Pre-Crime Prediction: Does It Have Value? Is It Inherently Racist?

David H. McElreath, University of Mississippi, USA
Sherri DioGuardi, University of Central Missouri, USA
Daniel Adrian Doss, University of Tennessee, USA*

https://orcid.org/0000-0002-3393-0488

ABSTRACT

This paper considered the emerging use of predictive analytics in the justice domain with respect to potential bias. It discussed predictive algorithms and methods from the perspectives of reported crime and community safety in the United States. Although predictive algorithms, techniques, and implementation contexts are emerging, imperfection exists with respect to their use. Despite any effectiveness or efficiency of using predictive algorithms, such use should neither deny human rights nor transgress societal laws. Regardless, the emergence of predictive policing fuels and enhances the classic debate of balancing liberty versus security within a civil society.

KEYWORDS

INTRODUCTION

It is unsurprising that data sets are used to anticipate crime. In the modern world, data drives decisions continuously. Prediction using algorithms is not new. For instance, the insurance industry has used predictors for decades in determining risk (Boodhun & Jayabalan, 2018). The banking industry employed algorithms to determine loan eligibility (Shie, Chen, & Liu, 2012). Political parties have collected and assessed data toward identifying, targeting, and influencing voters (van der Voort, Klievink, Arnaboldi, & Meijer, 2019). The marketing industry continually developed, refined and shaped messages to potential consumers (Du, Rong, Michalska, Wang, & Zhang, 2019). Amazon, Facebook, and Google all used machine learning techniques to analyze data derived from their customers (Hewage, Halgamuge, Syed, & Ekici, 2018). Each of these industries and corporations developed data sets to identify and target their respective consumers. What has changed over time is the advancement and refinement of the technology used to analyze the data. Artificial intelligence (AI) spawned Deep Learning (DL) involving artificial neural networks, modeled from the human brain, by applying a set of algorithms whereby the ‘machine’ will reach a solution to a specific problem (Marr, 2016a). For instance, Facebook’s DeepFace is a DL application that accurately recognized faces at a 97% success rate, as compared to the human success rate of 96% (Marr, 2016b). Even at a 97% success rate, it means that very accurate application will still get it wrong 3% of the time.
From a law enforcement and community safety perspective, the foundation for crime prediction is the concept that people behave predictably (to some degree) and future behavior may be both anticipated and predicted (Hayes, 2015). If Hayes’s assertion was true, can human behavior data be analyzed to examine whether behavior patterns may be anticipated? As a result, could more efficient intervention to deter crime and maintain societal order be crafted while not crossing the line with civil or human rights violations?

**PREDICTIVE ALGORITHMS**

*Cambridge Dictionary* (n.d.) defined algorithms as “a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem.” Predictive algorithms relied on artificial intelligence (AI) being applied to machine learning (Marr, 2016a), and all three (algorithms, machine learning, and artificial intelligence) were based on mathematical principles, such as probability theory and inferential statistics. Rigano (2019, para. 4), indicated that, “Conceptually, AI is the ability of a machine to perceive and respond to its environment independently and perform tasks that would typically require human intelligence and decision-making processes, but without direct human intervention.” While people should tend to think of mathematics as dealing in absolute truths and as an objective science, O’Neil (2016, 2017), a mathematician and data scientist, insisted that algorithms were nothing more than opinions embedded in code. An algorithm was a computer-coded instruction, written by human programmers, that allowed the discerning of patterns within massive amounts of historical data. Afterward, by assuming found patterns were fixed facts, outcomes of future predictions were provided for single locations and/or individual people (Ferguson, 2017a). In the case of crime prediction, ‘hot spots’ were flagged. Regarding recidivism risk, a single score was assigned to individuals identifying them within the justice system as having a high risk to recidivate. These predictive algorithms were used, over the past half dozen years, as supportive tools for decision-making within all components of the criminal justice system (courts, corrections, and law enforcement). Within policing, predictive algorithms have become a “multi-million dollar business” (Ferguson, 2017a, p. 1132).

**LAW ENFORCEMENT DATA ANALYSIS**

It should be unsurprising that law enforcement in the United States uses such emerging technologies toward more efficiently providing a wide range of services. Business entrepreneurs identified the law enforcement community as a consumer of technology. They continuously adapted technologies to appeal to the law enforcement arena (McElreath, et al., 2013).

The nature of law enforcement was historically reactive by responding to calls for assistance. Law enforcement agencies across the nation used ‘hot spot analysis’ in an attempt to anticipate future service needs. For many agencies, the analysis consisted of compiling lists of reported crimes and calls for assistance, overlaying those locations onto a map, and assigning departmental resources within those areas. The public safety sector identified and employed strategies from the ones that were capable of employing and utilizing resources (McElreath et al., 2014). Regarding a primary goal of predictive policing, the focus shifted toward forestalling future crime rather than emphasizing traditional crime response (Zedner, 2007). This was a focus on pre-crime versus post-crime. Pre-crime, as a term, was first used by science fiction author, Philip K. Dick, in a novella titled *The Minority Report*, which later became a 2002 Steven Spielberg blockbuster movie (Wray, 2018).

