Jessica Gabel Cino [a1]

DEPLOYING THE SECRET POLICE: THE USE OF ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM

Algorithms saturate our lives today; from curated song lists to recommending "friends" and news feeds, they factor into some of the most human aspects of decision-making, tapping into preferences based on an ever-growing amount of data. Regardless of whether the algorithm pertains to routing you around traffic jams or finding your next dinner, there is little regulation and even less transparency regarding just how these algorithms work. Paralleling this societal adoption, the criminal justice system now employs algorithms in some of the most important aspects of investigation and decision-making. The lack of oversight is abundantly apparent in the criminal justice system where various algorithm-based tools are now routinely deployed to investigate, prosecute, and sentence offenders. In the absence of suitable safeguards, decisions affecting life and liberty are contained in an impenetrable "black box." [1]

I. Overview

Police agencies, crime labs, courts, and corrections departments around the world use algorithms in a wide range of tools: facial recognition programs, probabilistic DNA genotyping, and bail and sentencing software. These proprietary tools are big business: law enforcement and government agencies license or buy the software *1074 from the private companies that purvey this technology--often on the promise of reduced budget expenditures by removing hours of human work. Once the software is installed, algorithmic outputs are delivered to the operator. For most software running sophisticated algorithms, the end user--often the government--had no hand in writing the code or developing the ultimate product. Thus, a private company owns the software and maintains a fist-hold on the source code (which contains the algorithm), while the purchaser (including the operator) has little to no knowledge as to how the algorithm makes decisions or draws conclusions. [2] This imbalance effectively means that the software's end users lack the ability to see how the software makes decisions. This lack of transparency, in turn, leads to serious consequences.

A. Science in the Courtroom

In the last twenty years, science (in particular, forensic science) has become a mainstay in the criminal justice system. Thousands of guilty defendants have been convicted with the help of forensic techniques. [3] In theory, scientific expert testimony must meet certain standards of reliability before being admitted in court. In federal *1075 court and some state courts, the *Daubert* standard governs the admissibility of such testimony. [4] Under *Daubert*, a judge acts as a gatekeeper and may admit scientific evidence as long as it is both relevant and reliable. [5] Other state courts have continued to follow the earlier *Frye* standard, under which scientific evidence "must be sufficiently established to have

gained general acceptance in the particular field in which it belongs" to be admissible. [6] Despite these roadblocks to admissibility, courts have routinely accepted much of the so-called science underlying forensic testing with little, if any, inquiry. [7] Many forensic techniques, such as hair and fiber analysis, toolmark comparison, and fingerprint analysis, rely upon little more than a matching of patterns wherein a forensic analyst compares a known sample to a questioned sample and makes the highly subjective determination that the two samples originated from the same source. Indeed, what passes as "science" plays a prominent role in many cases because of its easy availability.

Because of this, forensic science's armor has some cracks in it. For example, in 2015, the U.S. Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) formally admitted that almost every examiner in the FBI's microscopic hair unit gave misleading, exaggerated, or otherwise flawed testimony in criminal cases between 1972 and 1999. [8] A cloud of doubt now hangs over cases involving hair evidence, but these cases are not alone. A committee at the National Academy of Science (NAS) concluded in 2009 that "no forensic method has been rigorously shown to have the capacity to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source." [9] *1076 Simply put, the criminal justice system is "sending people to jail based on bogus science." [10]

The President's Council of Advisors on Science and Technology (PCAST) released a report on forensic science in September 2016. [11] While the Council acknowledged the ongoing efforts to improve forensic sciences after the 2009 NAS report, its report also emphasized the significant problems in multiple disciplines of forensic sciences. [12] The PCAST report focused on pattern identification evidence--evidence that requires interpretation by an examiner. [13] The main question asked by PCAST is whether pattern identification evidence is supported by reproducible research. [14]

PCAST suggested a discipline of forensic science must satisfy two types of validity. [15] The first is foundational validity, which means that the discipline is based on research and studies that are accurate and reproducible. [16] The second type of validity is applied validity, which means that the method is reliably applied in practice. [17] Among the disciplines of forensic science PCAST examined, including DNA *1077 analysis, bite marks, latent fingerprints, firearms identification, and footwear analysis, the only valid discipline--using both foundational and applied validity--was single-sourced DNA analysis, discussed below. [18]

Technology presents itself as a powerful tool in criminal investigations, so it is perhaps predictable that as our consumer technology becomes "smarter," so too does our crime-fighting technology. At the same time, efficiency and speed should not be the predominant factors in embracing technology, particularly in the legal field. The integrity of a criminal trial, and its attendant constitutional protections, must be maintained, and a fair trial requires that the evidence presented be relevant, reliable, and not unduly prejudicial. [19]

*1078 *B. Algorithms: Behind the Black Box*

In its most basic form, an algorithm is a series of instructions that tells a computer what to do, similar to a recipe that describes how to make a particular dish. Algorithms can be reduced to three simple operations, not unlike a Westlaw or Lexis search: AND, OR, and NOT. That is the basic premise of an algorithm. Of course, the complexities increase dramatically from those fundamental operating commands. In one way or another, most of these systems are examples of machine learning. Such systems do not just repeat a stable set of instructions; they rewrite themselves as they work and, depending on the software, produce additional algorithms. It is the final output of these "self-authored" programs upon which the end user relies.

Using Google Maps as an example, say that you want to go shopping at a store located about twenty minutes away. Google Maps will use four different algorithms to give you an estimated arrival time: (1) by car; (2) on foot; (3) on a

bicycle; and (4) on public transportation. All four of these algorithms reach the same result--getting you to the store--but each algorithm does so in a completely different way. Each algorithm also has a different cost and a different travel time. The same is true in more sophisticated applications of algorithms. The precise algorithm being used would be difficult to isolate because developers (the humans behind the black box) are unique, and thus, the structure and approach of any algorithm will be unique from one developer to the next. This only adds to the notorious opacity of algorithms and machine learning.

In the criminal justice arena, the touted advantage to using algorithmic software to investigate, prosecute, and sentence offenders is the ability to neuter an otherwise subjective process.[20] The output is meant to be more objective than, for example, a judge, jury, or law *1079 enforcement official. As a result, the twin goals of maximizing public safety and satisfying procedural fairness seem to be met.[21] Although these are certainly laudable goals, the issue remains: an algorithm is a software program that uses specific input to develop a predictive method. A known truism of software development is "garbage in, garbage out," which means that the result coming out is only as good as the data that went in.[22] Applied to software used for criminal justice purposes, this principle indicates that biased input from biased sources will inevitably lead to biased results. For example, failing to control for race in a poorly-optimized algorithm could result in sentencing software that gives black defendants inordinately higher sentences. Similarly, the same algorithm could overcorrect for gender because almost all offenders in prison are male. The sought-after neutrality boasted by algorithmic software is a much more difficult concept to actualize than it is to espouse.

The reality is that no algorithm can perfectly produce the optimal output, and all predictive software will differ. The disparity between the proclaimed advantages of such software and its real-life flaws then creates a tension between constitutional fairness and fighting crime. Moreover, the complexity of algorithms dissuades questions about accuracy; algorithms are perceived or marketed as too difficult to understand for either the individuals using them (criminal justice stakeholders) or for the people they apply to (defendants and prisoners).

II. Development Breakthroughs and Run-Time Errors

The emergence of algorithmic analysis programs creates new problems in a legal system increasingly ill-equipped to keep pace. The software is pricey, but widespread adoption will decrease the costs and will make the programs cheap enough even for smaller *1080 jurisdictions to afford. Some jurisdictions are employing three of these algorithm-based technologies upon which this article will focus: probabilistic DNA genotyping, facial recognition, and sentencing software.

