Prevention or Self-Fulfilling Prophecy? Predictive Policing’s Erosion of the Presumption of Innocence

Kimberly Lindenmuth

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

Part of the Law Commons

Recommended Citation
https://scholarship.shu.edu/student_scholarship/1018
Prevention or Self-Fulfilling Prophecy? Predictive Policing’s Erosion of the Presumption of Innocence

Introduction

Eric Hanson, a fifty-eight year old retired firefighter, is stopped by San Diego police after a dispute with a man he named a prowler.1 He is ordered to sit on the curb where officers then use an iPad to take photographs of his face without his consent.2 Officers also use a cotton swab to take Mr. Hanson’s DNA sample from the inside of his cheek, again without his consent, and without any arrest having been made.3 Officers then run his photograph through facial recognition software.4 Mr. Hanson has no criminal record.5 Nor does he have access to the photograph that was taken of him.6 Neither man is arrested.7

Similar to something straight from the pages of 1984,8 police departments throughout the United States have begun using technology to increase surveillance on citizens in the name of crime prevention.9 Mr. Hanson’s story is just one scenario playing out under the use of predictive

2 Id.
3 Id.
4 Id.
5 Id.
7 Id.
8 1984 is a dystopian novel published in 1949 by English author George Orwell.
policing\textsuperscript{10} programs throughout America.\textsuperscript{11} In the case of Tyrone Brown, a twenty-nine year old African American man on probation in Kansas City, Missouri, police surveillance looms especially close.\textsuperscript{12} Unlike Mr. Hanson, Mr. Brown does have a criminal record, so when his probation officer requested his presence at a community auditorium, he expected to be admonished into helping end violence within the community.\textsuperscript{13} Instead, Mr. Brown was met with his photograph on screen, included as part of a list of individuals local authorities were “cracking down” on.\textsuperscript{14} He was linked to a criminal group that was implicated in a homicide.\textsuperscript{15} Mr. Brown’s criminal record included only drug and assault charges, but this was enough to place him at the center of the Kansas City No Violence Alliance\textsuperscript{16} program where local authorities turn to algorithms\textsuperscript{17} to predict the individuals likely to be involved in future crime.\textsuperscript{18}

\textsuperscript{10} Predictive Policing, NATIONAL INSTITUTE OF JUSTICE (June 9, 2014), https://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx (“Predictive policing tries to harness the power of information, geospatial technologies and evidence-based intervention models to reduce crime and improve public safety. This two-pronged approach – applying advanced analytics to various data sets, in conjunction with intervention models – can move law enforcement from reacting to crimes into the realm of predicting what and where something is likely to happen and deploying resources accordingly.”)

\textsuperscript{11} See also Shane Dixon Kavanaugh, This Teen’s Story is Your Worst Predictive Policing Nightmare, VOCATIV (Apr. 12, 2017), https://www.vocativ.com/418541/predictive-policing-nightmare/index.html.


\textsuperscript{13} Id.

\textsuperscript{14} Id.

\textsuperscript{15} Id.

\textsuperscript{16} Kansas City No Violence Alliance, http://kansascitynova.org/about.php (last visited Nov. 16, 2018) (“The Kansas City No Violence Alliance (KC NoVA) is a community collaboration among several organizations committed to reducing violent crime in the urban core.”)

\textsuperscript{17} Mikella Hurley, Credit Scoring in the Era of Big Data, 18 YALE J. L. & TECH. 148, 159 (quoting THOMAS H. CORMEN, CHARLES E. LEISERSEN, RONALD L. RIVEST, & CLIFFORD STEIN, INTRODUCTION TO ALGORITHMS 1 (3d ed. 2009) (emphasis omitted)) (“An algorithm can be described as ‘any well-defined computational procedure that takes some value, or set of values, as input and procedures some value, or set of values, as an output. An algorithm is thus a sequence of computational steps that transforms the input into the output.’”)

\textsuperscript{18} Supra, note 12.
Police departments across the United States, including Los Angeles, Miami, and Nashville, have begun to make use of federally funded computer models that forecast crime. These models look to predictive analytics and data mining to predict behavior. The programs culminate in an approach termed “predictive policing” now in use in numerous communities not only in the United States, but other countries as well. Predictive involves using information, geospatial technologies, and evidence-based intervention models to reduce crime and improve public safety. More specifically, departments using predictive policing methods seek to apply advanced analytics to various data sets in conjunction with intervention models. The goal is to transition law enforcement from reacting to crimes, to predicting what and where crime is likely to occur, and positioning resources accordingly. However, the use of these predictive methods has been found to chip away at a well-founded right in the United States criminal justice system: the presumption of innocence.

19 Id.
21 Dictionary.com defines data mining as, “the process of collecting, searching through, and analyzing a large amount of data in a database, as to discover patterns or relationships.” https://www.dictionary.com/browse/data-mining (last visited Nov. 11, 2018).
22 Supra, note 17.
23 See Alexander Babuta, et al., Machine Learning Algorithms and Police Decision-Making: Legal, Ethical, and Regulatory Challenges, RUSI Whitehall Report 3-18, Sept. 2018, https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf (“In the UK, predictive policing algorithms have been in use for more than ten years, to identify geospatial locations that are most at risk of experiencing crime and to then pre-emptively deploy resources to where they are most needed – ‘predictive crime mapping.’”)
26 Id.
27 Id. (“Predictive policing leverages computer models – such as those used in the business industry to anticipate how market conditions or industry trends will evolve over time – for law enforcement purposes, namely anticipating likely crime events and informing actions to prevent crime.”)
The Fifth Amendment of the United States Constitution states that “no person shall be deprived of life, liberty, or property without due process of law.”\textsuperscript{29} Out of this due process right stems the accused’s right to be presumed innocent.\textsuperscript{30} While the presumption of innocence is not specifically codified in United States law, both the Supreme Court and state courts have solidified its place in the criminal justice system.\textsuperscript{31} In \textit{Coffin v. United States},\textsuperscript{32} the United States Supreme Court held that “[t]he principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law.”\textsuperscript{33} Despite this unequivocal proclamation, courts, law enforcement, and legislators alike, have failed to protect the presumption of innocence in the face of developing police technology, specifically, predictive policing methods. While many of the programs and strategies used are still in their infancy, the future of predictive policing raises significant concerns regarding constitutional rights.\textsuperscript{34}

