SURVEILLANCE TOOLS:[1]

Biometric tools:[2]

Biometric tools are those tools which use biometric information to identify an individual. They are used pre-arrest, during pre-trial investigation, and during post-release surveillance.

Facial Recognition:[3]

Facial recognition systems use algorithms to pick out distinctive features of someone's face, such as distance between eyes or shape of chin, convert them into a mathematical representation, and then compare them to faces collected in the database.[4] Some systems positively ID an unknown person, while others are designed to calculate a probability score and rank potential matches in order of likelihood of correct identification. Facial recognition technology can be used for "one to one" matching (verification) or "one to many" matching (identification). The federal government has various facial recognition systems, including the most relevant for law enforcement - FBI's Next Generation Identification database - which contains over 30 million records of facial recognition, iris recognition, palm prints and fingerprints.[5] Authorized federal, state and local law enforcement agencies are allowed access to this database with little oversight[6], cross-referencing social media, traffic cameras, closed circuit television ("CCTV"), or other forms of video or photographic surveillance.[7,8]

Iris Recognition:

Iris recognition works very much like facial recognition. When law enforcement scans someone's iris into a given database, the scan collects information on 240 specific features of the person's iris.[9] That data can then be compared to existing iris information stored in that database and others for either verification or identification.[10] Databases of iris information are ever-

---

[1] Other surveillance technologies include, but are not limited to: Gunshot analysis (e.g. Shotspotter), Bodycams, CCTV, Drones, IMSI capturers (e.g. Stingray), Malware, GPS tracking ("slap and track"), and physical phone break-in technologies (e.g. Cellebrite). Additionally, DNA technology, another form of biometric tech, faces many similar challenges as other databases and surveillance technology, and, additionally, its reliability is of growing concern as the technology to analyze it continuously develops. *See generally* Matt Shaer, *The Problems with DNA Evidence and Testing*, THE ATLANTIC, June 2016, https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.

[2] *See generally Street Level Surveillance*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/street-level-surveillance (last visited Feb. 4, 2020).

[3] *Face Recognition*, ELECTRONIC FRONTIERS FOUNDATION, https://www.eff.org/pages/face-recognition (last visited Feb 4., 2020).

[4] Common vendors include: MorphoTrust, 3M, Cognitec, DataWorks Plus, Dynamic Imaging Systems, FaceFirst, and NEC Global.

[5] *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Feb. 4, 2020).

[6] *See, e.g.*, Claire Garvey et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, THE GEORGETOWN LAW & PRIVACY CENTER (Oct. 16, 2016), https://www.perpetuallineup.org/.

[7] *Id*. *See also*, Electronic Privacy Information Center, Testimony to U.S. House Committee on Oversight and Government Reform at 2 (May 21, 2019), https://epic.org/testimony/congress/EPIC-HCOGR-FacialRecognition-May2019.pdf; *supra* note 6.

[8] The FBI has an entire team dedicated to facial recognition called Facial Analysis, Comparison, and Evaluation ("FACE").

[9] *Iris Recognition*, ELECTRONIC FRONTIERS FOUNDATION, https://www.eff.org/pages/iris-recognition (last visited Feb. 4, 2020).

[10] *Id.*

growing, with police departments and other law enforcement agencies, prisons, and the US military continuing to collect and use iris information.[11]

Tattoo Recognition:

Tattoo recognition also works very similarly to facial recognition. Tattoo recognition software uses an algorithm to either identify people based on their tattoos by comparing photographs of their tattoos to a database, or to interpret the meaning of the tattoos themselves. In 2016, an Electronic Frontier Foundation lawsuit revealed that the FBI and the National Institute for Science & Technology partnered to improve tattoo recognition technology.[12]

Concerns about Biometric Tools: The use of biometric tools and databases amplify the effects of racist policing practices. Because policing practices in the US disproportionately surveil and target people of color and immigrants,[13] a disproportionate number of Black people and non-Black people of color and immigrants are in these databases, which in turn means the technology is disproportionately used on Black and brown people.[14]

Biometric tools also raise civil liberties and privacy concerns, allowing law enforcement and anyone else who can access the databases to surveil and track people without their consent.[15] In 2016, over 117 million adults in the US were impacted by facial recognition surveillance at the local, state or federal level, representing almost half of all adults in the US.[16]