A. Probabilistic Genotyping: Unlocking Pandora's Box

In terms of biology, DNA "is the body's instruction manual."[23] It determines everything about an individual, from height to musical aptitude.[24] Said another way, our DNA determines who we are and makes each one of us a unique being.[25] Not only does our DNA make us unique as individuals, our DNA itself is unique.[26] Other than identical twins, no two people share the same DNA.[27] Because of this distinctive quality, forensic scientists can extract DNA from two samples and determine if the samples have a high likelihood of being from the same source.[28]

From its initial development in the 1980s as an identification tool, the use of DNA in criminal cases--both to convict defendants and exonerate the wrongly convicted--has been prolific. By the 1990s, Congress focused on forensic DNA research and development.[29] As DNA continued to expand its footprint as the ostensible gold standard in criminal investigations, an extraordinary amount of federal funding allocated to crime labs was specifically earmarked for DNA expansion.[30] Because of this, research and development of new DNA analytical techniques was a lucrative business.

Indeed, the abundance in funding for DNA collection, testing, and retention far outstripped other crime lab allotments, despite the fact that DNA analysis only ***1081** represented a small portion of crime lab work at that time.[31] Two decades later, DNA testing is now a primary hub of many labs, forcing other traditional forensic lab departments--such as trace evidence or fingerprints--to cut back or close shop.[32]

1. Great in Theory

DNA remains the gold standard for solving crimes, bolstered by academics and verified by scientific studies and experts around the world. Since the advent of DNA testing, nearly 200 people have been exonerated using newly tested evidence;[33] in some places, courts will only consider exonerations with DNA evidence.[34] Juries, too, have become more trusting of DNA, as evidenced by an increased likelihood of convictions in cases involving DNA evidence.[35] But, as the PCAST report notes, "DNA analysis, like all forensic analyses, is not infallible in practice."[36]

Many errors in DNA analysis are caused by humans: for example, one Texas crime lab was staffed with poorly trained technicians using outdated techniques. Others in Texas were found to be "drylabbing"--reporting results without doing any actual testing--leading to inaccurate results and hundreds, if not thousands, of subsequent appeals from relevant convictions, including at least one capital case.[37] But DNA analysis of complex mixtures--the kind that ***1082** require probabilistic genotype matching--is particularly error-prone. According to the PCAST report, sufficient evidence to establish foundational validity for complex mixtures has not yet emerged.[38]

When the technology was first developed, DNA matching required a significantly intact sample, pure and unpolluted by other bodily fluids, also known as single-source DNA.[39] As technology has improved, more processes, such as probabilistic genotyping, have become available to detect DNA in ultra-miniscule amounts; the DNA left by a finger touching a glass or even the saliva on a cigarette butt is sometimes enough.[40] Probabilistic genotyping can analyze such small amounts of DNA by using the kind of complex code that would be impossible for a human--but not a computer-- to run.[41] These processes can also often parse DNA when samples from multiple people are mixed together.[42] Through probabilistic genotype matching, programs like TrueAllele and STRMIX claim to reliably identify individual DNA strands presented in a multi-contributor or otherwise-dirty biological morass.[43]

The scientifically tested methods of polymerase chain reaction (PCR) and short tandem repeat (STR) differ in several respects from probabilistic genotyping testing, which uses a smaller--sometimes degraded, sometimes mixed-- sample.[44] Probabilistic genotyping thus requires more subjective profile interpretation on the part of an analyst.[45] Profile interpretation is perhaps the most troubling feature ***1083** of probabilistic genotyping because it inherently creates the greatest potential for human error. Profile interpretation involves a hazardous assumption about which alleles are or are not present. Once the profile is compiled by the machine component of the DNA analysis, the forensic scientist must manually interpret that profile.[46] The increased number of amplification cycles injects many variables in the profiles.[47] The forensic scientist interpreting the sample must account for these variables.[48] Thus, different forensic scientists may interpret the resulting profiles differently; this creates a near-impossible hurdle for a criminal defendant to overcome, especially if probabilistic genotyping is the sole DNA evidence used because it is nearly impossible to challenge.

In the early 1990s, much of the work in the DNA field focused on single-source DNA profiles and sought to achieve an exact match between the crime scene sample and the suspect's sample.[49] Later in the 1990s, Cybergenetics, a bioinformation company, began focusing on forensic technology and patented various algorithms that promised to discriminate and separate the presence of individual DNA profiles from a sample that might include several people's biological products.[50] The tool, called TrueAllele, promises an unparalleled advantage in criminal investigations.

TrueAllele's marketing material guarantees its results are free of subjective error and bias.[51] The founder of Cybergenetics quickly became an outspoken advocate and salesman for the tool's use, and by 2009, the first TrueAllele case reached a courtroom.[52] At the end of the day, however, ***1084** Cybergenetics is a business with the goal of making money. Because it is a private, for-profit business, TrueAllele comes with a high price tag. A license to use TrueAllele costs $60,000.[53] But the very thing that makes tools like TrueAllele valuable to courts--their ability to make connections that elude humans--also makes it difficult for those courts to assess the product's validity.

2. Problems in Execution

In 2017, a ProPublica investigation uncovered aspects of the probabilistic software used by New York City forensic labs that might make the results unreliable.[54] As New York forensic labs switched to STRmix--another probabilistic software--a coalition of criminal defense attorneys called for the New York State Inspector General to investigate the lab.[55] Similarly, in 2014, a judge found that STRmix contained coding errors involving certain mixtures of three-person DNA samples, which contributed to misleading results.[56] After the incident, STRmix released the algorithm publicly.[57] But the cofounder of STRmix, John Buckleton, believes the algorithm is far too complex for lawyers to unpack and determine whether the tool is free from error or bias.[58] Keeping the code public may quell critics of the black box but does little to assist in determining what inputs were used in its programming.[59]

TrueAllele is under the microscope more than ever before. Attorneys representing Billy Ray Johnson, a currently incarcerated ***1085** man who claims he was wrongfully convicted based on evidence processed by TrueAllele, are not so quick to accept Cybergenetics' assurances of accuracy.[60] In a newsletter, Cybergenetics writes about the Johnson case, saying that TrueAllele obtained results for eight samples where other methods found the results "inconclusive."[61] This should give anyone pause. But the newsletter further states that guilty pleas regularly follow TrueAllele's interpretation of previously inconclusive DNA samples.[62] This has caused the American Civil Liberties Union (ACLU) to intervene. As the ACLU indicates in its amicus brief for Johnson, the companies writing and selling algorithms like TrueAllele often serve the prosecution as their primary client, and--whether explicitly stated or not--that client is often best satisfied with more matches.[63] With such an incentive structure in place, it may be naïve to take Cybergenetics' assertions at face value.

Further, Johnson's lawyers argue that the source code is crucial to their defense even if TrueAllele's motives are entirely benign.[64] The claim that any algorithmic software such as TrueAllele is able to make decisions entirely detached from human bias is not based in reality.[65] From the bottom up, an algorithm must interpret large amounts of data and quantify the relevance of each piece; such a process is largely subjective, and algorithms merely apply a uniform level of subjectivity across the board.[66] In addition to built-in human bias, almost all software carries an expected number of programming ***1086** errors in the source code.[67] Even conservative estimates suggest that more than a dozen material errors are hidden amongst TrueAllele's thousands of lines of code.[68]

Johnson's case is just one of many that used TrueAllele or similar systems from other developers that promise their proprietary software will reveal all the secrets of DNA. But Johnson's lawyers--along with the ACLU, the Electronic Frontier Foundation, and the Northern California Innocence Project--are making the case that the trial court's decision not to allow defense experts to examine the source code prevented Johnson from receiving a fair trial.[69] Jennifer Friedman, the forensic expert for the Los Angeles Public Defender's Office, which also submitted a brief in the Johnson trial, compared the shift from single-source DNA to probabilistic DNA analysis to the difference between algebra and calculus.[70]

In trial documents in other cases, TrueAllele's front man Mark Perlin argues that allowing others to see his company's source code would violate his right to a trade secret and ultimately threaten his business.[71] He casts unlocking the code as unnecessary because his company performs its own quality control.[72] Perlin complains that the ACLU (and others) are just trying to "sow[] confusion" over an "unbiased system."[73]

Despite Cybergenetics' apparent dread of being compelled to reveal its trade secret, TrueAllele recently promised to make the code accessible to defense attorneys for a mere $10,000, plus $2,000 a day.[74] This "generosity" is entirely self-serving--it preserves ***1087** Cybergenetics' profit margin while shortchanging defendants who lack the financial resources to afford such a measure.