This note discusses the effect of predictive policing strategies on the presumption of innocence, particularly, its erosion of the same, and argues that legislation be adopted to monitor and regulate said strategies. Part I gives an overview of the history of the presumption of innocence with specific focus on its foundation and evolution in American law as well as the process to initiate criminal proceedings against an individual. Part II will discuss the origins and progression of predictive policing and examine the methodology behind strategies implemented by U.S. police departments. Part III seeks to analyze the effect of predictive policing on the

\textsuperscript{29} U.S. CONST. AMEND. 5.
\textsuperscript{30} See also \textit{Coffin v. United States}, 156 U.S. 432 (1895).
\textsuperscript{31} \textit{Coffin v. United States}, 156 U.S. 432 (1895) (holding that a reasonable doubt instruction is not the equivalent of a presumption of innocence instruction).
\textsuperscript{32} Id.
\textsuperscript{33} Id. at 453.
\textsuperscript{34} See Andrew Guthrie Ferguson, \textit{Predictive Policing and Reasonable Suspicion}, 62 EMORY L.J. 259 (2012) (“Predictive policing, like many new law enforcement strategies, raises issues of class-based and race-based targeting, as well as general civil liberties concerns.”)
presumption of innocence, analyzing first the departure from the reasonable suspicion standard, its effects on minority communities, and causation issues stemming from the gap between data and man-made decision-making. Part IV presents suggested solutions in the form of potential legislation regulating the use of predictive policing.

I. Background: The Origin and Evolution of the Presumption of Innocence in American Jurisprudence

This Part provides background information discussing the origins and evolution of the American criminal justice system paying specific attention to the development of the distinction between the presumption of innocence and the reasonable doubt standard. It provides an overview of the requirements to bring criminal charges against an individual and legal foundations law enforcement must follow to make an arrest and pursue criminal charges.

A. History and Distinctions Between the Presumption of Innocence and the Reasonable Doubt Standard

The origins of the presumption of innocence date far beyond even the founding of America. The development of the adversarial system and jury trial in England paved the way for a transition from crude medieval law to the systems and maxims in place in America today;\(^{35}\) “The evolution from an inquisitorial system to an adversarial system of justice reflected a consensus that a number of fundamental interests and rights required that the burdens of production and persuasion be shifted to the state.”\(^{36}\) This shifting of the burden from the accused to demonstrate his innocence, to the state to produce evidence of the accused’s guilt, laid the foundation for not only the reasonable doubt standard, but for the presumption of innocence as


\(^{36}\) *Id.* (“God could no longer reveal the innocent from the murderer, thief, and robber. Proof of factual innocence was replaced by proof of legal guilt or in its absence, legal innocence.”)
well. Early in America’s history, the Supreme Court reinforced the use of the adversarial system in *Rogers v. Richmond*,\(^{37}\) wherein Justice Frankfurter proclaimed, “[O]urs is an accusatorial and not an inquisitorial system – a system in which the State must establish guilt by evidence independently and freely secured and may not by coercion prove its charge against an accused out of his own mouth.”\(^{38}\)

The evolution of the presumption of innocence also finds roots in the United States Constitution being that courts have used the Fifth Amendment Due Process Clause to interpret as granting certain pretrial rights.\(^{39}\) Out of this Amendment stems the reasonable doubt standard and the presumption of innocence. However, not until *Coffin*, did a distinction exist between the two.\(^{40}\) In *Coffin*, the Supreme Court considered, as an original question, the distinction between the reasonable doubt standard and the presumption of innocence.\(^{41}\) The Court determined that the “presumption is an instrument of proof created by the law in favor of one accused, whereby his innocence is established until sufficient evidence is introduced to overcome the proof which the law has created.”\(^{42}\) The Court goes on to juxtapose the reasonable doubt standard from the presumption of innocence, defining reasonable doubt as “the result of the proof, not the proof itself; whereas the presumption of innocence is one of the instruments of proof, going to bring about the proof, from which reasonable doubt arises….”\(^{43}\) The *Coffin* Court essentially separated the two principles, further defining the presumption of innocence as a fundamental principle and

---


\(^{38}\) *Id.* at 541.

\(^{39}\) U.S. CONST. AMEND. 5; *In re Winship*, 397 U.S. 358, 364 (1970) (holding that the Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime he is charged with); *Coffin v. United States*, 156 U.S. 432 (1895).

\(^{40}\) *Coffin v. United States*, 156 U.S. 432 (1895).

\(^{41}\) *Id.* at 458.

\(^{42}\) *Id.* at 459.

\(^{43}\) *Id.* at 460.
legal burden separate from the prosecution’s burden of proof beyond a reasonable doubt.\textsuperscript{44} Both of these standards have been held to apply regardless of the factual guilt or innocence of the accused.\textsuperscript{45}

The distinction cemented in \textit{Coffin} has been further interpreted to grant the accused the right to be presumed innocent throughout trial up and until the prosecution meets its burden beyond a reasonable doubt.\textsuperscript{46} The Supreme Court confirmed this in \textit{Taylor v. Kentucky}, where it held that “one accused of a crime is entitled to have his guilt or innocence determined solely on the basis of the evidence introduced at trial, and not on grounds of official suspicion, indictment, continued custody, or other circumstances not adduced as proof at trial.”\textsuperscript{47} While the Supreme Court later ruled that an instruction on the presumption of innocence is not constitutionally required in every criminal case, it still requires an evaluation in light of the totality of the circumstances to ensure the defendant receives a constitutionally fair trial.\textsuperscript{48} Despite the requirements laid out in \textit{Taylor v. Kentucky}, police departments throughout the country have increased their use of predictive policing measures to determine guilt, innocence, and propensity far before trial and without the Constitutional safeguards underlying the reasonable doubt standard.