Biometric tools also raise First Amendment concerns, as the tools can be used to target dissenters and political activists, chill speech and association, and in the case of tattoos, gather additional information about people's beliefs, religion, or their family, friends, or other people to whom they're connected.[17] For example, during the Baltimore uprising after Freddie Gray's murder, the Baltimore Police Department ran social media photos of protests through facial

---

[11] *Id.*

[12] Dave Maass, *Documents Bare How Federal Researchers Went to Absurd Lengths to Undo Problematic Tattoo Recognition Research*, ELECTRONIC FRONTIERS FOUNDATION (Aug. 21, 2018), https://www.eff.org/deeplinks/2018/08/eff-bares-how-federal-researchers-went-absurd-lengths-undo-problematic-tattoo; Harper Neidig, *Group Sues Agencies for Info on Tattoo Recognition Technology*, THE HILL(Nov. 30, 2017), https://thehill.com/policy/technology/362636-group-sues-agencies-for-info-on-tattoo-recognition-technology.

[13] See, e.g., *supra* note 6; Alexi Jones, *Police Stops Are Still Married by Racial Discrimination, New Data Shows*, PRISON POLICY INITIATIVE, October 12, 2018, https://www.prisonpolicy.org/blog/2018/10/12/policing/; Malkia Amala Cyril, *Black America's State of Surveillence*, THE PROGRESSIVE, March 30, 2015, https://progressive.org/magazine/black-america-s-state-surveillance-cyril/.

[14] In addition, studies have shown that facial recognition software is particularly bad at distinguishing Black people's faces from each other, non-Black people of color's faces from each other, and "female" faces from each other. See, e.g., Claire Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY (May 16, 2019), https://www.flawedfacedata.com/.

[15] As the ACLU has explained, "these technologies have the potential to enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale," the attorneys wrote. "Such surveillance would permit the government to pervasively track people's movements and associations in ways that threaten core constitutional values." Drew Harwell, *ACLU Sues FBI, DOJ Over Facial-Recognition Technology, Criticizing 'Unprecedented' Surveillance and Secrecy*, WASHINGTON POST, Oct. 31, 2019, https://www.washingtonpost.com/technology/2019/10/31/aclu-sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/.

[16] Garvie, *The Perpetual Line-Up*, *supra* note 6.

[17] *Supra* note 12.

recognition software to identify and arrest protesters.[18] According to Georgetown Center on Privacy and Tech, only one agency out of 52 analyzed had a policy explicitly prohibiting use of this technology to track individuals engaged in protected speech.[19] In addition, Biometric tools can be used by federal agencies to effectively override state and local policies created to protect immigrant communities, such as when Immigration and Customs Enforcement ("ICE") uses facial recognition databases to match photographs of immigrants to state drivers' license databases in states that allow undocumented people to obtain licenses.[20]

Finally, biometric tools are prone to error, as evidenced by the difficulty the technology has in distinguishing people from each other.[21] Thus, as the reach of the tools is expanded to a wider range of databases and individuals, the potential for errors will be compounded.[22]

Gang Databases:

Law enforcement agencies use gang databases to collect surveillance information on people whom that law enforcement agency decides to label as a "suspected gang member" or "gang member." Law enforcement use gang databases to collect information on alleged "gang members," including information on their "associates."[23] Many major US cities, including New York,[24] Chicago,[25] and Boston,[26] among many others, and in addition to various states[27] and the federal government,[28] use a type of gang database as a surveillance and predictive tool. The NYPD has over 18,000 people in its gang database, including children as young as 13 years old.[29]

Concerns about gang databases: Gang database criteria are vague and there is little oversight, which means these databases amplify the racism already baked into the legal system. As the Brennan Center for Justice notes, "[t]he vague and broad criteria for in-clusion, open the door to racial bias. NYPD officials have acknowledged that as many as 95 percent of the people

---

[18] Kevin Rector and Alison Knezivich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALTIMORE SUN, Oct. 17, 2016, https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html

[19] *Supra* note 3.

[20] *See, e.g.*, Bill Chappel, *ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say*, NPR, Jul. 8, 2019, https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa

[21] Iris recognition is prone to error between 1-10% of the time. It is also possible to manipulate iris recognition databases by using data to create a false match. *Supra* note 9.

[22] *Supra* note 3.

[23] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT FOR THE ICEGANGS DATABASE 2 (Jan. 15, 2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icegangs.pdf.