In October, the Department of Commerce's National Institute of Standards and Technology (NIST) announced that it would embark on a study to determine the reliability of DNA testing, including the algorithmic methods used by companies like TrueAllele.[75] Expectedly, Perlin condemned this research, which NIST says serves to establish foundational validity (something the PCAST report noted has been lacking) of the methodology.[76] Perlin met this announcement with hostility aimed at external peer review (a foundational requisite for scientific validation) and derided the study as a governmental attack on science.[77] Perlin vehemently argued that prior scientific, peer-reviewed research studies had verified TrueAllele's validity.[78] Of course, the studies that Perlin relied on were self-serving, internal validation studies sponsored and conducted by Cybergenetics.[79]

The chief DNA scientist at NIST, Dr. John Butler, is a preeminent DNA expert[80] who understands the issues related to probabilistic DNA analysis. Butler explained that the NIST study focused on measuring and evaluating differentiations in software responses.[81] ***1088** Dr. Mike Coble at NIST, an expert on forensic sciences who has published his own studies on probabilistic genotyping,[82] explained that NIST's research focused on the practice of mixture evaluations as a whole rather than on individual companies.[83] Coble explained that the study is aimed at education across the criminal justice system--lawyers, judges, and juries: "There's a real hunger and desire to understand what's going on in that box, what the program is doing[,] and how does it do this."[84]

Information and transparency is sorely needed, but is it enough? Even the best defense lawyers may lack the resources and foundational knowledge needed to parse the nuances of the technology into flaws. Beyond the resource gap is the fundamental issue of a criminal defendant's right to due process. TrueAllele could be garbage or gospel, but that should not change a defendant's right to see what is in the box that could put him or her away for life.[85]

B. Facial Recognition Software

The Trump administration's efforts to impose new immigration rules drew attention--and legal fire--for restrictions placed on the ability of people born in certain majority Muslim countries to enter the U.S.[86] In the frenzy of concern, one obscure provision of the executive orders was given little attention: an expansion of facial recognition systems in major U.S. airports to monitor people leaving the U.S. in hopes of catching individuals who have overstayed their visas or are wanted in criminal investigations.[87]

*1089 This type of facial recognition is essentially a much more powerful version of the same type of technology your phone or computer might use to identify friends in your photos, and the possible applications are extensive.[88] Using computers to recognize people's faces and validate their identities can streamline access control for secure corporate and government buildings or devices.[89] Some systems can identify known or suspected criminals.[90] Businesses can analyze

their customers' faces to help tailor marketing strategies to people of different genders, ages, and ethnic backgrounds. [91] Even some consumer product companies are taking advantage of facial recognition technology through services such as virtual eyeglass fitting. [92]

Serious privacy concerns are also raised as government agencies and companies are better able to track individuals through their communities and even around the world. The facial recognition market is currently worth approximately $4 billion and is expected to grow to more than $7 billion by 2022. [93] Surveillance is a large reason for growth, and government entities are the primary consumers in the market. [94] The FBI has a database with images of approximately half the U.S. population. [95] Some commentators have expressed fear of **1090** people using facial recognition to engage in online harassment or even real-world stalking. [96]

As facial recognition becomes more common, we must know how it works. As someone who studies and researches the legal implications of new technology in criminal investigations, I believe it is important to understand what it can and cannot do and how the technology is progressing. Only then can we have informed discussions about when and how to use computers to recognize that most human of features--our faces.

1. Great in Theory

As one of several methods of what are called "biometric" identification systems, facial recognition examines physical features of a person's body in an attempt to uniquely distinguish one person from all the others. [97] Other forms of this type of work include fingerprint matching, retina scanning, and even voice recognition. [98] All of these systems take in data--often an image--from an unknown person, analyze the data in that input, and attempt to match the individual to existing entries in a database of known persons' faces or voices. [99] Facial recognition does this in three steps: detection, faceprint creation, and verification or identification. [100]

1091 When an image is captured, computer software analyzes it to identify where the faces are in, say, a crowd of people. [101] In a mall, for example, security cameras will feed into a computer with facial recognition software to identify faces in the video feed. [102] Once the system has identified any potential faces in an image, it looks more closely at each face. [103] Sometimes the image must be reoriented or resized. [104] A face very close to the camera may seem tilted or stretched slightly; someone farther from the camera may appear smaller or even partially hidden from view. [105]

When the software has arrived at a proper size and orientation for the face, it looks even more closely, seeking to create what is called a faceprint. [106] Much like a fingerprint record, a faceprint is a set of characteristics that, taken together, uniquely identify one person's face. Elements of a faceprint include the relative locations of facial features such as eyes, eyebrows, and nose shape. [107] A person who has small eyes, thick eyebrows, and a long narrow nose will have a very different faceprint from someone with large eyes, thin eyebrows, and a wide nose. Eyes are a key factor in accuracy. [108] Large dark sunglasses are more likely to reduce the accuracy of the software than facial hair or regular prescription glasses. [109]

A faceprint can be compared with a single photo to verify the identity of a known person, such as an employee seeking to enter a **1092** secure area. [110] Faceprints can also be compared to databases of many images in hopes of identifying an unknown person. [111]

2. Problems in Execution

Lighting is a key factor affecting how well facial recognition works. [112] An evenly lit face seen directly from the front, with no shadows and nothing blocking the camera's view, is best. [113] In addition, whether an image of a face contrasts well with its background, and how far away it is from the camera, can help or hurt the facial recognition process. [114] Uneven light, a bad angle, or a strange expression can cause facial recognition to fail. [115]

Another very important challenge to successful facial recognition is the degree to which the person being identified cooperates with--or is even aware of--the process. People who know they are using facial recognition, such as the employee trying to access a restricted room, are relatively easy to work with. [116] They know to look directly at the camera in proper lighting to make conditions optimal for the software analysis. [117] Others do not know their faces are being analyzed and may not even know that these systems are surveilling them at all. Images of their faces are trickier to analyze; a face picked out of a crowd may have to be digitally transformed and zoomed in on before the software can generate a faceprint. [118] That leaves more room for the system to misidentify the person. [119]

When a facial recognition system incorrectly identifies a person, the misidentification can cause a number of potential problems depending on what kind of error has occurred. A system restricting *1093 access to a specific location could wrongly admit an unauthorized person--if, say, she were wearing a disguise or even just looked similar enough to someone who should be allowed in. Or it could block the entry of an authorized person by failing to correctly identify her.

