by implementing a control question and eliminated all survey responses where the control (e.g. control question: "Answer strongly agree to this question?" all respondents failing to answer this question correctly were removed from the data). We also incorporated a required free text response question to our survey and removed responses where the length of the response was less than 10 characters in length. After all unsatisfactory data points were removed, we were left with n = 129 quality responses. We set out to investigate whether public opinion was in favor of or opposed to the legality of using these technologies on an individual without first obtaining their consent (crucially important for noninvasive lie detection technologies as they can be used on an individual caught blissfully unaware). Two multiple choice questions asked respondents their level of agreement on whether police should be allowed to use a computer program to detect lies in a criminal suspect when the accuracy levels of the device were 100% and 90% (See full question text below). The results from the survey responses were strongly indicative of opposition to unconsented usage when accuracy of the device was not absolute.

Survey Questions

Q1. If there were a 100% accurate computer program to detect lies from a video recording, police in the US should be allowed to use it on criminal suspects with their knowledge in an interrogation room, but without requiring the suspect's consent.

Q2. What if the computer program were only 90% accurate?

Q3. Please briefly explain your answers

TABLE I
SURVEY STATISTICS

| Question | #Agree | #Disagree | Neutral | p-value |
|---|---|---|---|---|
| Q1 | 73 | 44 | 19 | <0.01 |
| Q2 | 33 | 69 | 27 | <0.01 |

Survey questions Q1 and Q2 had five response options: strongly agree, agree, neutral, disagree, and strongly disagree. We combined the agree and strongly agree responses to find the number in favor as well as the disagree and strongly disagree responses to find the number opposed. 33 people were in favor, 69 people opposed and 27 were neither for nor against this usage case. We conducted a proportions statistical test with our null hypothesis being that there is no difference in public opinion regarding this question (e.g. the number in favor is equal to the number opposed). After running the statistical test, the probability of that null hypothesis given our data was p=0.0001 or 1/100th of a percent (0.01%). We thus reject the null hypothesis of there being no difference in public opinion and accept the alternative hypothesis that likely there is a difference (meaning a majority of people are opposed to unconsented use of these lie detection technologies).

Some of the free text responses are:

"If there was no margin of error then it would be acceptable. There is always that small percentage falsely accused and I would not be comfortable with a machine making a determination."

"I think it opens the door to more and more invasive policies."

"I believe it should be used in law enforcement, as it will help 10 fold in reducing and finding criminals"

"A suspec is not yet convicted of a crime. They are innocent until proven guilty. They have certain rights which shoulkd be respected under the constitution."

"Seems like to much Big brother to me."

"THESE TACTICS ARE AS LIKELY TO BE USED OR INTERRUPTED INCORRECTLY AGAINST A LAWFUL CITIZEN"

"This is way to Orwellian for me! Now an AI computer program detecting lies? What if this is hacked and made to work contrary to the original program? I say no to this."

"Accuracy of Program should be a guide."

Based on public opinion, there is certainly concern over unregulated lie detection technology being used maliciously and we have an obligation as a society to mitigate that outcome. We are hopeful that our proposed "Mental Trespass Act" and recommendations for updating the language in the EPA to reflect our technology definitions would greatly aid this communal effort.

## V. RECOMMENDATIONS

### A. Definitions and Proposed Law

In providing legal recommendations on how to mitigate the potential harms and ambiguity in the field, we first define two types of relevant technology as well as the different categories of their usage. We distinguish two major classes of lie detection tools including (1) accurate truth metering, and (2) accurate thought exposing (Depicted in figure 1). Accurate truth metering is defined as *Use of a device to measure an individual's level of belief in an intentional statement made by the individual, with the device usage having an accuracy exceeding typical human performance.* A statement broadly includes spoken utterances, written text and drawings, bodily gestures, and other forms of communication. An intentional statement, requires that the statement maker has the mental intent to make the statement. Thus, a spontaneous gasp of surprise, or the unconscious blushing after hearing a question are not intentional statements. In defining accurate, we use an excedat-hominem standard, i.e. a level of accuracy which clearly exceeds typical human ability. Thus, in defining an accurate truth meter, we consider the numerous studies on human performance regarding lie detection and note that this level of accuracy has been found to be approximately 54 % [13], even amongst expert judges [14].