\textbf{B. Traditional Constitutional Requirements for Police Intervention and Arrest}

\begin{itemize}
\item United States v. Doyle, 130 F.3d 523 (2d Cir. 1997) (affirming the proposition that the presumption of innocence and beyond a reasonable doubt standard apply to all criminal defendants without regard to their actual guilt or innocence).
\item \textit{See} Taylor v. Kentucky, 436 U.S. 478 (1978) (holding that the trial court’s refusal to give petitioner’s requested instruction on the presumption of innocence resulted in a violation of his right to a fair trial as guaranteed by the Due Process Clause).
\item \textit{Id.} at 485.
\item Kentucky v. Whorton, 441 U.S. 786, 789 (1979) (“The court’s inquiry should have been directed to a determination of whether the failure to give such an instruction in the present case deprived the respondent of due process of law in light of the totality of the circumstances.”)
\end{itemize}
The Fourth Amendment of the United States Constitution protects the right of the people against unreasonable searches and seizures, further stating that no warrants shall be issued but upon probable cause supported by oath or affirmation. The Supreme Court has interpreted seizure of persons to occur only when a reasonable person would feel that he or she was not free to decline the officer’s requests or otherwise terminate the encounter under a totality of the circumstances analysis. Additionally, the Court has interpreted the Fourth Amendment to require either a physical application of force by the officer or a submission to the officer’s show of force.

In order to make an arrest, an officer must have probable cause. Probable cause to arrest is present when, at the time of arrest, the officer has within his or her knowledge reasonably trustworthy facts and circumstances sufficient to warrant a reasonably prudent person to believe the suspect has committed or is committing a crime for which arrest is authorized by law. The warrant requirement listed in the Fourth Amendment is waived when officers attempt to arrest someone in a public place, even if they have time to obtain an arrest warrant. The Supreme Court has granted officers vast discretion in this regard, being that police may make a warrantless misdemeanor arrest even if the crime for which the arrest is made cannot be punished by incarceration. Even more troubling is the fact that an unlawful arrest by itself has no impact on a subsequent criminal prosecution; if police improperly arrest someone, they can

49 U.S. CONST. AMEND. 4.
51 California v. Hodari D., 499 U.S. 621 (1991) (stating that it is not enough that the officer merely ordered the person to stop to constitute a seizure of persons).
52 U.S. CONST. AMEND. 4.
53 Beck v. Ohio, 379 U.S. 89, 91 (1964); Brinegar v. United States, 338 U.S. 160, 176 (“The rule of probable cause is a practical, nontechnical conception affording the best compromise that has been found for accommodating . . . often opposing interests. Requiring more would unduly hamper law enforcement. Tow allow less would be to leave law-abiding citizens at the mercy of the officers’ whim or caprice.”)
detain them if they have probable cause to do so and the invalid arrest is not a defense to the offense charged.\textsuperscript{56} 

More particular to predictive policing efforts are investigatory detentions which stray even further from the warrant requirement of the Fourth Amendment.\textsuperscript{57} Landmark case \textit{Terry v. Ohio}\textsuperscript{58} allows law enforcement to briefly detain a person for investigative purposes even if they lack the probable cause necessary to make an arrest.\textsuperscript{59} \textit{Terry} stops merely require police have reasonable suspicion supported by articulable facts of criminal activity or involvement in a completed crime.\textsuperscript{60} Courts do not specifically define “reasonable suspicion,” only stating that it requires more than a vague suspicion judged under the totality of the circumstances.\textsuperscript{61} Further, if police have reasonable suspicion to believe the detainee is armed and dangerous, they can also conduct a frisk to ensure the detainee has no weapons.\textsuperscript{62} Reasonable suspicion, not unlike probable cause, need not arise from the police officer’s personal knowledge.\textsuperscript{63} Investigatory stops are not limited to a specified time limit, the only requirement being that police must act in a diligent and reasonable manner in confirming or dispelling their suspicions.\textsuperscript{64} The development of predictive policing technologies has raised questions regarding the sources of probable cause and reasonable suspicion to be analyzed later on in Part III of this paper.

\textbf{II. Predictive Policing: Methodology and History}

This section provides a cursory overview of the use of predictive software in policing. It begins by briefly defining the terms and methods underlying predictive policing. It examines the


\textsuperscript{57} U.S. \textsc{Const. Amend.} 4.

\textsuperscript{58} \textit{Terry v. Ohio}, 392 U.S. 1 (1968).

\textsuperscript{59} Id.

\textsuperscript{60} Id.


\textsuperscript{62} Terry, 392 U.S. 1.


transition from older methods to current, more advanced technologies, further examining some of the drawbacks to these methods. It places particular focus on transparency and accuracy issues presented by use of this type of technology.

A. The Underlying Methodology of Predictive Policing

To better understand the perils of predictive policing, the inner mechanisms of algorithms and machine learning must briefly be explored and further defined. Algorithms make use of machine learning to create their predictions. Machine learning describes “a set of methods that can automatically detect patterns in data, and then use the uncovered patterns to predict future data, or to perform other kinds of decision making under uncertainty. An algorithm is thus a sequence of computational steps that transforms the input into the output.” In other words, algorithms are mathematical computations that take in certain data, analyze patterns within that data, and use them to make predictions on future data based on those patterns.