[24] *See, e.g.*, Yasmeen Khan, *Damning Report on NYPD Gang Database Increases Calls to End "a Tool of Mass Criminalization,"* GOTHAMIST, Dec. 13, 2019, https://gothamist.com/news/damning-report-nypd-gang-database-increases-calls-end-tool-mass-criminalization.

[25] *See, e.g.*, Mick Dumke, *Chicago's Inspector General Finds the City's Gang Database Is Riddled with Errors*, PROPUBLICA ILLINOIS, April 11, 2019, https://www.propublica.org/article/chicago-police-department-gang-database-inspector-general-report.

[26] *See, e.g.*, Shannon Dooling, *Here's What We Know About Boston's Police Gang Database*, WBUR NEWS, July 26, 2019, https://www.wbur.org/news/2019/07/26/boston-police-gang-database-immigration.

[27] *See, e.g.*, Zak Cheney-Rice, *LAPD Officers Are Falsely Labeling People as Gang Members. It's Part of a Bigger Crisis,* NEW YORK MAGAZINE, Jan. 7, 2020, https://nymag.com/intelligencer/2020/01/lapd-falsely-labeling-gang-members.html.

[28] *See* FBI NATIONAL GANG INTELLIGENCE CENTER, https://www.fbi.gov/investigate/violent-crime/gangs/ngic (last visited Feb. 4, 2020).

[29] Nick Pinto, *NYPD Added Nearly 2,500 New People to Its Gang Database in the Last Year*, THE INTERCEPT, June 28, 2019, https://theintercept.com/2019/06/28/nypd-gang-database-additions/.

in its gang database are Black or Latinx."[30] People who are included on gang databases are then disproportionately surveilled and targeted by the police, who use the database designation as a gang member to justify this heightened targeting, creating a cycle.[31]

In addition to increased surveillance and targeting from the police, non-citizens face detrimental effects to their safety and security stemming from increased targeting by ICE, denials of discretionary relief,[32] denial of bond,[33] and it can even lead to deportation.[34] In New York City and many other cities, people have no legal right to know if they are on a gang database, and no way to find out or challenge their own inclusion in the database.[35] Recently, Providence, Rhode Island passed one of the most comprehensive police accountability ordinances, which requires, among other things, that the Police Department allow people to find out if they are on the database, and to challenge their inclusion. It also requires the Police Department notify parents or guardians of any minors who are added to the database.[36] In practice, however, the Providence Police Department has not followed this ordinance, and Providence residents have had to sue the Providence Police Department in federal court in the hopes that will compel the Department to enforce the ordinance.[37]

Law enforcement agencies use gang databases to collect information about first amendment-protected activities, such as speech and association. One such example, in Providence, the movement to challenge the Police Department's gang database uncovered that the gang database was using a "point system" to determine whether to designate someone as a gang member, the criteria for which included association with known gang members and "publication in a gang database."[38]

Stages used: Gang databases are used at pre-arrest, bail application, trial, and surveillance post-release.

Data-Sharing Programs Between Law Enforcement Agencies:

Law enforcement agencies, between jurisdictions and within agencies, take part in data-sharing programs that facilitate their sharing and coordination.[39] These programs allow agencies

---

[30] Angel Diaz, BRENNAN CENTER FOR JUSTICE, NEW YORK CITY POLICE DEPARTMENT SURVEILLANCE TECHNOLOGY (Oct. 7, 2019), https://www.brennancenter.org/sites/default/files/2019-10/2019_NewYorkPolicyTechnology.pdf

[31] *See* Alice Speri, *NYPD Gang Database Can Turn Unsuspecting New Yorkers into Instant Felons*, THE INTERCEPT, Dec. 5, 2018, https://theintercept.com/2018/12/05/nypd-gang-database/.

[32] *See, e.g.*, IMMIGRANT LEGAL RESOURCE CENTER, PRACTICE ADVISORY: UNDERSTANDING ALLEGATIONS OF GANG MEMBERSHIP/AFFILIATION IN IMMIGRATION CASES (April 2017), https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170509.pdf

[33] *See, e.g.*, NEW YORK CIVIL LIBERTIES UNION, STUCK WITH SUSPICION (2019), https://www.nyclu.org/sites/default/files/field_documents/020819-nyclu-nyic-report_0.pdf

[34] *See* Kade Crockford, *From Gang Allegations to Deportation: How Boston Is Putting Its Immigrant Youth in Harm's Way,* THE APPEAL, Jan. 18, 2018, https://theappeal.org/from-gang-allegations-to-deportation-how-boston-is-putting-its-immigrant-youth-in-harms-way-de3b0edc9327/

[35] *Supra* note 29.