Accurate thought exposing is defined as *Use of a device to expose an individual's thoughts, without the individual's consent, with the device usage having an accuracy exceeding typical human performance.* Accurate thought exposure specifically includes instances of questioning a suspect without consent and accurately measuring the suspect's physiological response to the questions. As with the definition of truth

metering, the definition of accurate thought exposure requires a level of accuracy which clearly surpasses human ability. A primary distinction of truth metering and accurate thought exposing, is that truth metering requires an overt/intentional statement by the individual regarding the issue being observed (Bottom portion of fig 1 illustrates this distinction). For example, in asking an individual what time it is, by evaluating whether they are being honest about the time involves only truth metering. However, if one then uses a system to gauge the level of anger in their voice, the technology has crossed the boundary into the realm of thought exposure because the overt response to the question being asked doesn't pertain to anger. Similarly, if an individual is talking out loud to others in public area on his/her own accord, and we evaluate the honesty of each of his/her overt statements, we are truth metering. However, if the individual's statements do not directly involve their emotions, and we determine that the individual feels high levels of arousal we are thought exposing (noting that a human observer would typically not be able to discern that information). In addition to the two different classes of non-invasive deception detection technology, it is important to independently consider whether the use is in the context of (1) a criminal investigation, (2) pertaining to one's employment, or (3) a "public use". Within context of criminal investigation, we consider not only direct involvement in a criminal trial, but also any police interrogations which led to the arrest, as well as any gathering of evidence or a crime either with or without probable cause by an agent of the state. The employment context involves both current employees of a business, as well as interviews of prospective employees. Within "public use", we also consider uses by commercial entities in interactions with customers, even though the action may occur in a private location. We concur with Greely and Illes that lie detection technologies and services must be regulated to prevent harm. Specifically, we believe that a federal Mental Trespass Act should be passed which: 1.) Provides a general ban on the use of "accurate thought exposing" on an individual without the individual's consent., 2.) Makes an exception to this ban for use of "accurate truth metering" on individuals in a public space, as long as the particular usage would not be found offensive by a reasonable person, 3.) Updates the Employee Polygraph Protection Act to explicitly include "accurate thought exposing" and "accurate truth metering", even when such devices are noninvasive.

## VI. Discussion

As much as these technologies have the potential to infringe upon the civil liberties of the people in a malevolent way, there is an abundance of instances where the proper use of sophisticated, AI-driven sensing technologies and their associated algorithms can provide benefits to society.

### A. Propagation of Fake News

Consider the infamous picture of the "MAGA teen" Nicholas Sandmann (Fig. 3a) that caused a recent social media and news firestorm as news commentators, actors, and numerous others, joined in for wave after wave of vilification towards Nicholas Sandmann's alleged harassment of Native American Nathan Phillips [60].


Fig. 3. **Infamous MAGA "smirking teenager"** a) Nicholas Sandmann's single frame expression taken out of context helped fuel a firestorm of rebuke even though automated facial expression analysis detects no contempt, b) Analysis of another image from the event suggests that Sandmann was experiencing more fear and surprise.

Attention was drawn to Sandmann's expression, one CNN commentator tweeting "Have you seen a more punchable face", as others issued Sandman and his classmates death threats [1]. Yet, an analysis of Sandmann's face with facial expression analysis tools [5] suggests that he was experiencing amusement rather than contempt. Indeed later reports validated Sandman's assertions that he and his fellow classmates were not harassing the native American Nathan Phillips, but rather that the students were victims of harassment themselves [2] (partially evidenced by Fig. 3b indicating that Sandman was displaying expressions of more fear and surprise than contempt feeling more afraid and caught off-guard). Had the news media used a noninvasive AI facial expression evaluation tool, this debacle (and other false news propagation like it) could have perhaps been avoided.