Various RAND researchers identified several categories of predictive methods in use to forecast, places vulnerable to crime, persons at risk of offending in the future, likely offenders of past crimes and potential victims of crime (Hayes, 2015). The RAND researchers cautioned, however: “[C]ompared with predictions related to spatiotemporal crime techniques, methods for making predictions involving people are much less mature” (Perry et al., 2013, p. 81) and recognized the potential civil rights violations inherent in predictive methods targeting individuals. The Level of Service Inventory – Revised (LSI-R) was a frequently used tool to assess and classify offender risk by using 54 items to
calculate a single score for any person; the higher the score, the greater the presumed risk (Perry et al., p. 81). O’Neal (2016) criticized the LSI-R for using information that was inadmissible in a court of law because of its prejudicial nature, such as “circumstances of a criminal’s birth and upbringing, including his or her family, neighborhood, and friends” (p. 26). While some states used the LSI-R merely as a tool in order to determine who should receive anti-recidivism treatment programs while imprisoned, other states depended on the scoring to make decisions on length of sentencing (O’Neal, 2016). Thus, there is a qualitative difference in whether the predictive method was used to help or harm an individual inmate. Ultimately, the decision on whether applying such a predictive technique was constitutional depended entirely on the palliative-punitive intention.

While the potential application of the technology was significant, in one way or another predictive policing was implemented for years and predated the development of the computer (McElreath et al., 2013, p. 229). Doss, et al., (2013, p. 501) indicated that early predictive approaches attempted identification of “individual tendencies” or “key indicators” through which predicting future behaviors could occur. Additionally, Holmes and Holmes (2009) indicated that profiling was used for predicting risks of criminal incidents and criminal behaviors. Law enforcement agencies have long identified high crime areas and criminal hot spots into which increased resources are typically directed. Drawing from earlier theories of resource utilization in law enforcement, the concept of preventive patrol which embraced the idea of significant law enforcement presence in an area would deter criminal activity, was accepted as a productive enforcement strategy. The use of this technology for predicting crime opened a new dimension in the strategic response to crime as the technology evolved.

**PRE-CRIME ANALYSIS AND PREDICTIVE ENFORCEMENT**

The goal of predictive policing was to forecast where and when crimes would occur (Moses & Chan, 2016). However, was data analysis for the purpose of pre-crime prediction another form of profiling, which in itself was controversial? While solid data from which to determine true value was largely unavailable, various firms worldwide claimed and anticipated its value.

The tech firm Predictive Policing (PredPol), a California company formed in 2012, claimed data analytics algorithms could improve crime detection by somewhere between 10% to 50% in some cities (Smith, 2018) through identification of areas in a neighborhood where serious crimes were more likely to occur during a particular period (Rieland, 2018). PredPol used an analysis initially developed for earthquake prediction, which was modified to predict crime (Moses & Chan, 2016). Police department officials used this data to direct assignment of resources toward deterring criminal activity or responding more efficiently to incidents (Lapowsky, 2018). PredPol maintained a focus on using past data to predict future property crimes. Three data points were used to develop its analytical model: crime type, crime location, and crime date/time.

Within the PredPol (2020) Internet site, an overview of the algorithm was displayed, and the site explained how the model included the three aspects of offender behavior: repeat victimization, near-repeat victimization, and local search. Repeat victimization assumed, for instance, that once a house was burglarized, the likelihood of that same house being burglarized again was increased. Near-repeat victimization assumed that every house in the surrounding neighborhood would then be at increased risk of being burglarized, and local search assumed that burglars would continue to operate within their established comfort zone area. The premise was that past behavior or events would reliably predict future behavior or future events. At least 60 police departments nationwide used PredPol as a predictive policing tool (Puente, 2019). The Los Angeles Police Department (LAPD) developed PredPol in collaboration with a UCLA professor. After a 2019 internal audit, the LAPD reported that there was not enough evidence to definitively state that PredPol was instrumental in reducing crime (Puente, 2019). Such lack of evidence was unsurprising. For instance, despite the usefulness of artificial intelligence approaches, human knowledge regarding initiatives involving data management and AI was constrained with respect to strategic initiatives (Lichtenthaler, 2021).
Lum and Isaac (2016) and the Human Rights Data Analysis Group (HRDAG) compared police records in Oakland, California, with a “demographically representative synthetic population” (para. 16) database of all crimes in Oakland, whether reported to police. This was done by estimating the number of drug users in that area through utilization of the 2011 National Survey on Drug Use and Health (O’Donnell, 2019). Lum and Isaac (2016) found PredPol dispatched police more often to minority neighborhoods and concluded that the PredPol algorithm tended to target Blacks at two times the rate of Whites. This disparate outcome was a consequence of a “pernicious feedback loop” (O’Neil, 2016, p. 87) in which predictive policing deployment created new data which justified and reinforced previous patterns observed in the original data.