In law enforcement, surveillance cameras cannot always obtain good-quality images of a suspect's face. That could mean identifying an innocent person as a suspect or even failing to recognize a known criminal who ran afoul of the law again. Regardless of how accurate facial recognition appears to be on television crime dramas, room for error exists, although the technology is improving. The NIST has estimated that stated error rates are declining by 50% every two years, and tests show they are currently around 0.8%. [120] That is better than voice recognition, which has error rates above 6%. [121] But facial recognition may still be more error-prone than iris scanning and fingerprint scanning. [122]

Even if it is accurate, however, facial recognition raises privacy concerns-- perhaps even more so as accuracy improves. [123] One of the chief worries is that, much like the rise of DNA databases, facial features and photos are being warehoused by government agencies, enabling them to track people and erase any notion of privacy or anonymity. [124] New privacy issues are cropping up all of the time. A new smartphone app, FindFace, allows people to take a person's photo and use facial recognition to find their social media accounts. [125] Ostensibly a convenient way to connect with friends and *1094 coworkers, the app invites misuse. People can use it to expose identities and harass others. [126]

These new capabilities also raise concerns about other malicious uses of publicly available images. For example, when police issue alerts about missing children, they often include a photograph of the child's face. There is little regulation or oversight, so nobody knows whether those images are also being entered into facial recognition systems. [127] This, of course, does not even delve into issues such as using facial recognition tools along with other technologies, including police body cameras, geolocation software, and machine learning to assist in real-time tracking. [128] That goes beyond simple identification and into the realm of where someone has been and where the software predicts that person will go. Combining technologies offers attractive options for crime fighting and deepens the fissures in our privacy.

C. Sentencing Software: Prepackaged Risk Assessment

Risk and Needs Assessment (RNA) is another iteration in the criminal justice system's continued goal of managing increasing incarceration rates with a limited budget through the use of technological advancements. RNA's original iteration, the selective incapacitation movement, started in the 1980s mostly as a criminal justice theory. [129] The concept behind the theory was to identify and *1095 incarcerate individuals prone to violence or recidivism for longer periods, thereby leading to an overall reduction in the crime rate. [130] As with many new, innovative systems, the selective incapacitation system had serious flaws--the most notable of which were its incredibly high false positive rates, which mistakenly identified between fifty-four and ninety-nine percent of participating individuals as "dangerous." [131]

Although the theory of selective incapacitation was quickly abandoned, its core concepts took root in legal literature, the broad theory being refined into the utilitarian goal of decreasing the crime rate by imprisoning the most dangerous felons while reducing mass incarceration. [132] The American system shifted to using clearer sentencing practices and increased the use of sentencing guidelines, culminating in Congress passing the Sentencing Reform Act (SRA) in 1984, from which the federal sentencing guidelines are derived. [133] The main theory behind the SRA was that sentencing practices had become unfair and uncertain under the rehabilitative model; thus, the U.S. Sentencing Commission formalized federal sentencing. [134]

1. Great in Theory

With a methodological and testable system instead of a purely theoretical conception, an evidence-based "risk/needs assessment" was at least ready to be tested out in practice and implemented into the sentencing process. [135] As of 2014, at least twelve states had integrated some form of RNA tool into their sentencing procedures through legislation, state sentencing policy, or a state supreme court *1096 decision. [136] The process, as applied to the criminal justice system, focuses on grouping offenders as low, medium, or high-risk offenders; sentencing and treatment guidelines are assigned based on these groupings. [137]

Although each RNA model uses its own algorithm or gives different weight to an offender's risk factors, the models generally try to embrace rehabilitation while still providing the standards and predictability of the retributive philosophy. [138] Furthermore, most RNA tools are based on the risk-needs-responsivity model (RNR), which itself is based on the three eponymous principles: the risk principle, which asserts that risk is predictable and offenders should be treated differently based on the risk grouping; the needs principle, which purports that rehabilitation and sentencing should be based on the needs that contribute to criminal behavior; and the responsivity principle, which describes how treatments should respond to each specific offender. [139]

Perhaps the most comprehensive categorization of the goals pursued by RNA tools is to (1) reduce judicial disparity; (2) promote consistent sentencing; (3) prioritize and allocate correctional resources; (4) adjust punishments for certain categories of offenders; (5) reduce prison overcrowding; and (6) encourage the use of non-incarceration sanctions. [140] Still, it is possible that different tools use modified or completely different principles, and depending on the system's algorithmic confidentiality, it may be impossible to know exactly what principles a specific tool prioritizes when determining an offender's risk group and ultimate sentence.

For example, the Northpointe Institute for Public Management's Correctional Offender Management Profiling for Alternative *1097 Sanctions--better known as COMPAS--was developed in 1998 and was last updated in 2005. [141] COMPAS is currently being used by departments of corrections and rehabilitation in California, Michigan, New Mexico, New York, South Carolina, Wisconsin, and Wyoming. [142] It is worth noting that only corrections departments have used COMPAS in their procedures, while courts have either been disallowed from using it or unimpressed by its results. [143]

Due to this system's prolific use, however, and its use as evidence in the fairly recent *Loomis* case, discussed below, the system will be evaluated on its merits as a decision-making tool for judges as well as for corrections officers.

COMPAS contains 43 separate scales formed from 135 risk items, which can be mixed and matched to different offender populations at different points of the criminal justice system to make a custom-built risk assessment for the particular department in question. [144] The risk items and scales are picked and formed by instrument developers, reflecting the fact that COMPAS is a company secret and that most of its algorithmic methodology is unknown. [145] The creators, however, do assert that their risk and needs factors include the eight normative subgroups that are utilized by many other risk analysis systems. [146] Although COMPAS still keeps its precise methodology and algorithm as a trade secret, this alignment with similar systems gives scholars a reference point as to COMPAS's approach.

It bears noting that, at least in Wisconsin courts, COMPAS must include the following five written warnings to judges reviewing a case with the assistance of a COMPAS risk score readout: (1) the ***1098** proprietary nature of COMPAS prevents the disclosure of how the risk scores are formulated; (2) COMPAS risk scores cannot identify specific high-risk offenders due to its scores being derived from group data; (3) COMPAS relies on a national data sample and has not been cross-validated with a Wisconsin population; (4) studies have warned that COMPAS disproportionately classifies minority offenders as having a higher risk of recidivism; and (5) COMPAS was developed specifically to help correctional departments in *post*sentencing determinations. [147] Despite these warnings, particularly the fifth warning, Wisconsin courts are allowed to take risk scores into consideration during presentencing determinations, and any legal and constitutional objections raised have proven unsuccessful to bar the use of risk scores. [148]

2. Problems in Execution

This leads to an underlying, pervasive ambiguity regarding the quintessential measuring factor of all RNA tools, calling their effectiveness into question. With such an imprecise measure of the core assessment standards of RNA tools, the system seems to function as junk science protected behind the wizard's curtain. This assessment is supported by a recent study which found that crowdsourced predictions from a random survey were *more accurate* at predicting rates of recidivism than those from COMPAS, even though the survey-takers based their decisions off only two factors (COMPAS uses 137 inputs, including 6 risk factors in its assessment). [149] Yet, the lack of an empirically watertight basis is not enough to discard a system from the court of law, as expressed by the ***1099** Supreme Court in *Heller v. Doe* when it said, "[t]he problems of government are practical ones and may justify, if they do not require, rough accommodations-- [however] illogical, it may be, and unscientific." [150] On this point, courts across the nation have been clear: just because the system is incapable of scientifically identifying with certainty an individual's chance of recidivism does not by itself invalidate the use of RNA tools in the sentencing process. [151]

The RNA algorithms lack the ability to control for several contingent factors. For example, the tendency of the tools to overrate male minorities over other offenders should automatically be a red flag. Some studies suggest that such factors cannot be controlled for, and the use of RNA tools will only aggravate the prison population's racial imbalance. [152] This capacity for algorithmic software to develop racial prejudices is well-documented. [153] For example, at first glance, Microsoft's @TayTweets, a quirky artificial intelligence-based Twitter account that learned to produce racist responses in conversation after less than twenty-four hours of live interaction with the Twitter universe, seemed like a comical mistake. [154]