### B. Ensuring Fairness and Justice in the Courts

Although the Frye and Daubert Standards would certainly keep out accurate stand to keep out inaccurate truth metering technologies from the courtrooms, there are approaches that can be taken to minimize fairness issues raised. issues those standards posit to maximize the probability of obtaining justice in our Nation's court proceedings. We demonstrate these aspects using three components: (1) an interview with a judge, (2) establishment of *essential design primitives* for developing accurate truth metering technologies, and (3) example steps to be taken to respect an individual's cultural background in use of technology through one example, hope to show the ramifications for respecting an individual's cultural background.

*1) Interview with Judge:* In order to get an expert opinion on the potential impact advances in lie detection technologies could have on the courts, we interviewed standing County Judge Dennis Cohen of Livingston County, New York, who has twelve years experience on the bench.

On the topic of emerging technologies in lie detection, Judge Cohen said *"I think it is a big area of advancement in law, and could help us resolve cases and work through*

*investigations ... just looking at what high resolution cameras have done for us with law shows that we can often identify the right culprit or prove that something happened or didn't happen."* Judge Cohen went on to say *"Our whole society is changing because of technology. If it could be determined to be reliable ... then it could open up a whole new phase of things."*. When asked about his opinion on relating the polygraph to these developing technologies threats and their associated threats of unreasonable searches, Cohen remarked *"Polygraphs are voluntary. This [referring to these developing technologies] would also be a voluntary procedure as well, at least for the foreseeable future. Therefore it would not ever reach the bounds of an unreasonable search."*. Here we see an important point brought up that when consent has been unquestionably obtained from an individual, usage of the polygraph or technologies to replace the polygraph never constitute an unreasonable search. However, the utility of such technologies designed in this way are vastly if not completely diminished due to their less than perfect 100% accuracy in ligt of their giving rise to the " highly prejudicial" nature. Thus, it is prudent that in developing these technologies, that an entirely different approach be taken in their design primitives, development and deployment.

*2) Essential Design Primitives:* If accurate truth metering and/or thought exposure is used by law enforcement, it should be equally effective across all races and genders. Therefore, it is the responsibility of individuals us and others who are researching and developing this technology to collect diverse data. We believe this could even be encouraged/enforced by federal funding guidelines for those who are studying deception detection using Artificial Intelligence. In order to receive federal grants for this purpose, labs could be required to meet certain diversity standards in the data they collect and use in their deception detection algorithms. Additionally, the performance of said lie detection technologies should be standardized across all law enforcement entities.

Another relevant issue is how to maximize accuracy (as well as ability to deploy such devices in the court rooms) while preserving investigator autonomy. One solution proposed by Kleinberg et al., in their prediction framework for whether judges should jail or release criminal defendants on bail, is to integrate *the machine* into the existing procedure, creating a human-machine symbiosis [47]. Instead of having the algorithm make all the decisions, the algorithm should give the people that are using it more information for them to make informed decisions themselves.

In this vein, it is our suggestion for lie detection researchers to create an output that is nuanced and detailed, rather than a binary 1 for "lying" and a 0 for "not lying." The lie detection device should detect and display indicators of deception when they appear. This fundamentally changes the role of the device. Instead of performing the evaluation based on an arbitrary decision boundary, it acts as a tool to assist people in doing the evaluation themselves. To interpret these more nuanced results, trained human operators should be employed. The use of such operators could even be required for the technology to be used. These operators should understand how to interpret the output and convey that information to investigators, while also understanding and conveying potential biases in certain questions as well as the potential for inaccuracy in the technology.

*3) Ramifications for Respecting Diverse Cultures:* In this section, we hope to show with one concrete example how we could operationalize these technologies to promote fairness. The US can easily be viewed as a conglomeration of diversity melting pot of cultures given that most of the population can trace their family roots back to a family that immigrated to the US in the first place. This causes there to be a melting pot of different cultural backgrounds inevitably find their way into the courtrooms. Challenged by how to integrate all these cultures successfully and fairly into the legal system, the AI-driven algorithms behind sensing technologies could provide valuable, novel solutions.