A Chinese company, Cloud Walk, developed technology allowing it to track the travel patterns of people and rate them on how likely they were to commit a crime using location data. HIS Markit, an industry research company, reported that China currently has over 170 million surveillance cameras in place (Ng, 2017). Researchers at Shanghai Jiao Tong University performed a study linking criminality and facial images. Training algorithms with headshots of over 1,000 faces from government IDs and 700 criminal images were used as a basis for recognition functions. Such supervised learning systems could segregate criminal and non-criminal groups and determine reoccurring traits in both sets (Reaney, n.d.). China’s widespread use of machine-learning algorithms for predicting crime and for preemptively detaining citizens brought criticism from the Human Rights Watch (HRW, 2018) which reported that Chinese ethnic minority groups received disproportionately higher risk scores, and these scores appeared to be – at least to some degree – related to religious practices (i.e., information was collected on how many times per day a person prayed). The HRW estimated that, in only a two-year period, tens of thousands of ethnic minorities, because of elevated scores, were sent to “political education centers” (HRW, para. 4), and some detainees were subsequently sent to prisons.

In searching for information pertaining to the use of computer-based resources by law enforcement in the prediction of crime trends, the technology was applied to a wide range of perceived threats. McCulloch and Pickering (2009) discussed the use of the information drawn from computer-based process in the struggle against radicalism in the United Kingdom. In 2001, 9/11 occurred within the United States, and then in 2005 the 7/7 bombings occurred within the United Kingdom; both were considered causative events for the heightened need for preemptive security measures globally (Dencik, Hintz, & Carey, 2018; Gillham, 2011). National security threats catalyzed the integrating of big data and probability theory to determine future risk (Arodou & Blanke, 2015; Dencik, Hintz, & Carey, 2018; & Hildebrandt, 2013). The British Broadcasting Company (BBC) reported that, out of the 14 police forces identified by Liberty as utilizing predictive policing programs, two of them – the Cheshire and Kent police forces – had terminated their use (Kelion, 2019).

The Los Angeles Police Department expanded the use of computer-based data during Operation ASER in 2011, which rates individual potential involvement in crime within a point system. The LASER system considered individual criminal history, including gang membership or affiliation, prior arrests and convictions, probation, and parole status. Those with high scores were identified and listed within the Chronic Offender Bulletin (Lapowsky, 2018). Uchida and Swatt (2013), through a panel design study, found that Operation LASER was effective in decreasing gun crime by 5.2% in the Newton Division of Los Angeles (the area covered by Newton patrol officers). When individual reporting districts (RDs) within the division were analyzed, the results showed that RDs utilizing interventions for both chronic offender and for chronic location were successful in decreasing gun crime.

The city of Memphis, Tennessee applied data analysis within the city’s Blue CRUSH (Crime Reduction Utilizing Statistical History) initiative beginning in 2006. Initially started as a pilot program, Operation Blue CRUSH was first launched in 2005 (Ashby, 2006). While the Blue CRUSH attracted nationwide attention with its use of data-driven enforcement, the benefit of the program was undetermined (Tulumello, 2016). The Memphis Police Department (MPD) indicated that both overall crime and violent crime had decreased as a result of Blue CRUSH, and a Nucleus Research
case study reported an 863% return on MPD’s investment in the predictive software (Kanarakus, 2010; Perry et al., 2013);

The software Beware analyzed behavior patterns and criminal trends to predict future activity by providing law enforcement officers with a color-coded threat score for an individual. It was derived from predictive algorithms that processed data from three sources: criminal records, purchased commercial information, and information publicly accessed from social media (Hoggard, 2015; Yang, 2019). One of the concerns was the potential of error and identifying people with nothing to do with crime. For instance, Ferguson (2017b) described that during a public hearing on the Beware program, one of the local council members requested that his address be run through the system, and the results were that his home was flagged as “an elevated yellow threat level” (p. 85), and no one present could explain why that city official’s residence was misidentified as high risk.

Instead of relying solely on predictive algorithms, the use of the data analysis might best be viewed as a solitary step in the process of crime response. As the application of automated data analysis is relatively new within the justice domain, continued refinements of software and its application will occur through time.

The information placed in many of the predictive policing algorithms was drawn from a wide variety of sources, not just the records of the justice agencies (i.e., see Beware above). Criminologists addressed crime and behavioral theories to anticipate future activity. For almost a century, social science researchers have recognized the significance of family and peer influence, economic and social conditions, and labeling as factors influencing behaviors (including criminal and deviant behaviors). The significance of relationships in data analysis played a key role in predicting not only the future of someone, but also of others who are similar. As an example, certain stressors had greater influence than others regarding those committing criminal offenses (Agnew & Scheuerman, 2015).

Additionally, Elijah Anderson (1994), in *The Code of the Street*, classified social units as families, the decent families, and the street families. He believed the decent families were more inclined to accept the values of mainstream society while street families demonstrated a lack of consideration of those values and of others. From the models he proposed, the children from the street families had a greater tendency to become involved in patterns of criminal behavior (Anderson, 1994).

