


# Cop Out:

## Automation in the Criminal Legal System

---

[www.copout.tech](http://www.copout.tech)

March 29, 2023

 GEORGETOWN LAW  
Center on Privacy & Technology

# Cop Out: Automation in the Criminal Legal System

---

## AUTHOR

Jameson Spivack, *Associate*

## CONTACT

[privacy@georgetown.edu](mailto:privacy@georgetown.edu) / 202-662-9779

## DESIGN

[rootid](#)

Cover Illustration by Lara Zigic, as part of a collaborative process,  
[larazigic.com](http://larazigic.com)

[www.copout.tech](http://www.copout.tech)

[www.law.georgetown.edu/privacy-technology-center](http://www.law.georgetown.edu/privacy-technology-center)

March 29, 2023

# Cop Out: Automation in the Criminal Legal System

---

The criminal legal system is increasingly fueled by algorithmic technologies like predictive policing, face recognition and risk assessments. Their use may worsen and make it more difficult to challenge existing inequities.

In February 2019, Nijeer Parks, a 33-year-old New Jersey man, was arrested after police accused him of shoplifting candy and attempting to drive a car into a police officer. As it turns out, Parks' arrest was the result of a face recognition<sup>1</sup> search that misidentified him as the suspect. In actuality, Parks was 30 miles away at the time of the incident, a fact of which he informed the police at the time of his arrest. In spite of his verifiable alibi, a judge denied Parks pretrial release, based in part on the “risk scores”<sup>2</sup> an algorithm generated, which suggested he was a risk to public safety.<sup>3</sup> Parks spent 10 days in jail.

Parks was the third publicly identified Black man to have been misidentified by police face recognition.<sup>4</sup> And he is one of countless others who have been denied bail because of an opaque risk assessment algorithm.<sup>5</sup> His story illustrates a major shift within the criminal legal system:<sup>6</sup> police, judges, prosecutors and other legal

---

1 Face recognition is a biometric technology that compares face images to determine the likelihood of a match, either for identification or verification purposes. For more on face recognition, see Appendix: Face recognition technology.

2 Risk assessment is a general class of algorithms that purport to predict the likelihood of an individual engaging in certain unwanted behavior in the future, specifically skipping bail, committing another crime or being rearrested. For more on risk assessment, see Appendix: Risk Assessment Tools (RATs).

3 Hill, K. (2020, December 9). Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match. *The New York Times*. <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

4 See Hill, K. (2020, June 24). Wrongfully Accused by an Algorithm. *The New York Times*. <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>. See also Anderson, E. (2020, July 10). Controversial Detroit facial recognition got him arrested for a crime he didn't commit. *Detroit Free Press*. <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002>. Since Parks' arrest, two more Black men – Randall Reid and Alonzo Sawyer – have been misidentified by police face recognition. See Simerman, J. (2023, January 2). JPSO Used Facial Recognition Technology to Arrest a Man. *The Tech Was Wrong*. *NOLA.com*. [https://www.nola.com/news/crime\\_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article\\_0818361a-8886-11ed-8119-93b98ecccc8d.html](https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html); Johnson, K. (2023, February 28). Face Recognition Software Led to His Arrest. *It Was Dead Wrong*. *Wired*. <https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong>.

5 Robinson, D. and Koepke, L. *Stuck in a Pattern: Early evidence on “predictive policing” and civil rights*. Upturn. (2016, Aug.) <https://www.upturn.org/reports/2016/stuck-in-a-pattern>.

6 This report uses the term “criminal legal system” to refer to what is commonly called the “criminal justice system.” Borrowing Oscar H. Gandy Jr.'s definition of the latter, it refers to “a complex amalgam of bureaucratic and administrative agencies that lend support and guidance to specialized agents responsible for the exercise of informed judgment about the use of force in their efforts to reduce crime and protect the public from those who would engage in criminal behavior.” See Gandy Jr., O.H. (2019). *The Algorithm made me do it! Technological Transformations of the Criminal Justice System*. *The Political Economy of Communication*, Vol. 7(2), 3–27. <https://www.polecom.org/index.php/polecom/article/view/110>. Put simply, this system includes police, prosecutors, defense attorneys, court systems, correctional officials and other actors engaged in enforcing a state's laws, prosecuting or defending the accused, and punishing those found to be in violation. There is also not one single, unitary “criminal legal system” but a vast array of actors engaged in work related to criminal law and justice that vary by jurisdiction. See Mayeux, S. (2018). The Idea of “The Criminal Justice System.” *American Journal of Criminal Law*, Vol. 45, 55–94. <https://scholarship.law.vanderbilt.edu/faculty-publications/898>.

authorities are increasingly using algorithmic technologies<sup>7</sup> to inform or make critical decisions about policing and punishment, which has profound consequences for peoples' rights and liberties.