B. The Transitional History of Predictive Policing Methods

Predictive Policing in its current form is a fairly recent development in the American criminal justice system. Previously, predictive software and methodology had primarily been used by American military and intelligence agencies. Military agencies used facial recognition


66 Id.

67 WALTER L. PERRY, ET AL., RAND CORPORATION, PREDICTIVE POLICING 4 (2013) ("Police Chief (ret.) William J. Bratton and the LAPD are credited with envisioning the predictive policing model. By 2008, Chief Bratton had spoken widely in the public arena about the successes of the LAPD, including the department’s recent introduction of predictive analytics to anticipate gang violence and to support real-time crime monitoring.")

68 See Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police*, N.Y. TIMES, Aug. 12, 2015, https://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?module=inline; see also Alex Campolo, et al., AI Now 2017 Report, https://assets.ctfassets.net/8wprhhvnpfc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb14f2b74b2be64c3ce0c78/_A_I_Now_Institute_2017_Report_.pdf (The United States military has been one of the most influential institutions making use of artificial intelligence, its capabilities largely suited to military goals and objectives).
software in Iraq and Afghanistan to identify potential terrorists. This same technology is now being used by police departments around the United States to pursue conventional criminal suspects. Some of the origins of predictive policing can also be found in crime mapping. A study done by the University of Chicago in the 1930’s concluded that crime was positively correlated with economically disadvantaged areas and demonstrated a link between delinquency rates and “features of community structure like economic status, stability, and racial composition.” This study formed the catalyst for the development of new theories of crime such as Social Disorganization Theory, Routine Activities Theory, and Defensible Space Theory, some of which are still considered today.

Currently, predictive methods are an underlying part of everyday American life from police-worn body cameras to ever-present surveillance footage. Facial recognition, using algorithms to match facial features via photos and video, is used in various ways, from tagging

---

69 Id.
70 Id.
74 Graham Steventon, DEFENSIBLE SPACE: A CRITICAL REVIEW OF THE THEORY AND PRACTICE OF A CRIME PREVENTION STRATEGY, (2010) (“Defensible space is a principle of crime prevention…Through enclosure, for instance cul de sac layouts, the intention is to create exclusive living environments, which will precipitate territoriality and a sense of community in residents, resulting in collective action against crime.”)
76 See Amanda Ripley, A Big Test of Police Body Cameras Defies Expectations, N.Y. TIMES (Oct. 20, 2017), https://www.nytimes.com/2017/10/20/upshot/a-big-test-of-police-body-cameras-defies-expectations.html (“By 2015, 95% of large police departments reported they were using body cameras or had committed to doing so in the near future….”)
friends in photos on Facebook, to unlocking cellphones, and soon to admit fans to Major League Baseball games. More traditionally, facial recognition technology has also been used by law enforcement agencies to compare photos or video stills to databases of license photographs or mugshots to identify suspects. This technology has developed into the use of “real-time” facial recognition where law enforcement is able to scan live video feeds constantly to match moving faces with a database of still images. The Federal Bureau of Investigation has numerous programs implementing facial recognition software: the FBI’s Next Generation Identification system (NGI), in use since 2011, and Facial Analysis, Comparison, and Evaluation Services Unit (FACE) to name a few. Instead of using biological or anatomical models of faces, these programs use pattern matching approaches chosen by developers. Programs like NGI have started to replace more traditional identification methods such as AFIS, the legacy Automated Fingerprint Identification System. While advances in policing techniques have provided some societal benefits, they have also created a system of structural surveillance that has been advanced by military level technology.

Police departments using predictive policing methods are relying on a new source: big data. Police departments engaged in predictive policing use data mining to find correlations

---

78 Id. Maryland’s system was used to identify the suspect who allegedly massacred journalists at the Capital Gazette newspaper in Annapolis and monitor protestors following the death of Freddie Gray in 2015 in Baltimore.
79 Id.
81 Id.
84 Julie E. Cohen, What Privacy is For, 126 HARV. L. REV. 1904, 1920-21 (2013) (“Big data’ is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short
between various input data and criminal outcomes, oftentimes using variables like crime locations and social networks.\(^8\) Put more simply, predictive algorithms sift through personal information to make projections about an individual’s likely actions or risks.\(^9\)

Large technology firms that create these types of programs have become one of the biggest sources of these algorithms and the government has become the biggest customer.\(^1\) Departments like the New York Police Department have partnered with companies like Palantir Technologies, a data analytics firm that works with intelligence agencies and police departments nationwide.\(^2\) Through this relationship, Palantir received arrest records, license plate numbers, and parking tickets to trace connections between people and crimes.\(^3\) Symbiotic relationships between tech companies and law enforcement agencies are not unique in the growing world of predictive policing.\(^4\) U.S. Immigration and Customs Enforcement has expanded its use of technology, using tools like Investigative Case Management (ICM), which allows agents to access previously separate databases holding information on a suspect’s schooling, employment information, phone records, family relationships, foreign exchange program status, personal connections, biometric traits, criminal history, and home and work addresses through another
Palantir system. Additionally, large companies like Amazon and Axon (the country’s largest supplier of police body cameras) have become targeted by civil liberties unions throughout the country because of their marketing to American law enforcement. Amazon was criticized by the American Civil Liberties Union of Northern California who revealed the company’s efforts to sell facial recognition software to American police forces, including using officers to scan live feeds from surveillance cameras and determine whether those images matched photos in a database of missing or wanted people.