When the same principle applies to RNA programs that commonly learn the same prejudices and consequently issue disproportionate recommendations or assessments to defendants of color, however, it is time to stop laughing. [155] Harsher critics point out that prior criminal history is merely a proxy for race and that the adoption of RNA tools would

exacerbate such an issue.[156] Professor Bernard *1100 Harcourt, in a forthcoming paper, examines previous actuarial assessments of the criminal population to tackle high rates of incarceration, including such assessments as early selective incapacitation, which resulted in a sharp increase in black representation in detention and incarceration.[157] Harcourt further notes that, as RNA tools have developed and evolved, the number of factors considered, as well as the increased focus on prior criminal history as a main factor in evaluation, has led to the further unequal targeting of blacks over other races.[158]

Gender is another difficult measurement factor, although for different reasons. Usually dismissed as a verified correlation, there are recognized and significant gender disparities in recidivism rates and rehabilitation potential.[159] The case cited in the *Loomis* decision, *Craig v. Boren*, stands as a seminal case concerning the unconstitutionality of using gender discrimination in lawmaking; however, like in *Loomis*, courts have often not considered the statistical use of gender in actuarial studies as an unconstitutional procedure.[160] As such, gender as a factor in RNA tools remains permissible, with any potential constitutional issues placated, if it is sufficiently reinforced with proper statistical evidence.

Subjective bias in judicial decisions setting bail or sentences should obviously be avoided, but no magic switch can be flipped to resolve the problem. RNA software is constructed by imperfect people, and their prejudices often spill over into their work despite even the best intentions. As that same software executes machine learning, the potential for substantial unfairness increases with its level of exposure. Although RNA software is promoted as a shift from biased practices to objective decision-making, without greater transparency and scrutiny, it merely hides the same biases from public view without diminishing their influence.

*1101 CONCLUSION

Algorithms are becoming an integral part of the criminal justice system, ultimately influencing a person's decision on the freedom or incarceration of a defendant. Algorithms are complex, difficult to understand, and often a mystery to pull apart, understood only by the company selling the algorithmic program. Currently, most are protected behind the cloak of trade secret, despite Confrontation Clause and other constitutional concerns.

In the end, the parties using algorithms in their decision-making processes must rely on the assumption that the programs' creators balanced public safety and fairness to ethical levels. Basic machine learning techniques are already being used in the criminal justice system. Further, the not-far-off role of artificial intelligence in our courts creates two potential paths for the criminal justice and legal communities: either blindly allow the march of technology to go forward, or create a moratorium on the use of opaque technologies in criminal justice risk assessment until processes and procedures allowing for a meaningful examination of these tools are in place.

The legal community has never fully discussed the implications of algorithmic tools. Now, attorneys and judges are grappling with the lack of oversight and the impact of these tools after their proliferation. To hit pause would allow courts time to create rules governing how algorithmic software can and should be used. It would give policymakers the window necessary to create standards and provide a mechanism for oversight. Finally, it would allow educational and advocacy organizations time to teach attorneys how to properly handle these novel tools in court.

These steps can reinforce the rule of law and protect individual rights. We should remember Melvin Kranzberg's first law of technology: it is neither good nor bad, but it certainly is not neutral.[161] His sixth law of technology is equally relevant: *1102 "Technology is a very human activity."[162] To blindly accept these algorithm-driven technologies in our courts without a plan is to defer to machines in a way that should make any advocate of judicial or prosecutorial discretion uncomfortable. Technology provides powerful tools, but the law is often ill-equipped to keep pace with new

developments. If we are to use these technologies when life and liberty are at stake, we must engage with its possibilities and its detriments and understand the issues of accuracy, fairness, and ethics these new capabilities raise.

Footnotes

a1   Professor of Law, Georgia State University College of Law. I would like to thank my two intrepid research assistants, Michael Duffey and Erik Badia, for their heavy lifting in bringing this article to publication.

1   The phrase "black box" commonly refers to the actions companies take to keep the source code containing the algorithm and related programming features secret. *See* Tom Simonite, *AI Experts Want to End 'Black Box' Algorithms in Government*, WIRED (Oct. 18, 2017, 3:00 PM), https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/ [https://perma.cc/UPA6-SJ4G].

2   Some software relies on a machine learning platform. *See, e.g.*, Ben Schreck et al., *Getting Value from Machine Learning Isn't About Fancier Algorithms--It's About Making It Easier to Use*, HARV. BUS. REV. (Mar. 6, 2018), https://hbr.org/2018/03/getting-value-from-machine-learning-isnt-about-fancier-algorithms-its-about-making-it-easier-to-use [https://perma.cc/3DXW-BV44]. The source code defines the machine learning algorithm, which then compiles the actual algorithm on prior input and converts it to output. *Id.* For example, in Google Maps, the source code doesn't code the route; instead, the source code accumulates data inputs from millions of users and forms a predictive model (an algorithmically generated algorithm) to route the driver to the desired destination. *See generally* Ravi Sharma, *How Google Maps Gets Its Remarkably Accurate Real-Time Traffic Data*, GADGETS360 (Mar. 2, 2017), https://gadgets.ndtv.com/apps/features/how-google-maps-gets-its-remarkably-accurate-real-time-traffic-data-1665385 [https://perma.cc/GN28-WWHG].

3   Jessica D. Gabel & Margaret D. Wilkinson, *Good Science Gone Bad: How the Criminal Justice System Can Redress the Impact of Flawed Forensics*, 59 HASTINGS L.J. 1001, 1002 (2008). At the same time, the Innocence Project estimates that forensic evidence with little to no probative value caused or contributed to a wrongful conviction in at least eighty DNA exoneration cases the Project has evaluated. *Id.*; *see also DNA Exonerations in the United States*, INNOCENCE PROJECT, http://www.innocenceproject.org/dna-exonerations-in-the-united-states/ [https://perma.cc/3GM8-CK7W] (last visited May 15, 2018) (reporting that 45% of the Innocence Project's 356 DNA exonerations "[i]nvolved misapplication of forensic science").

4   Daubert v. Merrill Dow Pharms., Inc., 509 U.S. 579, 597 (1993).

5   *Id.*

6   Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923); People v. Geier, 161 P.3d 104, 142 (Cal. 2007).

7   *See, e.g.*, Johnson v. Commonwealth, 12 S.W.3d 258, 263-64 (Ky. 1999).

8   Spencer S. Hsu, *FBI Admits Flaws in Hair Analysis Over Decades*, WASH. POST (Apr. 18, 2015), http://wapo.st/1OrujpH?tid=ss_tw-bottom&utm_term=.17d035df6e5a [https://perma.cc/2LN4-JX5E].

9   NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 7 (2009). In recent years, studies of certain forensic fields have demonstrated a lack of scientific foundation in testing methods, identified serious flaws, and questioned the continued use of such techniques. *See* INNOCENCE PROJECT ARSON REVIEW COMM., REPORT ON THE PEER REVIEW OF THE EXPERT TESTIMONY IN THE CASES OF *STATE OF TEXAS V. CAMERON TODD WILLINGHAM* AND *STATE OF TEXAS V. EARNEST RAY WILLIS* 40 (2006) ("The significant lack of understanding of the behavior of fire ... can and does result in significant misinterpretations of fire evidence, unreliable determinations, and serious miscarriages of justice with respect to the crime of arson."); NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., BALLISTIC IMAGING 3 (Daniel L. Cork et al. eds., 2008) ("The validity of the fundamental assumptions of uniqueness and reproducibility of firearms-related toolmarks has not yet been fully demonstrated.").

10   Kelly Servick, *Reversing the Legacy of Junk Science in the Courtroom*, SCI. MAG. (Mar. 7, 2016, 4:30 PM), http://www.sciencemag.org/news/2016/03/reversing-legacy-junk-science-courtroom [https://perma.cc/AD3E-LZG7].