Parks' story also illustrates a number of issues with algorithms in the criminal legal system. First, they make errors that have serious impacts on peoples' lives. As a result of face recognition and risk assessment, Parks was falsely arrested and imprisoned for 10 days. Second, they build upon one another in ways that can exacerbate the harms of each individual technology. The initial face recognition error led to Parks' wrongful arrest and imprisonment, funneling him into a criminal court proceeding in which a risk assessment algorithm's recommendation prolonged his incarceration. Finally, algorithms remove from public view contested questions about criminal justice — such as what the police's role should be, what makes a person dangerous and how society should respond to that person — while wrongly appearing, to many, neutral or objective. The algorithm that classified Parks as dangerous<sup>8</sup> was built on data from previous arrests and convictions, which means that the algorithm's recommendations were tainted by the well-documented racial disparities in the criminal legal system. That reinforces the status quo not only because the data itself is biased but also because developers privilege certain factors — namely arrest and convictions data — when building the algorithm.

At its most basic level, an algorithm is, according to the AI Now Institute, “the mathematical logic behind any type of system that performs tasks or makes decisions.”<sup>9</sup> In the criminal legal context, algorithms are built into software that police use to surveil people and that prosecutors, judges and correctional officials use to make decisions about the fate of those who come into contact with the system. Algorithms may replace or supplement human decision-making processes. They are ubiquitous in the criminal legal system, and as an individual moves through the system, nearly every decision legal authorities make about their rights and liberties may be mediated by algorithm. For example, crime forecasting directs police to patrol certain individuals and neighborhoods; face recognition provides investigators with potential identities of persons of interest; and risk assessment tools are used to determine whether a person gets bail or the level of supervision they receive during and after incarceration.<sup>10</sup>

Algorithmic technologies don't produce neutral<sup>11</sup> or objective<sup>12</sup> calculations. As legal scholars and social scientists have now exhaustively demonstrated, algorithms take their data from — and become integrated

---

7 In *Artificial Intelligence and Policing: First Questions*, Elizabeth Joh uses the term “artificial intelligence” in the context of policing to mean “the growing use of technologies that apply algorithms to large sets of data to either assist human police work or replace it.” This report uses the term “algorithmic technologies” or “tools” in a similar way. See Joh, E.E. (2018). *Artificial Intelligence and Policing: First Questions*. *Seattle University Law Review*, Vol. 41(4), 1139-1144. <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2550&context=sulr>.

8 New Jersey, where Nijeer Parks was arrested, uses the Public Safety Assessment (PSA) for pretrial risk assessment. See <https://www.njcourts.gov/courts/assets/criminal/psariskfactor.pdf>.

9 AI Now Institute. (2018, October). *Algorithmic Accountability Policy Toolkit*. <https://ainowinstitute.org/aap-toolkit.pdf>.

10 For a full discussion of algorithmic technologies used in the criminal legal system, see Appendix.

11 Mowshowitz, A. (1984). Computers and the myth of neutrality. *CSC '84: Proceedings of the ACM 12th annual computer science conference on SIGCSE symposium*, 85-92. <https://doi.org/10.1145/800014.808144>. See also Whelchel, R.J. (1986). Is Technology Neutral? *IEEE Technology and Society Magazine*, Vol. 5(4), 3-8. <https://doi.org/10.1109/MTAS.1986.5010049>.

12 Some technologists, law enforcement and policymakers claim algorithms are less biased than humans and therefore are the key to addressing inequity in the criminal legal system. See Miller, A. P. (2019, November 21). *Want Less-Biased Decisions? Use Algorithms*. *Harvard Business Review*. <https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms>. See also Mullainathan, S. (2019, December 6). *Biased Algorithms Are Easier to Fix Than Biased People*. *The New York Times*. <https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html>. See also Siegel, E. (2018, February 19). *How to Fight Bias with Predictive Policing*. *Scientific American*. <https://blogs.scientificamerican.com/voices/how-to-fight-bias-with-predictive-policing/>. See also Ovide, S. (2020, November 11). *A Case for Facial Recognition*. *The New York Times*. <https://www.nytimes.com/2020/11/11/technology/facial-recognition-software-police.html>.

with — existing systems, carrying with them the biases that already exist in the world.<sup>13</sup> For example, crime forecasting<sup>14</sup> makes predictions about where crime may occur in the future. But these forecasts are usually based on arrest and other police data, which reflects not just rates of previous criminal activity but also enforcement activity—and law enforcement more heavily polices Black, Brown and low-income communities.<sup>15</sup> The result is that historical racist and unfair practices — what Rashida Richardson, Jason Schultz and Kate Crawford call “dirty data” — form the foundation on which purportedly neutral technologies base their results.<sup>16</sup>