One of the programs at the very foundation of predictive policing is PredPol, a program created by UCLA scientists in coordination with the Los Angeles Police Department to see how scientific analysis of crime data could help spot patterns of criminal behavior. **This place-based prediction system relies on historical crime data in conjunction with near-repeat theory, which hypothesizes that certain crimes occur in close temporal and spatial windows to where they have already occurred.** PredPol is used in over sixty police departments throughout the United States to identify areas in a neighborhood where serious crimes are more likely to occur during a particular period. PredPol limits its predictions to location whereas other programs take the

---

91 Alex Campolo, et al., AI Now 2017 Report, https://assets.ctfassets.net/8wprhvnpc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb14f2b74b2be64c3ce0c78/_AI_Now_Institute_2017_Report_.pdf.
93 Id.
next step in predicting who is likely to commit crime, an approach used by Chicago police departments. In Chicago, police departments make use of a “Strategic Subject List” which includes individuals most likely to be involved in future shootings, either as victim or shooter. Factors considered in creating this list include criminal record, social circles, and gang connections, as well as whether one has been the victim of an assault or a shooting. An individual’s personalized threat score appears on police dashboard computers when making a stop. This score also determines who gets targeted for proactive police intervention, such interventions ranging from home visits from police officers, to added police surveillance, to an invitation to a community meeting. High risk individuals are prioritized using an algorithm that analyzes past arrests for violent crime, weapons or narcotics offenses, age, incidents where the individual was a victim of a shooting or assault, and the trend line of criminal activity. Also included in this strategy are elements of traditional policing with increased attention to crime “hot spots” and close monitoring of recent parolees. However, more nontraditional data

property crime maps at 1:30 a.m. each day, which are handed out to officers on the morning shift. The maps are updated later in the day for subsequent shifts.”)

97 Id.
98 See Jeff Asher, Inside the Algorithm that Tries to Predict Gun Violence in Chicago, N.Y. TIMES, (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html (The Strategic Subject List was created by the Illinois Institute of Technology in 2013 and applies an algorithm to hundreds of thousands of arrested subjects, and helps prioritize limited resources to focus on those at highest risk.)
102 Id.
103 Id.
is also used including friendships, social media activity, and drug use in adding individuals to the list and assisting authorities in forecasting crime.\textsuperscript{105}

Transparency behind these methods varies.\textsuperscript{106} While programs similar to Chicago’s are taking place around the country, “civil liberties groups question the legality and efficacy of such programs, saying citizens, besides having the right to a presumption of innocence, should be able to know exactly how they wind up on a list, and should be able to challenge their inclusion.”\textsuperscript{107}

Another challenge with programs of this nature is the level of accuracy.\textsuperscript{108} Programs like facial recognition have advanced from machine learning based on comparisons of certain facial features to “neural networks” that take a more holistic view of faces, thereby improving their accuracy.\textsuperscript{109} Accuracy depends on the data used to teach the algorithm, and therein lies another potential issue with the program: these programs require a broad database of faces and conditions, people with varied skin tones captured at various angles, distances, and lighting, to enable the algorithm to produce a more accurate prediction.\textsuperscript{110} These technical blind spots open the door to false identifications and improper predictions that can cause innocent people to become entangled in the criminal justice system, which will be discussed in further detail in the next section.

\textsuperscript{105} Id.
\textsuperscript{106} Andrew Guthrie Ferguson, \textit{Policing Predictive Policing}, 94 WASH. U. L. REV. 1109, 1164 (2017) (“The appeal of predictive policing has in large measure been that it offers a ‘black box’ solution to crime. The corresponding vulnerability, however, is that such solutions lack sufficient transparency to ensure that the ‘black box’ really works. The lack of transparency in data collection, data use, and effectiveness requires designing processes to guarantee that predictive policing technologies live up to the promise of their creation.”)
\textsuperscript{108} Andrew Guthrie Ferguson, \textit{Policing Predictive Policing}, 94 WASH. U. L. REV. 1109, 1145 (2017) (“Any data-driven system risks being undermined by bad data. This data includes flaws, fragmentation, and the internal and external pressures to collect vast amounts of information constantly, instantaneously, and without adequate financial resources to ensure accuracy.”)
\textsuperscript{110} Id.
III. Predictive Policing’s Effect on the Presumption of Innocence

Alongside the benefits, the pitfalls of predictive policing come in many shapes and forms. This section seeks to analyze them starting with the departure from the reasonable suspicion standard, discriminatory effects on minority communities, and causation issues caused by the gap between computer-driven data and man-made decision-making.

A. Effects on Minority Communities

Predictive policing efforts lead to increased police presence in areas already facing high rates of police surveillance.111 Algorithms used in these programs target poor and minority communities despite attempts to use and provide objective data.112 Additionally, bias is woven into the very fabric of these technologies through tainted input data.113 “Algorithmic policing threatens black and brown communities already saturated with other kinds of police surveillance technologies.”114 Threat scores like the ones in place in Chicago impact the way police interact with individuals on the street.115 Once police have declared an individual above a certain threat score, this knowledge changes how police interact with them; this knowledge leads to an increase in perceived danger, resulting in more frequent and aggressive interactions with

---

111 Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 GA. L. REV. 109, 130 (2017) (“The potential for harm stemming from racially imbalanced outcomes is the harm resulting from having more police in a neighborhood that is unfairly maligned as having more crime.”)
113 Id.; Ezekiel Edwards, Predictive Policing Software is More Accurate at Predicting Policing Than Predicting Crime, ACLU (Aug. 31, 2016), https://www.aclu.org/blog/criminal-law-reform/reforming-police-practices/predictive-policing-software-more-accurate (“Since predictive policing depends on historical crime data, and crime data is both incomplete (a large percentage of crime is unknown and/or unreported) and racially skewed (take drug offenses, for example), it seems inescapable that resulting predictions made by policing software will be inaccurate and arbitrary.”)
individuals the algorithm deems high risk. Risk assessment scores are particularly problematic with regard to the presumption of innocence because they assess the likelihood that a particular individual will commit another crime in the future. Another issue is that these scores do not affect all races equally. A report by ProPublica found that a popular software “was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants,” and routinely “mislabeled [white defendants] as low risk more often than black defendants.” These risk assessment scores again find themselves based in flawed data sets rather than individualized suspicion. Once a person has been deemed high risk, their presumption of innocence is effectively nonexistent. Instead of a police interaction based on observed suspicious behavior, these individuals can be approached by police for doing nothing at all other than appearing on a list they know nothing about and have no power to change.