If humans are creatures of habit, then it is reasonable to assume that the future may also be predictable. A consistent conclusion in the criminological literature is that past behavior can be a predictor for future behavior (Akers, 2017). Coding has no conscience, but the results of any analysis depend on the accuracy of the information entered into the system, the method of processing, and the ability of analysts to place outcomes within a larger context for proper interpretation.

**IS PRE-CRIME ANALYSIS ANOTHER FORM OF PROFILING?**

**CRITICISM OF DATA ANALYSIS IN CRIME PREDICTION**

There are concerns about racial and other biases hidden within datasets. Pre-crime software was intended to predict where and when specific crimes will occur. The information from which the analysis was drawn must remain updated in order to provide usable forecasts. Most predictive analysis depends on the input and analysis of three types of information: 1) information as to the type of crime committed or nature of the call for service, 2) the location the offense or call for service and 3) the time of the call for service or crime. This information, when analyzed, can be used to predict crime and service calls. Human reasoning was needed to analyze the data and to understand its limitations. The human aspect of decision algorithms must not be discounted. After all, sound outcomes from decisions result from good decision processes (Galli, 2020). As Pearl and Mackenzie, award-winning computer scientist and statistician, respectively, and well-known proponents for the probabilistic approach to A.I., cautioned: “[D]ata are profoundly dumb” (p. 6). Machine learning presumes reliable input to produce outcomes through the process of recognizing patterns within the data. Even Deep Learning systems will not know if those patterns are predicated on past prejudicial practices, and the old adage applies: garbage in, garbage out (Perry et al., 2013).
While members of society reject the use of age and race as an element of profiling, it is difficult to believe those elements are not factors in crime prediction because much individual information is available among any number and type of interconnected data bases. From a moral perspective, there was always a concern how data was used resulting in judgements. One major concern was the body of research suggesting that minority neighborhoods may have been historically overpoliced thereby resulting in disproportionately higher arrest rates for African Americans (Beckett, Nyrop, & Pfingst 2006; Black & Reiss, 1970; Gaston, 2019; Hetey & Eberhardt, 2018; Kochel, Wilson, & Mastrofiski, 2011; Lynch et al., 2013; Smith & Holmes, 2014; Smith, Visher, & Davidson, 1984). Therefore, even when race is not explicitly included in formulating an algorithm, frequency of arrests will be included, which means that past policing actions – whether legitimate or not – will be perpetuated by any machine learning system. Expecting a good outcome from bad input is, according to Bakke (2018), “like expecting Google Maps to find your destination after you typed in the wrong address” (p. 135). Claiming machine learning output is objective when dirty data were used is what critics call “tech-washing” – which is the idea that “the veneer of machine empiricism” covered injustice (Rainie & Anderson, 2017). Was there a reason for concern? History demonstrated that injustices, and even atrocities, occurred in the name of science (Shapiro, 2020; Weigmann, 2001). Thus, it became prudent to proceed with caution when using predictive algorithms as a decision-making tool.

On the other hand, there is value in being able to foresee and forestall tragedy. The individual responsible for the killings at the Pensacola Naval Air Station posted on his Twitter account statements about his hatred of the United States (a possible red-flag of future violence). Unfortunately, the postings were unidentified and not reported to the military or law enforcement rapidly enough to have prevented the tragedy (Schmitt, Robles, & Bogel-Burroughs, 2019).

PROBLEMS WITH PREDICTING FOR AN INDIVIDUAL

Hildebrandt (2013) referred to “Big Data” as a proper noun and succumbed to perceiving big data algorithmic systems as having minds of their own. Big data involves the amalgamating of a vast accumulation of semi-structured, unstructured, and structured data (Sangwan & Bhatnagar, 2020). Big data processing necessitated a much greater quantity of computing, processing, and storage capacities than ordinary database systems (Sangwan & Bhatnagar, 2020). Within the context of the justice system, big data applications were appropriate for fraud detection (Sangwan & Bhatnagar, 2020). Deep learning systems were deemed “high speed real time autonomic computing systems that increasingly determine our external environment” (Hildebrandt, 2013, p. 2). They were touted as being extremely accurate, more so than smaller data driven systems, mainly because of the massive amounts of data they analyzed. It was claimed that their “n” equaled “all” (n=all) meaning that they did not have to worry about generalizing to a larger population as they claimed to be the population. The bottom line, however, was that they were data modeling systems (Hildebrandt, 2013, p. 2), and very similar to O’Neil’s (2016, 2017), termed them as opinions embedded in code. All predictions, even when machine-generated, are estimates (Perry, et al., 2013), and estimates are nothing more than educated guesses (Siegel, 2017).