But the problem is not only that the data used to develop and train the algorithms derives from biased systems. It’s also that using algorithms at all requires accepting certain policy choices, which should remain the subject of political debate, as fixed or natural aspects of the criminal legal system.<sup>17</sup> Pretrial risk assessment algorithms, for example, are built on a set of assumptions: that the likelihood a person will commit another offense in the future should have a bearing on whether they’re released before trial; that the person’s arrest history is the most appropriate way to determine that likelihood; that certain previous offenses matter more than others in determining that; and so on.<sup>18</sup> These are public policy questions, and when developers build risk assessment algorithms, they are encoding particular answers to those questions within the algorithms. That works to inhibit external, public debate on these questions. When police officers, prosecutors and judges rely on those algorithms, the deliberative work of the justice system — weighing harms and equities, considering possible interventions in the context of system norms — is eliminated, condensed, outsourced or made superficial.

That is true for algorithms that inform a wide range of decisions made throughout the criminal legal system. How should a defendant be sentenced? Should an incarcerated person be released early? Where should police officers be stationed for patrol?

Each of those decisions reflect particular assumptions about both safety and justice. Algorithmic technologies, which are often designed by unaccountable private actors, standardize the process of making those decisions in a way that reinforces existing trends and values.<sup>19</sup> Given current inequities in the criminal legal system,<sup>20</sup>

---

13 For just a few examples, see Robinson, D. and Koepke, L. *Stuck in a Pattern: Early evidence on “predictive policing” and civil rights*. Upturn. (2016, Aug.) <https://www.upturn.org/reports/2016/stuck-in-a-pattern>; see also Eckhouse, L., Lum, K., Conti-Cook, C., & Ciccolini, J. (2018). Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment. *Criminal Justice and Behavior*, Vol. 46(2), 185–209. <https://doi.org/10.1177/0093854818811379>; Moy, L. (2021). A Taxonomy of Police Technology’s Racial Inequity Problems. *University of Illinois Law Review*, Vol. 139. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3340898](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3340898).

14 This report uses the term “crime forecasting” to refer to two separate but related processes: predictive policing and data-driven prosecution. Both of those methods involve analyzing historical crime data to inform future decision-making about who and where to police and prosecute. See Appendix: Crime forecasting.

15 Brayne, S. (2018). The Criminal Law and Law Enforcement Implications of Big Data. *Annual Review of Law and Social Science*, Vol. 14, 293–308. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3273800](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273800).

16 Richardson, R., Shultz, J., & Crawford, K. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review*, Vol. 94, 192–223. <https://www.nyu.edu/lawreview/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>. Eckhouse, L., Lum, K., Conti-Cook, C., & Ciccolini, J. (2018). Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment. *Criminal Justice and Behavior*, Vol. 46(2), 185–209. <https://doi.org/10.1177/0093854818811379>. See also Crawford, K. (2013, April 1). *The Hidden Biases in Big Data*. Harvard Business Review. <https://hbr.org/2013/04/the-hidden-biases-in-big-data>.

17 Tucker, E. (2022). Deliberate Disorder: How Policing Algorithms Make Thinking About Policing Harder. *NYU Review of Law and Social Change*. Vol. 46(1), 86–108. <https://socialchangenyu.com/review/deliberate-disorder-how-policing-algorithms-make-thinking-about-policing-harder>.

18 For more on risk assessment tools, see Appendix: Risk assessment tools (RATs).

19 “These are matters of values and law, and ultimately, the political process. They are not matters of science.” See Berk, R., Heidari, H., Jabbari, S., Kearns, M., Roth, A. (2018). Fairness in Criminal Justice Risk Assessments: The State of the Art. *Sociological Methods & Research*, <https://doi.org/10.1177/0093854818811379>; see also Green, B. (2018). “Fair” Risk Assessments: A Precarious Approach for Criminal Justice Reform. *5th Workshop on Fairness, Accountability, and Transparency in Machine Learning (FAT/ML 2018)*. <https://scholar.harvard.edu/files/bgreen/files/18-fatml.pdf>.