Currently, the US legal framework does not support the wearing of masks in the courtroom. However, given the circumstances brought on by the COVID19 pandemic, this restriction has temporarily been lifted. This begs the question, should it ever have been a stipulation in the first place? Take for example a woman with a Muslim background who wishes to uphold her cultural traditions and wear a hijab during a court proceeding (e.g., she is called as a witness to bear testimony to the actions of another person). With our advanced sensing technology many options exist. First and foremost, the identity of the witness can be unquestionably established. This is perhaps the most important aspect to uphold. In the rarest of cases, let us for arguments sake assume that the wearing of a hijab interferes with one or two jury members' interpretation/perceived credibility of the witnesses testimony. In such a situation, human operators interpreting the results of the technology employed in the courtroom could be trained to identify this bias and address it. This is just one small example of where these advanced AI-driven sensing algorithms can be used to treat every person that comes into the legal system with respect and fairness of the highest standard.

### C. Elaborations on Proposed Recommendations

While dishonesty might frequently be harmful to people and society as a whole, we do believe that people have the right to exercise their ability to lie in some circumstances non-maliciously. In the balance is an individual's right against unreasonable search and invasion of privacy, on the other is another individual's right to use a machine to detect when they are being lied to. As defined in our recommendations, a truth metering device (which is not a thought exposing device) only operates on an individual's statement. By uttering a voluntary statement, we view a speaker as inviting such a statement to be evaluated, in other words, providing consent. Respecting that such consent may be unintended, we believe a proper balance in the use of truth metering devices, borrowing principles from existing invasion of privacy law, is to ban only offensive uses. In contrast, a thought exposing device gives the power to go beyond evaluating the veracity of

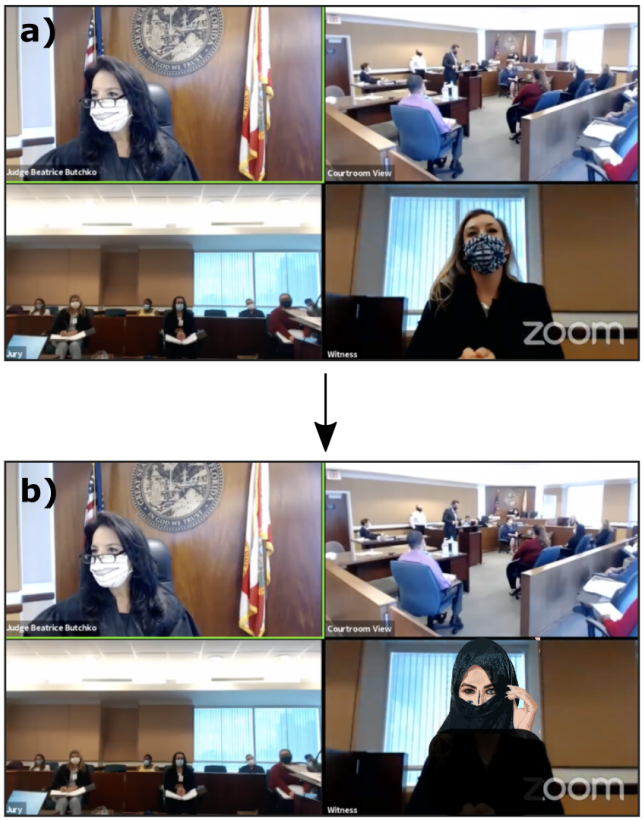


Fig. 4. **Positive Example of Applying AI-driven Algorithms to Promote Respect for Persons** a) A screen shot of the first jury trial during the COVID-19 pandemic in Florida that was livestreamed on YouTube on July 14, 2020 b) The same photo with a hypothetical Muslim witness wearing a Hijab

an individual's statements, potentially exposing one's most private and personal thoughts. For this reason, we not only suggest a complete public ban on use of accurate thought exposing technology, but also regulation on the production and dissemination of such devices. Non-malicious lies are frequently altruistic, or told by people to protect themselves or others, and allowing lie detection to remain unrestricted would prevent these kind of lies. We believe the harm caused by this would outweigh the benefit of allowing malicious lies to be detected, and therefore we believe that accurate thought exposing technologies should be regulated for the general public. Through establishing these regulations, we not only prevent potentially malicious uses, we offer further protections for the people against unreasonable searches of their mental sanctuaries. Recall in the case of Dow Chemical Co. v. United States, because the observation of the industrial complex was done through a high resolution camera and the general public had access to that technology, the court ruled that this did not constitute the bonds of an unreasonable search. With the public not having direct access to these emerging accurate thought exposing technologies, we thus prevent this legal precedent to be carried out in the future; enabling Government entities to take advantage of individuals in a variety of contexts. It is our position that truth metering devices could remain available to the general public, as long as they were limited to uses that would be deemed non-offensive to a reasonable person. This would allow them to be used for lie detection in contexts such as navigating a foreign environment and dealing more fairly and justly with children. We formally take the stance that thought exposure systems must be regulated more strictly, as they can reveal more private information about a person (recall the unfortunate circumstances that led to the death of Tyler Clementi). We recommend that accurate thought exposing technologies be regulated for the general public (potentially by using a permit schema that is externally audited by multiple third parties relatively frequently), and that their unconsented use be codified as an illegal mental trespass.