Statistics were useful for aggregates and sample descriptors, and not for individuals. Although individual data point estimators were made in any model for a sample in order to generate ‘predictions’ for the population and generalize findings from the sample, it did not mean that individuals within any population were individually pinpointed with any degree of accuracy for a certain future outcome. For instance, it is accurate to state that someone fits into a category in which 70% of the people will reoffend and 30% will not, but one would have to be either a psychic or genuine fortune-teller to know whether one specific ‘someone’ will end up being in the 70% or 30% subgrouping.

Much can be learned from the literature within bioethics and reputable medical journals. When doctors predict a chance of survival for a single terminal patient, the prediction seldom lines up with actual survival (Christakis & Lamont, 2000; Glare et al., 2003). Unless all possible variables for the individual person can be considered – even ones for which there is currently no known measurement
– a 100% accurate and reliable individual prediction is impossible. Henderson and Keiding (2005, p. 703) surmised the reasoning as, “[In all realistic scenarios we can imagine, the intrinsic statistical variations in lifetimes are so large that predictions based on statistical models and indices are of little use for individual patients. This applies even when the prognostic model is known to be true and there is no statistical uncertainty in parameter estimation.” Henderson and Keiding (2005) concluded, “Prognostic indices or palliative scores can be useful in assigning patients to risk groups and from some viewpoints—insurers perhaps—all that is necessary is to know the proportion of each group who will survive any given time. A difference between groups of 10% in one year’s survival probability can be important. For the individual patient however, our view is that such a between-group difference is small compared with the variability in residual lifetimes, even between patients with identical characteristics” (p. 705). This conclusion can be equally applied to pre-crime predictions for individuals. The inherent dangers associated with artificial intelligence and deep learning systems was what prompted the Future of Life Institute, in 2017, to publish a list of 23 Principles for Beneficial Artificial Intelligence, which was signed by over 1,600 AI researchers, including Steven Hawking (Rainie & Anderson, 2017). Boddington (2017, p. 105) indicated that a primary AI goal was, “. . . to create not undirected intelligence, but beneficial intelligence.” The following principles were particularly relevant to predictive algorithms implemented within the criminal justice system:

- Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.
- The application of AI to personal data must not unreasonably curtail person’s real or perceived liberty.
- The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.

An inevitable error rate existed which shall always be a part of forecasting and prediction. When future dangerousness predictions were evaluated, the findings showed that false-positive rates were significantly higher than false-negative rates; this meant that, on average, people were wrongly classified as high risk 65% of the time (Slobogin, 1984, 2006). Thus, false-positives must be considered from a constitutional rights perspective.

COURT RULINGS ON PREDICTIVE ALGORITHMS

Although the United States Supreme Court has not yet heard a case directly regarding the use of predictive algorithms within the criminal justice system, two state appellate courts rendered judgments (Zavrsnik, 2020). In 2016, *Loomis v. Wisconsin* (2016 WI 680), Wisconsin’s Supreme Court Judge Bradley affirmed the circuit court’s decision in allowing COMPAS, a risk assessment tool, to be one factor in sentencing a defendant. Justice Bradley ruled, “We determine that because the circuit court explained that its consideration of the COMPAS risk scores was supported by other independent factors, its use was not determinative in deciding whether Loomis could be supervised safely and effectively in the community” (p. 244). Interestingly, Judge Bradley, in her written opinion, referenced the American Bar Association’s recommendation that the states adopt assessment tools. Judge Roggensack, in a concurring opinion in order to clarify the Court’s position, wrote: “[C]onsideration of COMPAS is permissible; reliance on COMPAS for the sentence imposed is not permissible” (p. 286).

The Kansas Supreme Court, as of 2014, in Rule 110B(c) mandated that judicial branch court services officers complete the LSI-R assessment (2017 Kan. S.Ct. R 182). In *Kansas v. Walls* (396 P.3d 1261, 2017), a sentence was appealed on the grounds that the defendant was disallowed access to the LSI-R, which was relied on by the judge when probation conditions were imposed. The Kansas Court of Appeals vacated the defendant’s sentence and remanded the case back to the lower court “with directions to allow Walls access to the complete diagnostic LSI-R assessment and report” (para. 16).
CURRENT LIMITATIONS

The desire to accurately predict crime is not new. While the concept of predictive policing is clear, what is unclear (at this early stage in its development and evolution) are several issues. Ultimately, how effective will this tool prove to be when applied? Second, what type of data will be required to support the data analysis process (Hayes, 2015)?

Three major issues have been identified with predictive algorithms: accuracy, accountability, and transparency. No predictive algorithm, regardless of accuracy, will ever be 100% error-free. Amazon’s recommendation algorithm was highly successful and considered “optimized,” but was erroneous frequently (Fry, 2019). When Amazon’s predictive algorithm exhibited erroneous behavior, there were no dire consequences. Accountability involved the idea that machine decision-making allowed humans to be absolved from responsibility as well as the “temptation to outsource aspects of the decision-making process, and thus responsibility and accountability for the decision itself, to technological tools” (Moses & Chan, 2016, p. 817). Transparency was problematic because deep learning algorithms continually updated their pattern-finding function autonomously to reach the point where human programmers and/or analysts were unable to understand exactly how the final outcome was reached (i.e., the “black-box conundrum”) (O’Donnell, 2019, p. 546).