20 Alexander, M. (2012). *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*. New York, NY: The New Press.

reinforcing these patterns further harms people who are marginalized by the status quo.<sup>21</sup> The adage “what gets measured gets managed” is true for algorithms: They are built with, and reflect, only what can be quantified and measured. For example, when a judge uses a risk assessment tool to sentence defendants, the algorithm’s recommendation is based on a defendant’s supposed risk of being “dangerous” — as measured by their supposed likelihood of being rearrested based on their prior criminal history. But “risk” is traditionally just one factor that goes into sentencing decisions and one that disadvantages more heavily policed communities.<sup>22</sup> Sentencing decisions are typically also based on other considerations: deterring others from committing future crimes, rehabilitating the offender or punishing the offender, for instance.<sup>23</sup> But risk assessment algorithms can only input factors that can be, and are, measured. Recidivism is only one such factor. So individual “risk,” as measured by recidivism, becomes the default on which sentencing decisions are made.<sup>24</sup> And as police rely more on predictive and data-driven policing, the concept of “suspicion” becomes less clear; must suspicion be based on actual, observable behavior? Or does a person’s identification as “at risk” by an algorithm constitute the basis for suspicion?<sup>25</sup> If so, it’s harder to challenge the decision, because its reasoning is hidden behind an opaque algorithm.<sup>26</sup>

Parks’ two nonviolent drug-related offenses from 10 years prior — plus some unknown factors — were enough for a risk assessment algorithm to consider him a danger to public safety, after which a judge denied him bail.<sup>27</sup> But what is the criteria for being judged dangerous, and who made that decision? Despite a dearth of empirical guidance on what makes people “low risk” or “high risk,”<sup>28</sup> developers themselves often create these

---

21 Questions of bias, fairness, and equity are, of course, not unique to algorithms, nor are they novel in the context of the criminal legal system. But, in the words of Jack Balkin, “Instead of focusing on novelty, we should focus on salience. What elements of the social world does a new technology make particularly salient that went relatively unnoticed before? What features of human activity or of the human condition does a technological change foreground, emphasize, or problematize? And what are the consequences for human freedom of making this aspect more important, more pervasive, or more central than it was before?” See Balkin, J.M. (2004). Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society.” *NYU Law Review*, Vol. 79(1), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=470842](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=470842).

22 Relying on “recidivism” as a factor determining risk level has its own issues: Recidivism measures not just who goes on to commit another crime, but who goes on to be arrested, meaning communities that are more commonly and strictly policed will be over-represented. See Harcourt, B.E. (2010). Risk as a Proxy for Race. *University of Chicago Public Law & Legal Theory, Working Paper No. 323*. [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1265&context=public\\_law\\_and\\_legal\\_theory](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1265&context=public_law_and_legal_theory). It also ignores the impact that incarceration has on future recidivism. See Dobbie, W., Goldin, J., & Yang, C.S. (2018). The Effects of Pretrial Detention on Conviction, Future Crime, and Employment: Evidence from Randomly Assigned Judges. *The American Economic Review*, Vol. 108(2), 201–240. <https://doi.org/10.1257/aer.20161503>.

23 The American Law Institute. (1962). Model Penal Code § 1.02(2). <https://www.legal-tools.org/doc/08d77d/pdf>.

24 Green, B. (2018). “Fair” Risk Assessments: A Precarious Approach for Criminal Justice Reform. *5th Workshop on Fairness, Accountability, and Transparency in Machine Learning (FAT/ML 2018)*. <https://scholar.harvard.edu/files/bggreen/files/18-fatml.pdf>. See also Hart, Jr., H.M. (1958). *The Aims of the Criminal Law. Law and Contemporary Problems*, Vol. 23, 401–441. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2758&context=lcp>:

“A penal code that reflected only a single basic principle would be a very bad one. Social purposes can never be single or simple, or held unqualifiedly to the exclusion of all other social purposes; and an effort to make them so can result only in the sacrifice of other values which also are important.”

25 Ferguson, A.G. (2015). Big Data and Predictive Reasonable Suspicion. *University of Pennsylvania Law Review*, Vol. 163(2), 327–410. <https://dx.doi.org/10.2139/ssrn.2394683>. See also Joh, E.E. (2017). The Undue Influence of Surveillance Companies on Policing. *New York University Law Review Online*, Vol. 92, 19–47. <http://dx.doi.org/10.2139/ssrn.2924620>.

26 In *Wisconsin v. Loomis*, a criminal defendant challenged a judge’s use of the COMPAS risk assessment algorithm for sentencing on due process grounds, because the algorithm included gender as a factor. The Wisconsin Supreme Court allowed the judge’s use of COMPAS, finding gender to be a valuable and allowable factor to consider because the judge also considered factors beyond the COMPAS risk score. The court also ruled that developers are protected by trade secrets and do not have to provide data to defendants, judges, or researchers about how their algorithms work for the purpose of vetting for accuracy and bias. In most cases, only developers know specifically how their algorithms work and how they reach certain conclusions. See Eckhouse, L., Lum, K., Conti-Cook, C., & Ciccolini, J. (2018). Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment. *Criminal Justice and Behavior*, Vol. 46(2), 185–209. <https://doi.org/10.1177/0093854818811379>.