11   PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS at x (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf [https://perma.cc/9XKM-TLG5] [hereinafter PCAST REPORT].

12   *See id.* at 1-20 (summarizing the Council's findings and recommendations).

13   *Id.* at 1. Examples of such methods include the analysis of DNA, hair, latent fingerprints, firearms and spent ammunition, toolmarks and bitemarks, shoeprints and tire tracks, and handwriting. *Id.*

14   *See id.*

15   *Id.* at 4-5.

16   PCAST REPORT, *supra* note 11, at 4-5.

17   *Id.*

18   *Id.* at 7-14. The PCAST report received criticism for its findings, most notably from those on the prosecutorial side of the aisle. *See, e.g.*, Press Release, Nat'l Dist. Attorneys Ass'n, National District Attorneys Association Slams President's Council of Advisors on Science and Technology Report (Sept. 2, 2016), http://www.ndaa.org/pdf/NDAA%20Press%C20Release%C20on%C20PCAST%20Report.pdf [https://perma.cc/78ME-W4TC]. PCAST responded in detail, noting: "Forensic science is at a crossroads. There is growing recognition that the law requires that a forensic feature-comparison method be established as scientifically valid and reliable before it may be used in court and that this requirement can only be satisfied by actual empirical testing." PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, AN ADDENDUM TO THE PCAST REPORT ON FORENSIC SCIENCE IN CRIMINAL COURTS 9 (2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensics_addendum_finalv2.pdf [https://perma.cc/6NTR-U2VW]. PCAST also encouraged forensic science to be the author of its own destiny. *Id.*

19   William C. Thompson, The Potential for Error in Forensic DNA Testing (and How That Complicates the Use of DNA Databases for Criminal Identification) 2 (Aug. 12, 2008) (unpublished paper), http://www.councilforresponsiblegenetics.org/pageDocuments/H4T5EOYUZI.pdf [https://perma.cc/ML9J-EK99]. Indeed, there is recent and ongoing precedent for such a practice. The so-called psychopath test is often dispositive as to matters of parole and influential as to sentencing. Alix Spiegel, *Can a Test Really Tell Who's a Psychopath?*, NPR (May 26, 2011, 2:24 PM), http://www.npr.org/2011/05/26/136619689/can-a-test-really-tell-whos-a-psychopath. [https://perma.cc/DV9U-5VE9]. The test has even influenced whether the death penalty is administered. *Id.* This use of the test remains pervasive--even though the test's creator has expressed concern over the practice. Ira Glass et al., *The Psychopath Test*, THIS AM. LIFE (May 27, 2011), https://www.thisamericanlife.org/radio-archives/episode/436/the-psychopath-test [https://perma.cc/XC8W-P4PV] (interviewing Bob Hare, the test's creator).

20   *See*DANIELLE KEHL ET AL., ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM: ASSESSING THE USE OF RISK ASSESSMENTS IN SENTENCING 6 (2017), https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf?sequence=1 [https://perma.cc/A5QD-YERJ].

21   Sam Corbett-Davies et al., *Algorithmic Decision Making and the Cost of Fairness*, 23 SIGKDD CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 797, 797 (2017), http://www.kdd.org/kdd2017/papers/view/algorithmic-decision-making-and-the-cost-of-fairness [https://perma.cc/7KUK-XWFE] (click link below abstract to download full article).

22   L.J. KUTTEN & FREDERIC M. WILF., 3 COMPUTER SOFTWARE § 12:55 (2017).

23   D.P. LYLE, FORENSIC SCIENCE 179 (2012).

24   *Id.*

25   *Id.*

26   *See id.*

27   *Id.*

28   *Id.* at 187-88.

29   Jessica Gabel Cino, *Tackling Technical Debt: Managing Advances in DNA Technology That Outpace the Evolution of Law*, 54 AM. CRIM. L. REV. 373, 373 (2017).

30   *Id.*

31   *Id.*

32   *Id.*

33   *Exonerations by Year: DNA and Non-DNA*, NAT'L REGISTRY OF EXONERATIONS (2018), https://www.law.umich.edu/special/exoneration/Pages/Exoneration-by-Year.aspx [https://perma.cc/YE5W-LV85].

34   *See* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of State Statutes and Rules Governing Requests for Postconviction DNA Testing*, 72 A.L.R.6th 227 (2012).

35   Joseph L. Peterson et al., *Effect of Forensic Evidence on Criminal Justice Case Processing*, 58 J. FORENSIC SCI. S78, S80 (2013).

36   PCAST REPORT, *supra* note 11, at 7; *see also* Matthew Shaer, *The False Promise of DNA Testing*, ATLANTIC (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/ [https://perma.cc/EA2U-2YBW].

37   Eric Dexheimer, *Austin Crime Lab Bucked DNA Standard for Years, Yet Got Passing Grades*, AUSTIN AM.-STATESMAN (Jan. 12, 2017, 11:45 AM), https://www.mystatesman.com/news/crime--law/austin-crime-lab-bucked-dna-standard-for-years-yet-got-passing-grades/MZBboOfzXWWgqlem6867TO/ [https://perma.cc/KB2K-DGYF]; Chuck Lindell, *Court: Examine If Austin Crime Lab Botched Death Penalty Evidence*, AUSTIN AM.-STATESMAN (Oct. 18, 2017, 2:14 PM), https://www.statesman.com/news/court-examine-austin-crime-lab-botched-death-penalty-evidence/Fue0LIlp74CTWSUXoSrXuO/ [https://perma.cc/9DGR-FQV3].

38   PCAST REPORT, *supra* note 11, at 8.

39   *Id.* at 70.

40   *The Problem of Probabilistic Genotyping*, FORENSIC INST. (Apr. 2017), http://www.theforensicinstitute.com/news-articles/views-and-opinions/dna-interpretation-software [https://perma.cc/5BB5-XVNW].

41   *Id.*

42   *Id.*

43   Mark W. Perlin et al., *TrueAllele Genotype Identification on DNA Mixtures Containing Up to Five Unknown Contributors*, 60 J. FORENSIC SCI. 857, 857 (2015).

44   Frederick R. Bieber et al., *Evaluation of Forensic DNA Mixture Evidence: Protocol for Evaluation, Interpretation, and Statistical Calculations Using the Combined Probability of Inclusion*, 17 BMC GENETICS 1, 1-4 (2016).

45   People v. Megnath, 898 N.Y.S.2d 408, 413 (Sup. Ct. 2010).

46   Bruce Budowle et al., *A Perspective on Errors, Bias, and Interpretation in the Forensic Sciences and Direction for Continuing Advancement*, 54 J. FORENSIC SCI. 798, 803-04 (2009).

47   *Id.*

48   *Id.*

49   Jessica Pishko, *The Impenetrable Program Transforming How Courts Treat DNA Evidence*, WIRED (Nov. 29, 2017, 7:00 AM), https://www.wired.com/story/trueallele-software-transforming-how-courts-treat-dna-evidence [https://perma.cc/RF5E-6VFF].

50   *Id.*

51   LAW SERVICES, CYBERGENETICS, https://www.cybgen.com/solutions/brochures/law_brochure.pdf [https://perma.cc/23YX-MANE] (last visited May 12, 2018).

52   Pishko, *supra* note 49.

53   *Id.*

54   Lauren Kirchner, *Thousands of Criminal Cases in New York Relied on Disputed DNA Testing Techniques*, PROPUBLICA (Sept. 4, 2017, 6:00 PM), https://www.propublica.org/article/thousands-of-criminal-cases-in-new-york-relied-on-disputed-dna-testing-techniques [https://perma.cc/49SV-MZTL].

55   *Id.*

56   David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, COURIER-MAIL (Mar. 20, 2015, 8:00 AM), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b [https://perma.cc/NBG5-PUKW].