Algorithms used in predictive policing base their predictions on input data. The way these algorithms function leaves room for human bias to become entangled in the predictions

116 Id.
119 ProPublica is an independent, nonprofit newsroom.
121 Id.
122 See Ezekiel Edwards, Predictive Policing Software is More Accurate at Predicting Policing Than Predicting Crime, ACLU (Aug. 31, 2016), https://www.aclu.org/blog/criminal-law-reform/reforming-police-practices/predictive-policing-software-more-accurate (“Flagging individuals using predictive analytics also poses the serious risk to those individuals, and to entire neighborhoods, of the police acting on a presumption of guilt by association.”)
123 Jason Bloomberg, Bias is AI’s Achilles Heel. Here’s How to Fix It, FORBES (Aug. 13, 2018), https://www.forbes.com/sites/jasonbloomberg/2018/08/13/bias-is-ais-achilles-heel-heres-how-to-fix-it/#54e21876e682 (“AI – in particular, both machine learning and deep learning – take large data sets as input, distill the essential lessons from those data, and deliver conclusions based on them.”)

18
they create. Input, or training data, is often labeled by human hands, thereby incorporating human bias and cultural assumptions. This phenomena is known as, “selection bias,” where errors in estimation result when some members of a population are more likely to be sampled than others. For example, when a machine learning program is trained to recognize faces of one particular racial group and is then applied to a larger, more diverse population group, it may produce biased results with a lower measure of accuracy. Additionally, crimes recorded by police departments are not a complete census of all crimes committed due to nonreporting; nor are they a wholly representative random sample. Being that data-driven programs are still relatively new to policing, it can be difficult to obtain diverse data. Data is also expensive to acquire, which leads algorithm developers to make use of data that is easy to obtain regardless of its diversity. This can easily lead to skewed data because it can come from saturated sources, where data is collected extensively from one group and not another. “[E]ven algorithms used to predict the location of crime will only be as good as the information that is fed into them. If an algorithm is populated primarily with crimes committed by black people, it will spit out results that send police to black neighborhoods.” Because people of color are already

---

124 See Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 GA. L. REV. 109 (“Data mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society.”)

125 Alex Campolo, et al., AI Now 2017 Report, https://assets.ctfassets.net/8wprhvnpc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb14f2b74b2be64c3ce0c78/_A I_Now_Institute_2017_Report_.pdf.

126 Id.

127 Id.


129 Alex Campolo, et al., AI Now 2017 Report, https://assets.ctfassets.net/8wprhvnpc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb14f2b74b2be64c3ce0c78/_A I_Now_Institute_2017_Report_.pdf.

130 Id.

disproportionately represented in America’s criminal justice system, and are stopped, detained, arrested, and incarcerated at higher levels than whites, regardless of crime rates, predictive policing algorithms require close monitoring. Researchers Kristian Lum and William Isaac of the Human Rights Data Analysis Group published a case study analyzing a predictive policing algorithm’s projected effects if applied in Oakland, California to police drug crime. The study found that “the police data appear to disproportionately represent crimes committed in areas with higher populations of non-white and low-income residents.” Results like these illuminate the nature of policing in these neighborhoods. The logical conclusion is not farfetched: once you find yourself present in a low-income minority neighborhood, your likelihood of being arrested or detained by police increases.

The accuracy of programs like facial recognition also disfavor minorities. Research from the Georgetown Law School estimated that 117 million American adults are present in facial recognition networks in use by law enforcement and that African Americans were most likely to be singled out due to their disproportionate representation in mug-shot databases. Facial recognition technology has varying rates of error depending on race and gender. This again speaks to the issue of data set inclusion being that one widely used facial recognition data set was assessed to be seventy-five percent male and over eighty percent white. This presents a problem because algorithms are only as good as the data they use, so if there are more white

---

132 Id.
134 Id.
137 Id.
138 Id.
people than black in the system, it will be worse at identifying black people.\textsuperscript{139} If police departments then implement these algorithms, they are accepting and perpetuating the bias and discrimination present in the predictive programming.\textsuperscript{140} Arrests are then being made based on faulty information and without the resources to combat these false allegations, innocent people will be placed in the criminal justice system with little to no recourse.\textsuperscript{141} Instead, systems police departments intend to use should be publicly audited and monitored on an ongoing basis to oversee their disparate impact on minority communities with results broken down by race and neighborhood to better address disparities.\textsuperscript{142}

B. Causation Issues: Data v. Man-made Decision-Making

Predictive policing methods bring about causation issues. If additional officers are dispatched to the same locations consistently then it follows they will witness and report more crime, resulting in higher arrest rates. But correlation is not causation. The mere presence of additional officers skews the data in that it begs the question, is more crime being committed in these areas or is more crime being reported in these areas due to increased police presence? “Predictive policing thus raises some profound questions about the nature of prediction in an era influenced by data collection and analysis.”\textsuperscript{143} These theories are based in the belief that certain