[36] Julia Rock and Lucas Smolcic Larson, *Providence Police Gang Database Policy "Tramples Fundamental Constitutional Rights," Lawsuit Says*, THE APPEAL, Jan. 10, 2020, https://theappeal.org/rhode-island-police-gang-database/.

[37] *Id.*

[38] *Id.*

[39] Examples of the federally run data-sharing programs include: The National Information Exchange Model (NIEM), Global Justice XML, the FBI's Criminal Justice Information Services (CJIS), the Department of Justice-sponsored

to share information on individuals gathered through other tools, like facial recognition technology and gang databases.

Concerns about data-sharing programs: A major concern of these programs is the privacy protections and safety considerations applied to the information that is shared. By facilitating sharing data, problems with how this data is gathered are amplified, since they will be more widely available. Additionally, there are safety and privacy concerns with whom this information is shared with, including when information is shared with ICE, even when sanctuary state or city policies are in place[40]

Stages used: Data-sharing programs are ubiquitous, and are used at all stages of the criminal punishment system.

Intelligence-Driven Prosecution:[41]

Predictive prosecution combines the use of multiple surveillance and prediction technologies - including databases, social network analysis, facial recognition, license plate scanners, cell phone tracing, CCTV, and digital tracking - to flag people law enforcement believes to be responsible for violent crime, and to share that information across agencies. These technologies include data-sharing programs between law enforcement agencies. One example of this technology is the Manhattan District Attorney's Offices' Arrest Alert System, which alerts the District Attorney's office when a person of interest has contact with any law enforcement agency participating in the system.

Concerns with Intelligence-Driven Prosecution: There are a number of concerns raised by intelligence-driven prosecution models including privacy concerns, the possibility for abuse and error, and issues related to the evidence the prosecution is required to disclose to the defense pursuant to obligations imposed by the U.S. Constitution and *Brady v. Maryland*.

First, these systems carry with them similar privacy concerns as those related to surveillance tools generally. These systems also leave open the possibility of abuse and error because risk factors are established by those with an interest in prosecuting certain individuals, so objectivity is in question and transparency, similar to gang databases, is lacking.[42] Lastly, there are serious concerns that result from the vast amounts of data, including, inevitably, exculpatory data

---

Regional Information Sharing System (RISS), the FBI National Data Exchange N-DEx, and the Department of Homeland Security's Law Enforcement Information Sharing System (LEISS).

[40] *See* Lily Hay Newman, *Internal Docs Show How ICE Gets Surveillance Help from Local Cops*, WIRED, March 13, 2019, https://www.wired.com/story/ice-license-plate-surveillance-vigilant-solutions/; Felipe De La Hoz, *New York, A Sanctuary State, Provides Criminal Justice Data to ICE*, DOCUMENTED, May 8, 2019, https://documentedny.com/2019/05/08/new-york-a-sanctuary-state-provides-criminal-justice-data-to-ice/.

[41] The Manhattan DA's office under Cyrus Vance in 2010 is widely credited for first developing and implementing intelligence-driven prosecution. *See* Heather McDonald, *Prosecution Gets Smart*, CITY-JOURNAL, Summer 2014, https://www.city-journal.org/html/prosecution-gets-smart-13663.html. Since then, a number of jurisdictions have adopted similar practices, including Albuquerque, Baltimore, Baton Rouge, Boston, The Bronx, Brooklyn, Chicago, Delaware, Jersey City, Philadelphia, Phoenix, Rockford, Seattle, San Francisco, Santa Clara, St. Louis, Staten Island, and Tucson. NEW YORK COUNTY DISTRICT ATTORNEY, OUR WORK: CRIME STRATEGIES, https://www.manhattanda.org/our-work/crime-strategies/ (last accessed Feb. 4, 2020).

[42] Andrew Guthrie Ferguson, *How the Manhattan DA's Use of Big Data Targeting Risks Changing the Rules of Prosecution,* THE APPEAL, Oct. 10, 2017, https://theappeal.org/how-the-manhattan-das-use-of-big-data-targeting-risks-changing-the-rules-of-prosecution/.

on witness credibility and law enforcement biases.[43] The prosecution is constitutionally mandated to disclose exculpatory evidence to the defense. However, since the purpose of these systems is not to identify or separate such data to mee that obligation, there is a risk that evidence is not being provided to defense counsel.