Another limitation of predictive algorithms was the lack of theoretical frameworks for interpreting the outputs and for formulating fair and effective law enforcement responses (Innes, Fielding, & Cope, 2005; Kitchin, 2014; Meijer & Wessels, 2019; Vlahos, 2012). Much of this may be attributed to the different domains involved with this policing tool, such as the private software companies seeking to generate income, as well as the computer programmers and data analysts far removed from the human elements involved. Accountability and transparency were important considerations to ensure external stakeholder buy-in to the benefits, but a better understanding of evidence-based theory – such as Tyler’s procedural justice theory (1990) in which personal respect and concern for human dignity were prioritized – provided a basis for ensuring that internal stakeholders remained acutely aware that machine learning need not (and, in an ethical sense, should not) automatically result in a machine-generated decision. A computer cannot substitute for humanity when it comes to interpreting context or understanding the complexities involved in the ‘why’ of any generated score; that will always require human reasoning.

Again, a lesson from medicine may be appropriate: do no harm. In the case of predictive policing, it would mean doing no harm to either society or to its citizens. The cost of public safety is too high if it comes at the expense of private citizens’ rights. The public may be more accepting of machine-generated predictive policing if it resulted in (rather than purely punitive objectives) social services directed toward those at risk in an attempt to break past patterns in people or places. A carrot is easier to accept than a stick, and may be more effective in the long run.

ORGANIZATIONAL USE OF PREDICTIVE TOOLS

Entities within the federal justice system may have sufficient budgets to afford sophisticated predictive tools and resources whereas smaller organizations, such as a small-town sheriff’s office or a state police entity, may lack financial resources to expend toward purchasing such large-scale systems. Their predictive analyses may accommodate crime that occurs within their respective jurisdictions. For instance, they may predict the quantity of traffic tickets that occur within a given period via the use of the moving average technique. Hyndman and Athanasopoulos (2018) indicated that the concept of moving average originated in the 1920s, and was extensively used through the 1950s. Mathematically, Doss, Guo, and Lee (2012) indicated that its fundamental premise was the summation of demand within the preceding $n$ periods divided by the number of periods used within the moving average.

Although they may have a need to implement mathematical formulae, they may lack sophisticated software (e.g., SPSS, SAS, etc.) and personnel knowledgeable of its operations. In such cases, they
may acquire predictive tools that are commensurate with their municipal budgets, such as Microsoft Excel or Calc (Doss, et al., 2013; Doss, Sumrall, & Jones, 2012). Calculating a moving average may be accomplished through the use of MS Excel or Calc. With respect to predictive methods, the Excel data analysis function facilitates the use of moving averages and regression. For example, if an agency desired to implement a moving average for predictive purposes, use of MS Excel would be both affordable and straightforward. Using public, open access secondary data obtained from the Federal Bureau of Investigation Uniform Crime Reports database, implementing a moving average within MS Excel could easily be accomplished by specifying the ‘Moving Average’ function from the Data Analysis interface. Next, one would enter the desired data input range of cells, the interval period, and the desired cell for generating data output. The period for generating the moving average values was five years. Table 1 shows the results of these steps when applied against motor vehicle theft data for the state of Mississippi spanning twenty years.

Table 1 MS Excel Moving Average

<table>
<thead>
<tr>
<th>Year</th>
<th>State</th>
<th>Motor Vehicle Theft</th>
<th>Moving Average Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>Mississippi</td>
<td>9473</td>
<td>#N/A</td>
</tr>
<tr>
<td>2002</td>
<td>Mississippi</td>
<td>9523</td>
<td>#N/A</td>
</tr>
<tr>
<td>2003</td>
<td>Mississippi</td>
<td>8996</td>
<td>#N/A</td>
</tr>
<tr>
<td>2004</td>
<td>Mississippi</td>
<td>7879</td>
<td>#N/A</td>
</tr>
<tr>
<td>2005</td>
<td>Mississippi</td>
<td>7492</td>
<td>8672.6</td>
</tr>
<tr>
<td>2006</td>
<td>Mississippi</td>
<td>8330</td>
<td>8444.0</td>
</tr>
<tr>
<td>2007</td>
<td>Mississippi</td>
<td>7191</td>
<td>7977.6</td>
</tr>
<tr>
<td>2008</td>
<td>Mississippi</td>
<td>6252</td>
<td>7428.8</td>
</tr>
<tr>
<td>2009</td>
<td>Mississippi</td>
<td>5439</td>
<td>6940.8</td>
</tr>
<tr>
<td>2010</td>
<td>Mississippi</td>
<td>5359</td>
<td>6514.2</td>
</tr>
<tr>
<td>2011</td>
<td>Mississippi</td>
<td>4908</td>
<td>5829.8</td>
</tr>
<tr>
<td>2012</td>
<td>Mississippi</td>
<td>4329</td>
<td>5257.4</td>
</tr>
<tr>
<td>2013</td>
<td>Mississippi</td>
<td>4387</td>
<td>4884.4</td>
</tr>
<tr>
<td>2014</td>
<td>Mississippi</td>
<td>4474</td>
<td>4691.4</td>
</tr>
<tr>
<td>2015</td>
<td>Mississippi</td>
<td>4271</td>
<td>4473.8</td>
</tr>
<tr>
<td>2016</td>
<td>Mississippi</td>
<td>4307</td>
<td>4353.6</td>
</tr>
<tr>
<td>2017</td>
<td>Mississippi</td>
<td>4347</td>
<td>4357.2</td>
</tr>
<tr>
<td>2018</td>
<td>Mississippi</td>
<td>5145</td>
<td>4508.8</td>
</tr>
<tr>
<td>2019</td>
<td>Mississippi</td>
<td>5721</td>
<td>4758.2</td>
</tr>
<tr>
<td>2020</td>
<td>Mississippi</td>
<td>6083</td>
<td>5120.6</td>
</tr>
</tbody>
</table>