\begin{flushright}
\textsuperscript{139} Id.
\textsuperscript{140} See Andrew D. Selbst, \textit{Disparate Impact in Big Data Policing}, 52 GA. L. REV. 109, 140 (2017) (“[T]he harm is that racial disparities in the outcome of the algorithm create a greater degree of suspicion and higher likelihood of finding probable cause due to a suspect’s race.”)
\textsuperscript{141} See also Ezekiel Edwards, \textit{Predictive Policing Software is More Accurate at Predicting Policing Than Predicting Crime}, ACLU (Aug. 31, 2016), https://www.aclu.org/blog/criminal-law-reform/reforming-police-practices/predictive-policing-software-more-accurate (“The harmful consequences of relying on bad (and secret) predictions in the context of policing are significant, including increased profiling of individuals and communities, deploying police resources inefficiently, and creating deeper fissures between police and the communities they are entrusted to protect.”)
\textsuperscript{143} Andrew Guthrie Ferguson, \textit{Policing Predictive Policing}, 94 WASH. U. L. REV. 1109, 1114.
\end{flushright}
aspects of physical and social environment encourage acts of criminal wrongdoing that can be predicted and prevented.\textsuperscript{144} Predictive policing hypothesizes that interfering with those elements of environment will deter crime.\textsuperscript{145} Despite these intentions, predictive policing effectively amounts to a self-fulfilling prophecy wherein police resources are disbursed to the same areas, already labeled “high crime” to surveil people that have already had contact with the criminal justice system. “Suspicion based on correlation may be acceptable when talking about place-based crimes, but it is insufficient when talking about person-based crimes. Sending a police car to patrol a suspected area is less consequential than sending a police detective to interrogate a suspect.”\textsuperscript{146} These methods have been used to justify violent crime-focused or person-focused technology without the equivalent empirical testing to support it.\textsuperscript{147}

This lack of testing contributes to a lack of transparency surrounding predictive policing around the country.\textsuperscript{148} Companies providing police departments with the programs they use attempt to prevent the inner workings of their products from becoming public knowledge through claims of trade secrecy or business confidentiality.\textsuperscript{149} Instead, departments put these programs in place with little, if any, public input and very little disclosure.\textsuperscript{150} Because officers using the technology may be unable to explain how it works and companies creating the

\begin{flushleft}
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
\textsuperscript{147} Id.
\textsuperscript{148} Andrew Guthrie Ferguson, \textit{Policing Predictive Policing}, 94 WASH. U. L. REV. 1109, 1164 (2017) ("The lack of scientific studies remain a real vulnerability in the development of predictive policing. . . . This problem is exacerbated by the fact that much of the data rests in private hands and is controlled by proprietary interests.")
\textsuperscript{150} Id. ("Vendors are shrouding their products in secrecy, and even seeking gag clauses or asking departments to pledge to spend officer time resisting relevant public records requests, as a precondition for trying out their products.")
\end{flushleft}
technology refuse to do so, the accused stands unable to articulate how or why the police
department erred, thereby giving an undeserved upper hand to law enforcement.

C. Departure from the Reasonable Suspicion Standard

The presumption of innocence has long been deemed a foundational principle in
American law.\footnote{Coffin v. United States, 156 U.S. 432 (1895).} Despite this designation, American courts have been nearly silent in the face of
advancing technology that chips away at the presumption of innocence and relies less and less on
human decision-making. The traditional system of checks and balances in place since the
founding of America stands at risk of being set aside in favor of predictive technologies.

Computer-driven hunches or predictions should not be an exception to the Fourth Amendment’s
requirement of reasonable suspicion.\footnote{Predictive Policing Today: A Shared Statement of Civil Rights Concerns [Statement of Concern About Predictive
concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.} Predictive policing programs that rely on algorithms to
predict who is likely to commit crime detract from the reasonable suspicion requirement. “It
undermines the constitutional requirement that police should target people based upon an
individual suspicion of wrongdoing, not statistical probability.”\footnote{Faiza Patel, Be Cautious About Data-Driven Policing, N.Y. TIMES (Dec. 3, 2015),
articulable facts, as required by the Supreme Court, police departments can point to vague
algorithmic outcomes that they are unlikely to be able to explain.\footnote{See Terry v. Ohio, 392 U.S. 1 (1968).} Generally, police develop
reasonable suspicion from activities they observe or information they have been given.\footnote{Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, Jan. 23, 2015, 163 U. PA. L. REV. 327 (2015).} This is
individualized suspicion based on the perceived actions the individual has taken, not an
algorithm based on previous conduct. Conventional reasonable suspicion is said to be based on “small data,” discrete facts, limited information, and little knowledge about the actual suspect. Small data is traditionally thought of as solving discrete questions with limited structured data generally controlled by one institution. Predictive policing seeks to expand this notion to big data suspicion by basing reasonable suspicion on a vast network of information sources provided by big data technology. While it has been established that reasonable suspicion need not arise from the arresting officer’s personal knowledge, the source should be more than mere speculation based on an individual’s past crimes and propensity to commit another. In many other areas of law, the use of propensity is barred. Evidence of a crime or wrongdoing is not admissible at trial to prove a defendant’s character to show that on a particular occasion the person acted in accordance with that character. This propensity evidence is exactly what predictive policing seeks to use to supposedly predict and prevent crime. It effectively uses an individual’s past behavior to predict how they will act and what crimes they will commit in the future. While other portions of our criminal justice system take into consideration past conduct, bail and sentencing for example, predictive policing must draw the line in the sand. Arrests should not be made solely on predictions that cause certain individuals to be under increased law enforcement surveillance. These things require, and our Constitution requires,

\begin{footnotesize}
\begin{enumerate}
\item[156] Id.
\item[157] Id.
\item[158] Id.
\item[159] Id.
\item[162] Id.
\item[163] WALTER L. PERRY, ET AL., RAND CORPORATION, PREDICTIVE POLICING xvi (2013) (Methods to identify individuals at high risk of offending in the future can be in part based on regression and classification models for individuals who may become reoffenders).
\item[164] See Andrew Guthrie Ferguson, Policing Predictive Policing, 94 WASH. U. L. REV. 1109, 1123 (2017) (“The prevalence of predictive technologies in the criminal justice system has not gone unchallenged, and many scholars have critiqued the growing reliance and even legitimacy of some of the chosen tools.”)
\end{enumerate}
\end{footnotesize}
observed conduct; an arrest must typically be based on a warrant that requires probable cause.\footnote{U.S. CONST. AMEND. 4.}

Predictive policing programs seek to satisfy the probable cause and reasonable suspicion requirements by allowing law enforcement to rely on oftentimes flawed algorithmic data. If safeguards are not implemented, then innocent people and people that have only committed crimes in the past, will be under constant police surveillance based only on the predictions of a computer rather than any actual conduct the individual has engaged in.