27 Hill, K. (2020, December 9). Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match. *The New York Times*. <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

28 “...there is relatively little empirical guidance available on how to determine cutoff points...” See “What Is Risk Assessment?” *Public*

normative distinctions on which judges rely.<sup>29</sup> In calculating a “risk” score, the algorithm also took a number of other considerations for granted. It assumes that prior offenses are a good basis for deciding whether a person poses a public safety risk; that whether a person is considered a public safety risk should play a role in bail determination; and that other factors, such as the impact of incarceration on Parks’ and his family’s well-being, are not relevant to that determination.

Of course, a judge may always choose to overrule the algorithm or consider other factors when making a decision. But to do so requires the judge to recognize the algorithm’s assumptions, which is difficult when the algorithm is hidden, and consider whether those assumptions are appropriate. The more automation introduced into systems of policing and punishment, the fewer opportunities to recognize and reconsider the assumptions that constitute criminal legal institutions.<sup>30</sup> Thus, algorithmic technologies can make it harder for advocates, officials and the public to understand or question critical decision-making processes in the criminal legal system. That is true for individual cases<sup>31</sup> (why was *this* particular decision made *this time*?<sup>32</sup>) as well as for the overall system (why is this the particular method or process used?). And often, defendants and their attorneys aren’t even aware algorithmic technologies were used in the first place.<sup>33</sup>

Algorithmic technologies are also opaque because they’re designed by unaccountable private actors who wield significant power in shaping criminal legal outcomes. Developers, product managers and corporate management<sup>34</sup> make decisions about how the tools are built,<sup>35</sup> including the data on which they’re based and their capabilities.<sup>36</sup>

---

*Safety Risk Assessment Clearinghouse*. <https://bja.ojp.gov/program/psrac/basics/what-is-risk-assessment#dc2bg6>.

29 Some risk assessment algorithms, such as the Public Safety Assessment (PSA) created by Arnold Ventures, are created in consultation with judges and legal system experts. However, the issue remains: The normative distinctions between varying degrees of “dangerous” are not based on an empirical foundation. For more information on PSA, see <https://advancingpretrial.org/psa/factors>.

30 “...AI and algorithms are especially dangerous because they can simultaneously obscure problems and amplify them—all while giving the false impression that these problems do not or could not possibly exist.” See Slaughter, R.K. (2019). Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission. *Yale Law School Information Society Project Digital Future Whitepaper and Yale Journal of Law and Technology Special Publication*. [https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms\\_and\\_economic\\_justice\\_master\\_final.pdf](https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf).

31 Hildebrandt, M. (2017). Law As Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics. *University of Toronto Law Journal*, Vol. 68(1), 12–35. <https://doi.org/10.3138/utlj.2017-0044>.

32 Waldman, A.E. (2019). Power, Process, and Automated Decision-Making. *Fordham Law Review*, Vol. 88(2). <https://ir.lawnet.fordham.edu/flr/vol88/iss2/9>.

33 The five publicly reported face recognition misidentification cases – Robert Williams, Michael Oliver, Nijeer Parks, Randall Reid, and Alonzo Sawyer – are merely the five the public knows about. There are more cases, but the overall number is currently unknown. See Garvie, C. (2022). *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*. Center on Privacy & Technology. [forensicwithoutscience.org](https://forensicwithoutscience.org).

34 Brayne, S. & Christin, A. (2020). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*, 1–17. <https://doi.org/10.1093/socpro/spaa004>.

35 See Eckhouse, L., Lum, K., Conti-Cook, C., & Ciccolini, J. (2018). Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment. *Criminal Justice and Behavior*, Vol. 46(2), 185–209. <https://doi.org/10.1177/0093854818811379>.

36 Developers also shape what the definition of a “fair” algorithm means in practice. There is no agreement on exactly what a “fair” algorithm is, and varying definitions are mutually exclusive. See Verma, S. & Rubin, J. (2018). Fairness Definition Explained. *ACM/IEEE International Workshop on Software Fairness*. <https://doi.org/10.1145/3194770.3194776>. See also Friedler, S.A., Scheidegger, C., & Venkatasubramanian, S. (2016). On the (im)possibility of fairness. *ArXiv*. <https://arxiv.org/abs/1609.07236>.