## VII. Conclusion

Accurate deception detection likely will not be developed for some time does not currently exist, although it is probably closer than most of us think. The technology's ambiguous legal status makes it necessary to establish guidelines before it is fully developed and available. The introduction of AI-driven advanced sensing technologies for this task raises new concerns regarding privacy and consent due to their noninvasive nature. Defining the technologies precisely as "accurate thought exposing" and "accurate truth metering" technologies is essential for proposing legal doctrine that is as airtight as possible to safeguard our civil liberties appropriately. Otherwise, potential loopholes could emerge in the future causing harm to society and bypassing the intentions of the law and the protections that it offers (as is the case currently with No Lie fMRI and the Employee Polygraph Protection Act). Emerging lie detection technology will be a powerful tool, benefiting the criminal justice system, the medical community, and many others. In order to utilize it to its fullest potential, however, it must be developed and used responsibly with the necessary restrictions - or it may end up doing more harm than good.

## Acknowledgment

## References

[1] punchable face description. https://www.washingtontimes.com/news/2020/jan/13/reza-aslan-likely-be-sued-over-now-deleted-punchab/. Accessed: 2020-08-21.
[2] real story description. https://reason.com/2020/01/21/covington-catholic-media-nick-sandmann-lincoln-memorial/. Accessed: 2020-08-21.
[3] People v. jennings, 1911. 96 N.E. 1077.
[4] Douglas Adkins. The supreme court announces a fourth amendment general public use standard for emerging technologies but fails to define it: Kyllo v. united states. *U. Dayton L. Rev.*, 27:245, 2001.
[5] Affectiva. Determining accuracy, 2018. Retrieved August 8, 2018 from /urlhttps://developer.affectiva.com/determining-accuracy/.
[6] Ken Alder. *The lie detectors: The history of an American obsession*. Simon and Schuster, 2007.
[7] Karim Alghoul, Saeed Alharthi, Hussein Al Osman, and Abdulmotaleb El Saddik. Heart rate variability extraction from videos signals: Ica vs. evm comparison. *IEEE Access*, 5:4711–4719, 2017.
[8] Akhil Reed Amar. Fourth amendment first principles. *Harvard Law Review*, 107(4):757–819, 1994.
[9] Akhil Reed Amar and Renee B Lettow. Fifth amendment first principles: The self-incrimination clause. *Michigan Law Review*, 93(5):857–928, 1995.

[10] Tuvya T Amsel. Planting the seeds of polygraph's practice a brief historical review. *European Polygraph*, 13(3):141–154, 2019.

[11] Jeffrey A Bekiares. Constitutional law: Ratifying suspicionless canine sniffs: Dog days on the highways-illinois v. caballes. *Fla. L. Rev.*, 57:963, 2005.

[12] David E Bernstein. Frye, frye, again: The past, present, and future of the general acceptance test. *Jurimetrics*, pages 385–407, 2001.

[13] Charles F Bond Jr and Bella M DePaulo. Accuracy of deception judgments. *Personality and social psychology Review*, 10(3):214–234, 2006.

[14] Charles F Bond Jr and Bella M DePaulo. Individual differences in judging deception: Accuracy and bias. *Psychological bulletin*, 134(4):477, 2008.

[15] MT Bradley and KI Klohn. Machiavellianism, the control question test and the detection of deception. *Perceptual and Motor Skills*, 64(3):747–757, 1987.