57   Pishko, *supra* note 49.

58   *Id.*

59   *Id.*

60   Vera Eidelman, *Secret Algorithms Are Deciding Criminal Trials and We're Not Even Allowed to Test Their Accuracy*, AM. CIVIL LIBERTIES UNION (Sept. 15, 2017, 2:00 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-algorithms-are-deciding-criminaltrials-and [https://perma.cc/F8Z7-UKQ8].

61   Jeffrey K. Robinson, *Cybergenetics June/July 2015 Newsletter* (2015), http://www.duq.edu/assets/Documents/forensics/CybgenNewsJuneJuly2015.pdf [https://perma.cc/EJ84-GVLS].

62   *Id.*

63   Brief of Amici Curiae Am. Civil Liberties Union & Am. Civil Liberties Union S. Cal. in Support of Defendant-Appellant Seeking Reversal at 15-16, California v. Johnson, No. F071640 (Cal. Ct. App. Sept. 14, 2017).

64   *Id.* at 22.

65   *Id.* at 12.

66   *Id.* at 12-13.

67   *Id.* at 15.

68   *Id.*

69   Brief of Amici Curiae, *supra* note 63, at 29.

70   Pishko, *supra* note 49.

71   Findings of Fact and Conclusions of Law on Defense Motion to Compel Cybergenetics' TrueAllele Casework Source Code at 5, Washington v. Fair, No. 10-1-09274-5 (Wash. Super. Ct. Jan. 12, 2017).

72   *Id.*

73   Press Release, Cybergentics, ACLU Zealots March Against Truth-Seeking DNA Technology (Sept. 19, 2017), https://www.cybgen.com/information/newsroom/2017/sep/ACLU-zealots-march-against-truth-seeking-DNA-technology.shtml [https://perma.cc/CAU7-7S8E].

74   *See* Pishko, *supra* note 49.

75   *NIST to Assess the Reliability of Forensic Methods for Analyzing DNA Mixtures*, NAT'L INST. OF STANDARDS & TECH. (Oct. 3, 2017), https://www.nist.gov/news-events/news/2017/10/nist-assess-reliability-forensic-methods-analyzing-dna-mixtures [https://perma.cc/PRP4-5JXF].

76   *Id.*; *see also* Press Release, Cybergenetics, NIST Launches Wasteful Study That Undermines Science and Justice (Oct. 5, 2017), https://www.cybgen.com/information/newsroom/2017/oct/NIST-launches-wasteful-study-that-undermines-science-and-justice.shtml # [https://perma.cc/4BCV-SXTY].

77   Press Release, *supra* note 76; *see also* NAT'L INST. OF STANDARDS & TECH., VALIDATION STANDARDS FOR PROBABILISTIC GENOTYPING SYSTEMS 8-9 (2016), https://www.nist.gov/sites/default/files/documents/2017/10/13/validation_standards_for_probabilistic_genotyping_systems_3.pdf [https://perma.cc/83RM-9NQA].

78   TrueAllele, *Virginia TrueAllele Validation Study: Casework Comparison*, YOUTUBE (Oct. 6, 2015), https://www.youtube.com/watch?v=jS4tHVkb87k&feature=youtu.be [https://perma.cc/VPY9-KFMD].

79   *Id.*; TrueAllele, *Practical Aspects of the Implementation of TrueAllele Casework*, YOUTUBE (July 29, 2015), https://www.youtube.com/watch?v=8Qoetze3fkE [https://perma.cc/4GTG-5JNX].

80   *John Butler*, NAT'L INST. OF STANDARDS & TECH. (Apr. 4, 2017), https://www.nist.gov/people/john-butler [https://perma.cc/D8EL-TM2R].

81   Lauren Kirchner, *Putting Crime Scene DNA Analysis on Trial*, PROPUBLICA (Oct. 11, 2017, 8:00 AM), https://www.propublica.org/article/putting-crime-scene-dna-analysis-on-trial [https://perma.cc/7EQU-F3ST].

82   *See Michael Coblei*, NAT'L INST. OF STANDARDS & TECH., https://strbase.nist.gov/Coble.htm [https://perma.cc/46YD-ZNR8] (last visited Apr. 4, 2018).

83   Pishko, *supra* note 49.

84   *Id.*

85   *Id.*

86   Laura Jarrett, *Trump Administration Appealing Halt of Revised Travel Ban*, CNN (Mar. 30, 2017, 6:15 PM), https://www.cnn.com/2017/03/29/politics/hawaii-trump-travel-ban-extended [https://perma.cc/A5WU-HGVJ]; *Trump's Executive Order on Immigration, Annotated*, NPR (Jan. 31, 2017, 10:46 AM), https://www.npr.org/2017/01/31/512439121/trumps-executive-order-on-immigration-annotated [https://perma.cc/6TNE-JEX9].

87   Aliya Sternstein, *Trump's Immigration Order Vastly Expands Border Surveillance*, CHRISTIAN SCI. MONITOR (Feb. 10, 2017), https://www.csmonitor.com/World/Passcode/2017/0210/Trump-s-immigration-order-vastly-expands-border-surveillance [https://perma.cc/968B-H6R5].

88   *iPhoto '09 & iPhoto '11: Improving Face Recognition Results*, APPLE SUPPORT (May 6, 2016), https://support.apple.com/en-us/HT201891 [https://perma.cc/RAX6-NCU7].

89   U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 9 (2015).

90   *Id.* at 8.

91   *Id.* at 9.

92   Frederico Viticci, *iPhone App with Face Tracking Technology Lets You Try Virtual Glasses*, MACSTORIES (Feb. 23, 2011, 5:32 PM), https://www.macstories.net/news/iphone-app-with-face-tracking-technology-lets-you-try-virtual-glasses [https://perma.cc/6XPS-QSGN].

93   Laura Wood, *Facial Recognition Market 2017 by Component, Technology, Use Case, End-User, and Region--Global Forecast to 2022--Research and Markets*, BUS. WIRE (Dec. 1, 2017, 9:30 AM), https://www.businesswire.com/news/home/20171201005396/en/ [https://perma.cc/HN73-8Z82].

94   *See id.*; *see also* Jessica Gabel Cino, *Facial Recognition Is Increasingly Common, But How Does It Work?*, CONVERSATION (Apr. 4, 2017, 9:09 PM), http://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354 [https://perma.cc/7GCZ-TEEU].

95   Olivia Solon, *Facial Recognition Database Used by FBI Is Out of Control, House Committee Hears*, GUARDIAN (Mar. 27, 2017, 6:00 AM), https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports [https://perma.cc/7XLA-DEZH].

96   Jeff John Roberts, *Our Facial Recognition Nightmare Is Upon Us*, FORTUNE (May 20, 2016), http://fortune.com/2016/05/20/facial-recognition-nightmare [https://perma.cc/T22P-DBPW].

97   *What Is Face Recognition?*, FACEFIRST, https://www.facefirst.com/face-recognition-glossary/what-is-face-recognition/ [https://perma.cc/UK7S-B5SQ].

98   Justin Lee, *Pindrop Voice Authentication to Be Integrated with Amazon Connect*, BIOMETRIC UPDATE (Mar. 29, 2017), https://www.biometricupdate.com/201703/pindrop-voice-authentication-to-be-integrated-with-amazon-connect [https://perma.cc/85E5-8DE7]; Mark Rockwell, *Making Fingerprints More Reliable Biometrics*, GCN (Jan. 26, 2017), https://gcn.com/articles/2017/01/26/iarpa-fingerprints.aspx [https://perma.cc/GKU2-2MBD]; Jeffrey A. Tucker, *Welcome Aboard, but First US Marshals Will Scan Your Retina*, FOUNDATION FOR ECON. EDUC. (Feb. 25, 2017), https://fee.org/articles/welcome-aboard-but-first-us-marshals-will-scan-your-retina [https://perma.cc/U645-YAPE].