Most famously, a ProPublica investigation revealed a conflict over the definition of “fair” in Northpointe’s COMPAS risk assessment algorithm. See Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine Bias. *ProPublica*. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. See also Corbett-Davis, S., Pierson, E., Feller, A., & Goel, S. (2016, October 17). A computer program used for bail and sentencing decisions was labeled biased against Blacks. It’s actually not that clear. *The Washington Post*. <https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas>. See also Kleinberg, J., Mullainathan, S., Raghavan, M. (2017). Inherent Trade-Offs in the Fair Determination of Risk Scores. *8th Innovations in Theoretical Computer Science Conference (ICTS 2017)*, No. 43, 1–23.

Sometimes even those developers don't know how the formulas work, such as in the case of "black box" algorithms.<sup>37</sup> In that way, a small, private group of people, whose primary responsibility is to maximize profit, has a significant impact on the criminal legal system: in essence, "acting like political entities but with none of the checks and balances," in the words of Ruha Benjamin.<sup>38</sup> Typically, they're shielded from outside inspection and accountability by intellectual property protections that prevent third parties from auditing or inspecting their data or models.<sup>39</sup> Palantir<sup>40</sup> and ShotSpotter,<sup>41</sup> two of the most influential crime forecasting developers, do not reveal how their algorithms are built. Yet, those tools shape how criminal legal actors do their jobs, often in the absence of policies or legal protections for the public.<sup>42</sup>

Algorithmic technologies have proliferated partly due to the increasing production and collection of personal data, which has created a paradigm of "big data surveillance" in both the public and commercial spheres.<sup>43</sup> As a result, law enforcement's surveillance capabilities have both intensified and grown in scope, with two complementary effects. First, more non-law enforcement data ends up in law enforcement databases; and second, law enforcement data increasingly ends up in other non-law enforcement domains.<sup>44</sup> Inclusion in a law enforcement database was historically premised on having contact with law enforcement officials; for instance, if you were arrested, your mugshot photo, fingerprints and other basic details would be recorded by and available to police. The threshold is now much lower; increasingly, people without any police contact are ending up in law enforcement databases.<sup>45</sup> Not only are police surveillance databases wider, collecting information from more people, but they are also deeper, incorporating more types of personal data. Police departments also seek out new sources of external data to integrate into databases, whether that is data collected by other departments or purchased from private entities.

Because there are far fewer constraints on how police can obtain and use private data, often they will purchase it from third parties instead of acquiring it through the warrant process.<sup>46</sup>

---

37 Pasquale, F. (2016). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

38 "Consider that machine-learning systems, in particular, allow officials to outsource decisions that are (or should be) the purview of democratic oversight. Even when public agencies are employing such systems, private companies are the ones developing them, thereby acting like political entities but with none of the checks and balances. They are, in the words of one observer, 'governing without a mandate,' which means that people whose lives are being shaped in ever more consequential ways by automated decisions have very little say in how they are governed." See Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity Press.

39 Joh, E.E. (2017). The Undue Influence of Surveillance Companies on Policing. *New York University Law Review Online*, Vol. 92, 19-47. <http://dx.doi.org/10.2139/ssrn.2924620>.

40 Palantir provides customized software to organizations like law enforcement agencies to analyze vast amounts of disparate data. That includes predictive policing. See Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford, UK: Oxford University Press.

41 ShotSpotter, which entered the market as a gunshot detection tool, considers itself a "precision policing platform" that uses data to "more rapidly and precisely deploy resources to respond to crime, as well as proactively prevent it." That includes "patrol management," which provides a directed patrolling function that acts essentially as predictive policing. See ShotSpotter. <https://www.shotspotter.com>.

42 Joh, E.E. (2017). The Undue Influence of Surveillance Companies on Policing. *New York University Law Review Online*, Vol. 92, 19-47. <http://dx.doi.org/10.2139/ssrn.2924620>.

43 See Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, Vol. 82(5), 977-1008. <https://journals.sagepub.com/doi/pdf/10.1177/0003122417725865>. See also Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, Vol. 19(7). <https://firstmonday.org/article/view/4901/4097>. See also Zuboff, S. (2019). *Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

44 Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, Vol. 82(5), 977-1008. <https://journals.sagepub.com/doi/pdf/10.1177/0003122417725865>.

45 Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, Vol. 82(5), 977-1008. <https://journals.sagepub.com/doi/pdf/10.1177/0003122417725865>.

46 Shenkman, C., Franklin, S.B., Nojeim, G., and Thakur, D. (2021). *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*. Center for Democracy & Technology.