[16] Spencer J Brooks. Scanning the horizon: The past, present, and future of neuroimaging for lie detection in court. *U. Louisville L. Rev.*, 51:353, 2012.

[17] Robert H Cauthen. The fifth amendment and compelling unencrypted data, encryption codes, and passwords. *Am. J. Trial Advoc.*, 41:119, 2017.

[18] Vinay Chamola, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. *IEEE Access*, 8:90225–90265, 2020.

[19] Bei Chen, Simon Marvin, and Aidan While. Containing covid-19 in china: Ai and the robotic restructuring of future cities. *Dialogues in Human Geography*, page 2043820620934267, 2020.

[20] Xun Chen, Juan Cheng, Rencheng Song, Yu Liu, Rabab Ward, and Z Jane Wang. Video-based heart rate measurement: Recent advances and future prospects. *IEEE Transactions on Instrumentation and Measurement*, 68(10):3600–3615, 2018.

[21] David W Cunis. California v. greenwood: Discarding the traditional approach to the search and seizure of garbage. *Cath. UL Rev.*, 38:543, 1988.

[22] Charles Darwin. *The Expression of the Emotions in Man and Animals*. D. Appleton, 1873.

[23] Yunbin Deng and Arya Kumar. Standoff heart rate estimation from video: a review. In *Mobile Multimedia/Image Processing, Security, and Applications 2020*, volume 11399, page 1139906. International Society for Optics and Photonics, 2020.

[24] George M Dery III. Who let the dogs out-the supreme court did in illinois v. caballes by placing absolute faith in canine sniffs. *Rutgers L. Rev.*, 58:377, 2005.

[25] Rajvikram Madurai Elavarasan and Rishi Pugazhendhi. Restructured society and environment: A review on potential technological strategies to control the covid-19 pandemic. *Science of The Total Environment*, page 138858, 2020.

[26] Florian Eyben, Martin Wöllmer, and Björn Schuller. Opensmile—introducing the munich open-source emotion and affect recognition toolkit. In *2009 3rd international conference on affective computing and intelligent interaction and workshops*, pages 1–6. IEEE, 2009.

[27] Rosemarie Falcone. California v. ciraolo: The demise of private property. *La. L. Rev.*, 47:1365, 1986.

[28] Martha J Farah, J Benjamin Hutchinson, Elizabeth A Phelps, and Anthony D Wagner. Functional mri-based lie detection: scientific and societal challenges. *Nature Reviews Neuroscience*, 15(2):123–131, 2014.

[29] Rana Seif Fathalla and Wafa Saad Alshehri. Emotions recognition and signal classification: A state-of-the-art. *International Journal of Synthetic Emotions (IJSE)*, 11(1):1–16, 2020.

[30] Simon James Fong, Nilanjan Dey, and Jyotismita Chaki. Artificial intelligence for coronavirus outbreak, 2020.

[31] Amanda S Froh. Rethinking canine sniffs: The impact of kyllo v. united states. *Seattle UL Rev.*, 26:337, 2002.

[32] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In *Advances in neural information processing systems*, pages 2672–2680, 2014.

[33] Henry T Greely and Judy Illes. Neuroscience-based lie detection: The urgent need for regulation. *American Journal of Law & Medicine*, 33(2-3):377–431, 2007.

[34] Kamrul Hasan, Wasifur Rahman, Luke Gerstner, Taylan Sen, Sangwu Lee, Kurtis Glenn Haut, and Mohammed Hoque. Facial expression based imagination index and a transfer learning approach to detect deception. In *2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII)*, pages 634–640. IEEE, 2019.

[35] MA Hassan, AS Malik, D Fofi, B Karasfi, and F Meriaudeau. Towards health monitoring using remote heart rate measurement using digital camera: A feasibility study. *Measurement*, 149:106804, 2020.

[36] Mohamed Abul Hassan, Aamir Saeed Malik, David Fofi, Naufal Saad, Babak Karasfi, Yasir Salih Ali, and Fabrice Meriaudeau. Heart rate estimation using facial video: A review. *Biomedical Signal Processing and Control*, 38:346–360, 2017.