\textbf{IV. Suggested Solutions}

The progression of technology provides opportunities for advancement within many aspects of life. Predictive policing could be considered the next step in policing for departments around the world. It is nearly counterintuitive to suggest that such agencies refuse to even consider it. Technological advancements are an unavoidable component of a developing society.\footnote{See Lindsey Barrett, \textit{Reasonably Suspicious Algorithms: Predictive Policing at the United States Border}, 41 N.Y.U. REV. L. & SOC. CHANGE 327.} That being said, the idea is not to prevent police departments from using this technology, but to regulate it in the name of protecting the civil rights of the accused and the innocent.

First, it bears mention that in addition to traditional and predictive policing methods, social services can be used to address problems with at-risk individuals and communities before crimes take place.\footnote{Predictive Policing Today: A Shared Statement of Civil Rights Concerns [Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations], Aug. 31, 2016, https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.} Communities making use of this technology should consider using it to determine where to allocate not only police officer presence, but social resources more generally to provide things like educational opportunities, health services, and job training.\footnote{Id.} This type of
community policing constitutes a more holistic approach that touches the actual root of the problem instead of attributing all crime to an offender.

Second, issues of transparency and accountability must be addressed.\textsuperscript{169} Predictive policing programs must be regulated to standardize procedures across the nation and monitor departments’ and companies’ use of predictive technology. This regulation may best be found in the form of legislation. First, police departments using predictive policing technologies must make this public record. Transparency is key to maintaining a just system that protects the rights of the accused, including those that have only been predicted to be accused. Such efforts have already been undertaken by the Brennan Center for Justice at New York University School of Law.\textsuperscript{170} The Brennan Center undertook litigation pursuant to the Freedom of Information Law to force the New York Police Department to disclose certain methods of predictive policing.\textsuperscript{171} The litigation was successful in that it forced court action on the issue, which then ruled that the agency bears the burden of demonstrating that the material sought is exempt from disclosure.\textsuperscript{172} The court went on to require an \textit{in camera} inspection of documents if the court cannot determine whether they fall entirely within the scope of the asserted exemption.\textsuperscript{173} The court also articulated several factors to determine whether information constitutes a trade secret: the extent to which the information is known outside the business of the party seeking to keep it confidential; the extent the information is known by employees in the business; the extent of

\textsuperscript{169} See William S. Isaac, \textit{Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice}, 15 OHIO ST. J. CRIM. L. 543 (“The concerns about implementation and efficacy raise critical questions about the appropriate degree of transparency and regulation that algorithmic decision support tools should have.”)
\textsuperscript{170} See Brennan Ctr. for Justice at New York Univ. Sch. of Law v. New York City Police Dept., 2017 N.Y. Misc. LEXIS 5138 (2017) (ordering the NYPD to provide email correspondence with vendors and output data from its predictive policing program).
\textsuperscript{171} Id.
\textsuperscript{172} Id.
\textsuperscript{173} Id.
measures taken to guard the information; the value of the information to the party and its competitors; the amount of effort and funds expended in developing the information; and the ease or difficulty in acquiring or duplicating the information by others.\textsuperscript{174} Courts throughout the country should follow New York’s lead in placing guidelines and giving instructions to police departments using these methods. Such rulings set the transparency parameters for what police departments can and cannot avoid disclosing to the public.

Next, due process mechanisms must be put into place for those affected by predictive policing tactics. If the name of an individual appears on a Strategic Subject List, that individual should have the ability to take advantage of a procedure to dispute that finding. Review by a judge of prior record, current status, and rehabilitative efforts contrasted by the predictive data supplied and used by the police department is one possible first step. While some may argue that this kind of procedural remedy will further slow down the courts and is not a constitutional guarantee, this is not the case. Being that the right to be presumed innocent exists, those standing accused of crimes should have the recourse to be made aware of and face their accuser. This confrontation will also form a check on the system that searches for any discrimination or disparities within the system. The aforementioned concepts are accountability measures that place the burden on the police agency using the technology to be held accountable for the way they use it. This also prevents the arbitrary use of police data in a way that violates the constitutional rights of the accused. Transparency and procedural due process measures will help ensure that constitutional protections are enforced, and personal data is being used properly and efficiently.

\textsuperscript{174} \textit{Id.}
Accountability must also be shared with the technology companies that are providing the algorithms and programs police departments use to restrain suspects’ liberty. Tech companies should not be able to hide behind supposed trade secrets when it causes police departments to be unable to articulate or defend their methodology, something that becomes imperative when an arrest is questioned in court. Accountability in this sense may take the form of requiring tech companies to disclose the algorithms used in programs they license to police departments they know will be using them for the administration of justice.

Conclusion

Developing predictive policing technology continues to erode the accused’s right to be presumed innocent. The lack of transparency from police departments leads to the arbitrary use of these systems and the absence of accountability methods on artificial intelligence models leaves criminal defendants with little recourse against improper arrests based on predictive data. Despite the constitutional pitfalls of many predictive policing methods, they are most likely here to stay. The argument lies not in the eradication of such methods, but in their regulation. Therefore, legislation needs to be implemented that will require transparency and accountability from police departments using this technology so that the presumption of innocence is not completely eroded.