99   *See generally* Anil K. Jain, Arun Ross & Silil Prabhakar, *An Introduction to Biometric Recognition*, 4 IEEE TRANSACTIONS ON CIRS. & SYSS. FOR VIDEO TECH. 4, 4 (2004).

100   U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 4.

101   *Facial Recognition: Who's Tracking You in Public?*, CONSUMER REPS. (Dec. 30, 2015), https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1 [https://perma.cc/XX2X-PW6X].

102   *Id.*

103   STAN Z. LI & ANIL K. JAIN, HANDBOOK OF FACE RECOGNITION 3-4 (2d ed. 2011).

104   *Id.* at 7.

105   *See id.*

106   U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 90, at 4.

107   *Id.*

108   *Cf.* Andy Greenberg, *How to Hide Your Face from Big Brother? Try Sunglasses*, FORBES (Sept. 27, 2010, 9:55 AM), https://www.forbes.com/sites/andygreenberg/2010/09/27/how-to-hide-your-face-from-big-brother-try-sunglasses/#22b3f781456f [https://perma.cc/4RQK-TKER] (explaining how sunglasses or other methods of obscuring the area around the eyes can reduce the accuracy of facial recognition software).

109   *Id.*

110   *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 9.

111   LI & JAIN, *supra* note 103, at 3.

112   *See id.* at 2, 11.

113   *See id.*

114   *See id.* at 7.

115   *See id.*

116   *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 34-36.

117   *See id.*

118   *See id.* at 3 n.5, 16.

119   *See id.*

120   G.H. Givens et al., *Introduction to Face Recognition and Evaluation of Algorithm Performance*, 67 COMPUTATIONAL STAT. & DATA ANALYSIS 236, 237 (2013); Alex Perala, *NEC Gets Top Ranking in Latest NIST Facial Recognition Test*, FINDBIOMETRICS (Mar. 16, 2017), https://findbiometrics.com/nec-nist-facial-recognition-test-403163/ [https://perma.cc/ K3ED-HG3A].

121   Liam Tung, *Microsoft's Newest Milestone? World's Lowest Error Rate in Speech Recognition*, ZDNET (Sept. 14, 2016, 11:41 AM), http://www.zdnet.com/article/microsofts-newest-milestone-worlds-lowest-error-rate-in-speech-recognition/ [https://perma.cc/KR72-M8U5].

122   *See generally* Rupinder Saini & Narinder Rana, *Comparison of Various Biometric Methods*, 2 INT'L J. ADVANCES SCI. & TECH. 24 (2014), http://www.sciencepublication.org/ijast/documents/ijastiss2/4.pdf [https://perma.cc/T89U-7CK6].

123   U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 89, at 13.

124   *See* Solon, *supra* note 95.

125   Darlene Storm, *Face Recognition App Findface May Make You Want to Take Down All Your Online Photos*, COMPUTERWORLD (May 18, 2016, 9:46 AM), https://www.computerworld.com/article/3071920/data-privacy/ face-recognition-app-findface-may-make-you-want-to-take-down-all-your-online-photos.html [https://perma.cc/8DHK-WNUK].

126   Olivia Solon, *SXSW Panel Opens Window into Dangers of Facial Recognition Software*, GUARDIAN (Mar. 11, 2017, 7:00 AM), https://www.theguardian.com/culture/2017/mar/11/sxsw-facial-recognition-biometrics-surveillance-panel [https:// perma.cc/Z4DC-GTVV]; Ethan Chiel, *This Face Recognition Company Is Causing Havoc in Russia--and Could Come to the U.S. Soon*, SPLINTER (Apr. 29, 2016, 7:00 AM), https://splinternews.com/this-face-recognition-company-is-causing-havoc- in-russi-1793856482 [https://perma.cc/2VSM-QQDG].

127   Solon, *supra* note 95.

128   Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, INTERCEPT (Mar. 22, 2017, 2:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn- cops-body-cameras-into-surveillance-machines/ [https://perma.cc/RDK6-8SHD].

129   Tamar Lewin, *Making Punishment Fit Future Crimes*, N.Y. TIMES (Nov. 14, 1982), http://www.nytimes.com/1982/11/14/ weekinreview/making-punishment-fit-future-crimes.html [https://perma.cc/CM7T-VSQ9].

130   *Id.*

131   KEHL ET AL., *supra* note 20, at 4.

132   *Id.* at 3.

133   *Id.* at 7.

134   *Id.*

135   Sonja Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 809 n.11 (2014).

136   *Id.*

137   Richard E. Redding, *Evidence-Based Sentencing: The Science of Sentencing Policy and Practice*, 1 CHAPMAN J. CRIM. JUST. 1, 3-4 (2009), http://works.bepress.com/richard_redding/11 [https://perma.cc/93WC-QEGU].

138   KEHL ET AL., *supra* note 20, at 8.

139   *Id.* at 10.

140   Kelly Hannah-Moffat, *Actuarial Sentencing: An "Unsettled" Proposition*, 30 JUST. Q. 195, 271 (2013).

141   PAMELA M. CASEY ET AL., NAT'L CTR. FOR STATE COURTS, OFFENDER RISK & NEEDS ASSESSMENT INSTRUMENTS: A PRIMER FOR COURTS app. at A-20 (2014).

142   *Id.*

143   Ed Yong, *A Popular Algorithm Is No Better at Predicting Crimes Than Random People*, ATLANTIC (Jan. 17, 2018), https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/ [https://perma.cc/3LAV-Y7K7].

144   *See*NORTHPOINTE, PRACTITIONERS GUIDE TO COMPAS CORE 2 (2015), http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf [https://perma.cc/DWK4-KBWP].

145   *Id.* at 26.

146   *Id.* at 11.

147   *Criminal Law--Sentencing Guidelines--Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing--* State v. Loomis, 881 N.W.2d 749 (Wis. 2016), 130 HARV. L. REV. 1530, 1533 (2017).

148   *Id.* at 1536-37.

149   Seth Augenstein, *COMPAS Software to Predict Recidivism No More Accurate Than Crowdsourcing, Study Says*, FORENSIC MAG. (Jan. 18, 2018, 1:12 PM), https://www.forensicmag.com/news/2018/01/compas-software-predict-recidivism-no-more-accurate-crowdsourcing-study-says?et_cid=6237469&et_rid=%%Csubscriberid%C%&type=headline [https://perma.cc/7QYE-ZXUD].

150   Heller v. Doe, 509 U.S. 312, 321 (1993).

151   *See, e.g.*, State v. Loomis, 881 N.W.2d 749, 763-64 (Wis. 2016).

152   Starr, *supra* note 135, at 838.

153   Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/BA3T-KJWU].

154   Elle Hunt, *Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter*, GUARDIAN (Mar. 24, 2016, 2:41 AM), https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter [https://perma.cc/E3ZW-SVNX].

155   Angwin et al., *supra* note 153.

156   Bernard E. Harcourt, *Risk as a Proxy for Race* 2 (Univ. of Chi. Pub. Law & Legal Theory, Working Paper No. 323, 2010).

157   *Id.* at 3-4.

158   *Id.* at 4.

159   Melissa Hamilton, *Risk-Needs Assessment: Constitutional and Ethical Challenges*, 52 AM. CRIM. L. REV. 231, 254 (2015).

160   *Id.* at 252.

161   Christopher Mims, *The Six Laws of Technology Everyone Should Know*, WALL ST. J. (Nov. 26, 2017, 8:00 AM), https://www.wsj.com/articles/the-6-laws-of-technology-everyone-should-know-1511701201 [https://perma.cc/WV5J-YUH7].

162   *Id.*

34 GASTULR 1073