[37] Madeline A Herdrich. California v. greenwood: The trashing of privacy. *Am. UL Rev.*, 38:993, 1988.

[38] Charles R Honts and Mary V Perry. Polygraph admissibility. *Law and Human Behavior*, 16(3):357–379, 1992.

[39] Kristian P Humble. International law, surveillance and the protection of privacy. *The International Journal of Human Rights*, 25(1):1–25, 2021.

[40] Fred E Inbau. Self-incrimination–what can an accused person be compelled to do? *J. Crim. L. & Criminology*, 89:1329, 1998.

[41] Harrison Jacobs and Pat Ralph. Inside the creepy and impressive startup funded by the chinese government that is developing ai that can recognize anyone, anywhere. Business Insider, 2018. Retrieved August 15, 2018 from https://www.businessinsider.com/china-facial-recognition-tech-company-megvii-faceplusplus-2018-5.

[42] Sheila Jasanoff. *The ethics of invention: technology and the human future*. WW Norton & Company, 2016.

[43] Sheila Jasanoff and Sheila Jasanoff. *Science at the bar: Law, science, and technology in America*. Harvard University Press, 2009.

[44] Thomas J Joyce. The epa's use of aerial photography violates the fourth amendment: Dow chemical co. v. united states. *CoNN. L. REv.*, 15:327, 1982.

[45] Ian Kerr, Max Binnie, and Cynthia Aoki. Tessling on my brain: the future of lie detection and brain privacy in the criminal justice system. *Canadian Journal of Criminology and Criminal Justice*, 50(3):367–387, 2008.

[46] Leo Kittay. Admissibility of fmri lie detection-the cultural bias against mind reading devices. *Brook. L. Rev.*, 72:1351, 2006.

[47] Jon Kleinberg, Himabindu Lakkaraju, Jure Leskovec, Jens Ludwig, and Sendhil Mullainathan. Human decisions and machine predictions. *The quarterly journal of economics*, 133(1):237–293, 2018.

[48] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

[49] Daniel D Langleben and Jane Campbell Moriarty. Using brain imaging for lie detection: Where science, law, and policy collide. *Psychology, Public Policy, and Law*, 19(2):222, 2013.

[50] Siddique Latif, Muhammad Usman, Sanaullah Manzoor, Waleed Iqbal, Junaid Qadir, Gareth Tyson, Ignacio Castro, Adeel Razi, Maged N Kamel Boulos, Adrian Weller, et al. Leveraging data science to combat covid-19: A comprehensive review. 2020.

[51] John Leuner. A replication study: Machine learning models are capable of predicting sexual orientation from facial images. *arXiv preprint arXiv:1902.10739*, 2019.

[52] Avner Levin and Mary Jo Nicholson. Privacy law in the united states, the eu and canada: the allure of the middle ground. *U. Ottawa L. & Tech. J.*, 2:357, 2005.

[53] James R McCall. Misconceptions and reevaluation-polygraph admissibility after rock and daubert. *U. Ill. L. Rev.*, page 363, 1996.

[54] Hamed Monkaresi, Nigel Bosch, Rafael A Calvo, and Sidney K D'Mello. Automated detection of engagement using video-based estimation of facial expressions and heart rate. *IEEE Transactions on Affective Computing*, 8(1):15–28, 2016.

[55] Joëlle Anne Moreno. The future of neuroimaged lie detection and the law. *Akron L. Rev.*, 42:717, 2009.

[56] Thomas Muender, Matthew K Miller, Max V Birk, and Regan L Mandryk. Extracting heart rate from videos of online participants. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4562–4567, 2016.

[57] Bryan Myers and Jack Arbuthnot. Polygraph testimony and juror judgments: A comparison of the guilty knowledge test and the control question test 1. *Journal of Applied Social Psychology*, 27(16):1421–1437, 1997.

[58] United Nations. Universal declaration of human rights, December 1948.

[59] Ian Parker. The story of a suicide. *The New Yorker*, 87(47):36–51, 2012.

[60] Stephanie Perry. Trump and his tweets: Presidential propaganda and its potential influence on the actions of others. 2019.

[61] Edwin J Peterson. Bud lent and doc cambell: Two esteemed justices of the oregon supreme court. *Willamette L. Rev.*, 25:243, 1989.