*Note:* If Excel lacked sufficient information to determine a moving average for any standard error, it generated an error message within the specific cell. Therefore, the initial cells of the Moving Average Value column show the value of #N/A. The ‘Motor Vehicle Theft’ column shows values per 100,000 population.

Justice system entities may also use MS Excel to perform regression analysis. With respect to the years between 2001 and 2020, a question may be explored: What was the relationship between automobile theft incidents between the states of Mississippi and Alabama? Both were adjacent states
that shared numerous transportation routes. Initially, in order to ensure that mathematical analysis could occur, data values across the years were expressed in the terms of annual crime incidents per 100,000 population. Doing so ensured a ratio basis for comparison of crime rates through time and accommodated population fluctuations. Table 2 shows the data sets expressed in the terms of motor vehicle thefts per 100,000 population.

Table 2 Mississippi versus Alabama – Motor Vehicle Theft

<table>
<thead>
<tr>
<th>Year</th>
<th>Alabama per 100k</th>
<th>Mississippi per 100k</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>282.37</td>
<td>331.25</td>
</tr>
<tr>
<td>2002</td>
<td>310.12</td>
<td>332.19</td>
</tr>
<tr>
<td>2003</td>
<td>332.10</td>
<td>312.08</td>
</tr>
<tr>
<td>2004</td>
<td>309.90</td>
<td>271.62</td>
</tr>
<tr>
<td>2005</td>
<td>288.90</td>
<td>257.59</td>
</tr>
<tr>
<td>2006</td>
<td>326.55</td>
<td>286.20</td>
</tr>
<tr>
<td>2007</td>
<td>307.66</td>
<td>246.37</td>
</tr>
<tr>
<td>2008</td>
<td>288.85</td>
<td>212.75</td>
</tr>
<tr>
<td>2009</td>
<td>235.54</td>
<td>184.25</td>
</tr>
<tr>
<td>2010</td>
<td>225.27</td>
<td>180.43</td>
</tr>
<tr>
<td>2011</td>
<td>221.95</td>
<td>164.84</td>
</tr>
<tr>
<td>2012</td>
<td>204.96</td>
<td>144.95</td>
</tr>
<tr>
<td>2013</td>
<td>218.51</td>
<td>146.61</td>
</tr>
<tr>
<td>2014</td>
<td>209.25</td>
<td>149.46</td>
</tr>
<tr>
<td>2015</td>
<td>212.98</td>
<td>142.87</td>
</tr>
<tr>
<td>2016</td>
<td>241.04</td>
<td>144.27</td>
</tr>
<tr>
<td>2017</td>
<td>262.50</td>
<td>145.40</td>
</tr>
<tr>
<td>2018</td>
<td>271.56</td>
<td>172.59</td>
</tr>
<tr>
<td>2019</td>
<td>258.68</td>
<td>192.09</td>
</tr>
<tr>
<td>2020</td>
<td>222.00</td>
<td>205.04</td>
</tr>
</tbody>
</table>

Afterward, using the Excel Data Analysis menu, the regression option was chosen to examine the relationship between the Mississippi and Alabama values. Using an alpha value of 0.05 and the $p$-value approach regarding the hypothesis that no relationship existed between the Mississippi and Alabama data sets representing motor vehicle theft, the Excel regression analysis showed a statistically significant outcome ($p = 0.00; \alpha = 0.05; \text{Multiple } R = 0.83; R^2 = 0.69$). Thus, the null hypothesis was rejected in favor of the alternative hypothesis that some relationship existed between Alabama and Mississippi motor vehicle theft.

Both the values of Table 1 and Table 2 were analyzed using MS Excel. Excel is an acceptable resource for data sets of such size and type (Anderson, Sweeney, & Williams, 2015). Usually, justice systems entities may have available a copy of Excel (or Calc) as a component of its office suite (Doss, Sumrall, & Jones, 2012; Doss, Sumrall, McElreath, & Jones, 2013). In so doing, the chances are
greater that justice system personnel may be easily trained to use Excel software to perform a variety of predictive functions.