At the same time, data concerning an individual's interaction with the criminal legal system “follows” them into other life domains. Incarceration has historically been accompanied by a stigma that carries over and affects postrelease life opportunities, but in the digital age, the availability of personal data may extend the stigma even further.<sup>47</sup> This “scarlet letter” of collateral legal consequences can impact an individual's employment, housing, public benefits eligibility, voting rights, immigration rights, access to education grants and private and federal loans, and parental rights.<sup>48</sup> Even if you have not been incarcerated or had any contact with the criminal legal system, the search algorithm environment can treat you as if you have, particularly if you are Black. In a landmark study, Latanya Sweeney found that ads by Google AdSense were more likely to suggest that individuals with Black-coded names had been arrested compared to individuals with white-coded names.<sup>49</sup> Search engines reflect and reinforce racist attitudes in other ways as well.

As Safiya Noble documents in “Algorithms of Oppression,” the top results of search engines like Google are influenced by advertising money. Because of bad actors willing to promote hateful content, searches for “black girls” often turn up pornographic images, while searching “jew” can lead to anti-Semitic websites.<sup>50</sup>

That is particularly troubling at a moment when society is once again reckoning with racial inequities in the criminal legal system. With fundamental questions about justice being contested, there is a risk that algorithmic technologies will be invoked as a panacea for the problems in law enforcement. Tech companies, law enforcement, academics and policy analysts have advocated for risk assessments to reduce mass incarceration, face recognition to curb prejudiced police officers, and crime forecasting to rein in racially biased over-policing.<sup>51</sup>

But algorithms will not solve the deep problems in law enforcement; if anything, they could reinforce or aggravate them.<sup>52</sup> For example, research suggests the use of risk assessment scoring may actually lead to worse outcomes for Black defendants. One study found that judges in Kentucky, when making bail decisions, were more likely to set *harsher* conditions for Black defendants than the risk score recommended, as compared to similarly situated white defendants.<sup>53</sup>

In another study, participants using risk assessment tools rated Black defendants as higher risk than did evaluators who were not given a risk assessment score.<sup>54</sup> Another study demonstrated that the presence of a

---

47 Luca, D.L. (2018). The Digital Scarlet Letter: The Effect of Online Criminal Records on Crime. <http://dx.doi.org/10.2139/ssrn.1939589>.

48 Ajunwa, I. (2015). The Modern Day Scarlet Letter. *Fordham Law Review*, Vol. 83(6), 2999–3026. <https://core.ac.uk/download/pdf/144230406.pdf>. See also The Sentencing Project. *Collateral Consequences*. <https://www.sentencingproject.org/issues/collateral-consequences>.

49 Sweeney, L. (2013). Discrimination in Online Ad Delivery: Google Ads, Black Names and White Names, Racial Discrimination, and Click Advertising. *Association for Computing Machinery Queue*, Vol. 11(3), 10–29. <https://dl.acm.org/doi/10.1145/2460276.2460278>.

50 Noble, S. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York, NY: NYU Press.

51 Miller, A. P. (2019, November 21). *Want Less-Biased Decisions? Use Algorithms*. Harvard Business Review. <https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms>. See also Mullainathan, S. (2019, December 6). Biased Algorithms Are Easier to Fix Than Biased People. *The New York Times*. <https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html>. See also Siegel, E. (2018, February 19). *How to Fight Bias with Predictive Policing*. Scientific American. <https://blogs.scientificamerican.com/voices/how-to-fight-bias-with-predictive-policing>.

52 Moy, L. (2021). A Taxonomy of Police Technology's Racial Inequity Problems. *University of Illinois Law Review*, Vol. 139. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3340898](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3340898).

53 Albright, A. (2019). If You Give a Judge a Risk Score: Evidence from Kentucky Bail Decisions. *Multidisciplinary Program in Inequality & Social Policy at Harvard University*. [https://thelittledataset.com/about\\_files/albright\\_judge\\_score.pdf](https://thelittledataset.com/about_files/albright_judge_score.pdf). See also Cowgill, B. (2018). The Impact of Algorithms on Judicial Discretion: Evidence from Regression Discontinuities. *Working paper*. <http://www.columbia.edu/~bc2656/papers/RecidAlgo.pdf>.