[62] David C Raskin. The polygraph in 1986: Scientific, professional and legal issues surrounding application and acceptance of polygraph evidence. *Utah L. Rev.*, page 29, 1986.

[63] David C Raskin and Charles R Honts. The comparison question test. 2002.

[64] Richard Rice. Big brother speaks mandarin: Ethnic eradication in xinjiang.

[65] Martha T Roth. Mesopotamian legal traditions and the laws of hammurabi. *Chi.-Kent L. Rev.*, 71:13, 1995.

[66] Peter J Rubin. Square pegs and round holes: Substantive due process, procedural due process, and the bill of rights. *Columbia Law Review*, pages 833–892, 2003.

[67] Seth H Ruzi. Reviving trespass-based search analysis under the open view doctrine: Dow chemical co. v. united states. *NYUL Rev.*, 63:191, 1988.

[68] Aharon Satt, Shai Rozenberg, and Ron Hoory. Efficient emotion recognition from speech using deep learning on spectrograms. In *Interspeech*, pages 1089–1093, 2017.

[69] Richard H Seamon. Kyllo v. united states and the partial ascendance of justice scalia's fourth amendment. *Wash. ULQ*, 79:1013, 2001.

[70] Taylan Sen, Md Kamrul Hasan, Zach Teicher, and Mohammed Ehsan Hoque. Automated dyadic data recorder (addr) framework and analysis of facial cues in deceptive communication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(4):1–22, 2018.

[71] Ric Simmons. The two unanswered questions of illinois v. caballes: How to make the world safe for binary searches. *Tul. L. Rev.*, 80:411, 2005.

[72] Duncan Simpson. California v. greenwood: The pruning of the fourth amendment. *Loy. L. REv.*, 35:549, 1989.

[73] James E Starrs. "a still-life watercolor": Frye v. united states. *Journal of Forensic Science*, 27(3):684–694, 1982.

[74] Sarah E Stoller and Paul Root Wolpe. Emerging neurotechnologies for lie detection and the fifth amendment. *American journal of law & medicine*, 33(2-3):359–375, 2007.

[75] John Synnott, David Dietzel, and Maria Ioannou. A review of the polygraph: history, methodology and current status. *Crime Psychology Review*, 1(1):59–83, 2015.

[76] John Synnott, David Dietzel, and Maria Ioannou. A review of the polygraph: history, methodology and current status. *Crime Psychology Review*, 1(1):59–83, 2015.

[77] Michael N Tennison and Jonathan D Moreno. Neuroscience, ethics, and national security: the state of the art. *PLoS Biol*, 10(3):e1001289, 2012.

[78] Sean Kevin Thompson. A brave new world of interrogation jurisprudence? *American journal of law & medicine*, 33(2-3):341–357, 2007.

[79] Paul V Trovillo. History of lie detection. *Am. Inst. Crim. L. & Criminology*, 29:848, 1938.

[80] Paul V. Trovillo. History of lie detection. *Journal of Criminal Law and Criminology*, 29, 1939.

[81] Michael Wachtel. Give me your password because congress can say so: An analysis of fifth amendment protection afforded individuals regarding compelled production of encrypted data and possible solutions to the problem of getting data from someone's mind. *Pitt. J. Tech. L. & Pol'y*, 14:44, 2013.

[82] Yilun Wang and Michal Kosinski. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, 114(2):246, 2018.

[83] Russell J Weintraub. Voice identification, writing exemplars and the privilege against self-incrimination. *Vand. L. Rev.*, 10:485, 1956.

[84] Sera Whitelaw, Mamas A Mamas, Eric Topol, and Harriette GC Van Spall. Applications of digital technology in covid-19 pandemic planning and response. *The Lancet Digital Health*, 2020.

[85] Lawrence P Wilkins. Introduction: The ability of the current legal framework to address advances in technology. *Ind. L. Rev.*, 33:1, 1999.

[86] Paul Root Wolpe, Kenneth R Foster, and Daniel D Langleben. Emerging neurotechnologies for lie-detection: promises and perils. *The American Journal of Bioethics*, 5(2):39–49, 2005.