CONCLUSIONS, IMPLICATIONS, AND RECOMMENDATIONS

Conclusions

Does this article make the claim that predictive algorithms have no value? Not at all. The desired outcome or value of precrime prediction is to facilitate safer communities. Within this outcome is embedded the hope of more efficient assignment and usage of justice system resources. However, when attempting to achieve some level of security, some may question the pervasive use of technology as a means of enhancing enforcement. In other words, issues may arise regarding the basic premise of the immutability of security versus liberty with respect to the emerging of an integration of predictive technologies, policing, and enforcement. Where would demarcation occur between perceptions of an authoritarian state versus one of civil freedoms, liberties, and privacy? After all, technology is a neutral tool useful for fulfilling human purposes. However, the human intention toward achieving any given purpose may be utopian, dystopian, or neutral.

Despite moral, legal, or ethical debates or questions, the developing and refining of predictive tools are continuous processes. While it is impossible to identify and input information on every single crime that is committed, or to ensure data will be coded accurately, predictive policing appears promising. As time passes and the collection, analysis, and use of the data and corresponding predictive methods and models become further refined, their practical and societal values will increase. After all, the justice system is an agent for public good within society. In other words, public sector organizations are intended to ensure public safety and service. From the lens of public service, their resources exist to generate outcomes that are societally beneficial (Baporikar, 2020).

Predictive resources may be viewed in terms of resource availability and allocation within the context of justice system organizations. For instance, large organizations, such as federal agencies (e.g., U.S. Marshal Service, Federal Bureau of Investigation) may possess large-scale tools for performing predictive analysis, but smaller or local law enforcement agencies may lack such resources. Regardless, they still possess the ability to perform some types of predictive analysis, such as the moving average example demonstrated herein.

Implications

Some uses of predictive technologies involve recidivism. When one has paid a debt to society for a crime committed and completed a period of imprisonment, then would former offenders be prone to heightened scrutiny via the use predictive technologies? After all, if the debt to society was paid and one regained freedom, then would not the members of a civil society disfavor intrusions of privacy or surveillance of specific individuals (unless some form of post-condition was mandated)? Basically, how would society view the various uses of predictive tools as a measure to diminish recidivism? If such technologies showed substantial promise toward abating the recidivism rate thereby reducing the impact of crime and decreasing the societal costs of the justice system, how would society react to their use(s)?

However, even if the predictive algorithms were to become 100% accurate (which currently could never be), they should not come at the expense of human rights. Given the constraints of technology, decision domains, and data, there will always be an error rate involved in forecasting or predicting the behavior of one single individual or any single location, and there will also always be unforeseen and unintended consequences when certain neighborhoods or people are targeted for more intensive surveillance. There is an old truism: If you look for dirt, you will find it.
Recommendations

This article highlighted the primary concepts that were fundamental to the emerging domain of predictive policing. Thus, any consideration of the integrating of man and machine was beyond the scope of discussions herein. However, Guermah, et al., (2021, p. 110) indicated that systems considerations were secondary to emphasizing the “user and his actions.” Future studies may examine predictive policing from the perspective of human-computer interaction.

Future research may consider viewing prediction from the perspective of resource allocation. With respect to the precrime prediction goal of safer communities, one may consider the efficient assigning and using of agency resources toward generating public good. Such a context introduces the basic theme of economics: how does one allocate scarce, limited resources to satisfy the unlimited human needs and wants of society? Future studies may consider predictive algorithms and their uses from such a perspective.

The emerging and using of predictive technologies will influence policy decisions among a variety of organizations, both public and private. At the time of this writing, an insufficient amount of time existed for data to accumulate regarding the impacts of predictive policing from a long-term, strategic view. Frei and Ruloff (1989) and Doss, et al., (2021, 2020) indicated that an average of 20 years of data should be collected and analyzed before effective policy assessment or evaluation may occur. Given that upwards of two decades of data may be necessary for such analysis, future researchers may examine predictive tools as strategic organizational resources when sufficient time has passed to accumulate data.

FUNDING AGENCY

The publisher has waived the Open Access Processing fee for this article.
REFERENCES


Boddington, P. (2017). Towards a code of ethics for artificial intelligence. Springer. doi:10.1007/978-3-319-60648-4


---

**David H. McElreath** is Professor and former Chair, University of Mississippi, Department of Legal Studies. His research interests include criminal justice, homeland security, law enforcement, and terrorism.

**Sherri DioGuardi** is an Associate Professor at the University of Central Missouri. Her research interests include criminal justice and ethics.

**Daniel Adrian Doss** is an Associate Professor of Cybersecurity at the University of Tennessee. He earned a Ph.D. from Jackson State University. His research interests include business administration, cybersecurity, homeland security, information systems, and technology.