54 Green, B. & Chen, Y. (2019). Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments. *ACM Conference on Fairness, Accountability, and Transparency (FAT\* '19)*. <https://doi.org/10.1145/3287560.3287563>.

face recognition recommendation, even when it incorrectly identifies two faces as the same person, strongly influences people to accept the machine's recommendation.<sup>55</sup> And when criminal legal officials make biased or suboptimal decisions on an algorithm's recommendation, they can shift the burden of responsibility for harmful outcomes from themselves onto the technology.<sup>56</sup>

To be clear, bias is not the only issue with algorithmic technologies. Nor is bias merely a technical problem; as Julia Powles and Helen Nissenbaum point out, bias "is a social problem, and seeking to solve it within the logic of automation is always going to be inadequate."<sup>57</sup>

What algorithmic technologies do is take complex social issues like crime and bias and reduce them to individual decisions, ignoring their underlying sources. Crime is viewed as individual behavior to be anticipated and managed, without addressing the systemic issues that fuel it.<sup>58</sup> Bias among law enforcement is viewed as the delinquent views and actions of a few bad apples without considering institutional discrimination.<sup>59</sup> In all cases, the underlying conditions that drive crime, inequity and discrimination are not addressed. In a fight to transform the criminal legal system, algorithmic criminal legal technologies can reinforce the status quo under the guise of reform.<sup>60</sup>

"Predictive" technologies largely tell us what we already know: that certain people and neighborhoods disproportionately experience social ills and crime connected to poverty, inequality,<sup>61</sup> and a cyclic carceral environment.<sup>62</sup> Law enforcement then uses this information to surveil and punish.<sup>63</sup> This makes it more difficult to disrupt crime and incarceration cycles, particularly as it does not address the effect the criminal legal system itself has on perpetuating crime.<sup>64</sup>

---

55 Howard, J.H., Rabbitt, L.R., & Sirotin, Y.B. (2020). Human-Algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision-Making. *PLoS ONE*, Vol. 15(8). <https://doi.org/10.1371/journal.pone.0237855>.

56 This makes the process of making decisions with potentially harmful outcomes more palatable, because the algorithm lends credence to the decision in the official's mind. It also incentivizes the official to act in accordance with the algorithm's recommendation, because deviation from it shifts the burden of responsibility from the algorithm back to the official. See <https://link.springer.com/content/pdf/10.1007/s11077-020-09414-y.pdf>.

57 Powles, J. & Nissenbaum, H. (2018, December 7). The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. *OneZero*. <https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>.

58 Bunge, M. (2006). A Systemic Perspective on Crime. *The Explanation of Crime: Context, Mechanisms and Development*, 8-30. <https://www.cambridge.org/core/books/explanation-of-crime/systemic-perspective-on-crime/CF34BD07EF5DFAD945B81451DA6B218A>.

59 Green, B. (2020). The False Promise of Risk Assessments: Epistemic Reform and the Limits of Fairness. *ACM Conference on Fairness, Accountability, and Transparency (FAT\* '20)*. <https://scholar.harvard.edu/files/bggreen/files/20-fat-risk.pdf>.

60 Moy, L. (2021). A Taxonomy of Police Technology's Racial Inequity Problems. *University of Illinois Law Review*, Vol. 139. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3340898](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3340898).

61 Higher rates of property crime are driven by poverty levels and police activity, while violent crime is driven by inequality. See Kelly, M. (2000). Inequality and Crime. *Review of Economics and Statistics*, Vol. 82(4), 530-539. <https://doi.org/10.1162/003465300559028>.

62 Roodman, D. (2017). The impacts of incarceration on crime. Open Philanthropy Project. [http://www.antonioacasella.eu/nume/Roodman\\_sept2017.pdf](http://www.antonioacasella.eu/nume/Roodman_sept2017.pdf).

63 The use of risk assessment tools, and the discourse around their use, focuses on their "predictive" function while ignoring their potential "diagnostic" function. Some, however, have advocated for the use of these tools for diagnostic purposes to better understand the underlying societal and institutional drivers of crime and to evaluate the effectiveness of various interventions. See Barabas, C., Dinakar, K., Ito, J., Virza, M., & Zittrain, J. (2018). Interventions Over Predictions: Reframing the Ethical Debate for Actuarial Risk Assessment. *ACM Conference on Fairness, Accountability, and Transparency (FAT\* '18)*. <https://arxiv.org/pdf/1712.08238.pdf>.

64 Barabas, C., Dinakar, K., Ito, J., Virza, M., & Zittrain, J. (2018). Interventions Over Predictions: Reframing the Ethical Debate for Actuarial Risk Assessment. *ACM Conference on Fairness, Accountability, and Transparency (FAT\* '18)*. <https://arxiv.org/pdf/1712.08238.pdf>.

At a time when communities most impacted by the inequities in systems of policing and punishment are demanding a reconsideration of those systems, algorithmic technologies reinforce the status quo. These tools give private, profit-driven actors significant influence over critical justice-related processes and outcomes. To many, they appear neutral but are actually based on historical data and perpetuate discrimination and inequities in law enforcement. If we want to build a more equitable justice system, it is imperative to be able to better understand, and challenge, how criminal legal officials make decisions. Algorithmic technologies do the opposite.