Stages used: Prosecutor's offices use this information to guide decisions on investigation, pursuing charges against people, making bail requests, plea offers, sentencing recommendations.

"PREDICTIVE" TOOLS

Gang databases:

In addition to the ways in which gang databases are used as surveillance tools, they can also be used in conjunction with other software and information-sharing systems to become a predictive technology. For example, the company Palantir creates and sells data-mining software that organizes and arranges information for law enforcement to "visualize" potential or suspected relationships between multiple people and groups, and that law enforcement uses to create lists of people to target.[44] Technologies like this provide yet another layer of opacity on top of law enforcement decision-making, making it that much more difficult to understand, evaluate, and correct biased law enforcement decision-making and practice.

Risk Assessments:

Risk assessment tools are commonly used to make determinations about pretrial release or pretrial detention; remand; sentencing; prison designation; or parole. Risk assessment tools weigh given factors to produce a "risk level" decision or recommendation.[45] They generally do so by "us[ing] data about groups of people, like those who have been arrested or convicted, to assess the probability of future behavior."[46] In the case of a pretrial detention risk assessment, for example, the "risk" calculated might be purported to be the risk of the defendant's failure to appear; in a parole risk assessment, the "risk" calculated might be the risk of rearrest if released. Commonly considered factors in risk assessments include age, drug and alcohol use history, criminal record, zip code, active community, pending charges, employment stability, education level, housing stability, family relationships, community ties.[47]

Concerns about Risk Assessments: Scholars and advocates have warned that risk assessment tools reproduce and amplify the racism and inequality in the criminal punishment, rather than reduce bias as some proponents have argued.[48] Over 100 civil rights organizations in

---

[43] AI NOW, LITIGATING ALGORITHMS 2019 REPORT: NEW CHALLENGES TO GOVERNMENT USE OF ALGORITHMIC DECISION SYSTEMS 15 (Sept. 2019), https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf.

[44] Peter Waldman et al., *Peter Thiel's Data-Mining Company is Using War on Terror Tools to Track American Citizens. The Scary Thing? Palantir is Desperate for New Customers*, BLOOMBERG, Apr. 19, 2019, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

[45] Risk assessments commonly take into account and weigh against each other "risk factors, which are personal characteristic and environmental factors associated by the algorithm with higher "risk," and "protective factors," which are personal characteristic and environmental factors associated by the algorithm with lower "risk."

[46] John Logan Koepke & David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, 93 Wash. L. Rev. 1725, 1752 (2018)

[47] Risk assessments can be strictly algorithmic, or can have built into them the judgement and discretion of a human decision-maker.

[48] *See, e.g.*, Kelly Hannah-Moffat, *The Uncertainties of Risk Assessment: Paritality, Transparency and Just Decisions*, 27 FED SENTENCING REPORTER 244 (Apr. 2015); COMMUNITY JUSTICE EXCHANGE, AN ORGANIZER'S GUIDE TO CONFRONTING PRETRIAL RISK ASSESSMENT TOOLS IN DECARCERATION CAMPAIGNS (Dec. 2019),

the U.S. agree.[49] The premise of risk is inherently racist because, in the context of a legal system that targets Black and brown people and the communities in which they reside, it is a proxy for race.[50] Furthermore, many factors often used in risk assessment algorithms are specific proxies for race, and their use in risk assessments amplifies existing racism in the criminal punishment system. Such factors include prior arrests, prior convictions, parental criminal record, "community disorganization" and zip code.[51] These factors reflect over-policing, the behaviors of law enforcement in Black and brown communities, larger patterns of socio-economic disadvantage resulting from the racial caste system, rather than anything about the behaviors of people who are targeted. In other words, the data is more predictive of racialized disadvantage and police presence in an accused person's community than a person's behavior.

Scholars have highlighted several points at which bias may taint a risk assessment: 1) whether the instrument's algorithm is fair, 2) whether the data used to calculate the score are biased in some fundamental way, and 3) whether there are moral and constitutional issues with using "group" data (such as the zip code someone lives in) to predict behavior and make decisions about an individual person's freedom.[52] Despite proponents' claims, risk assessments do not automatically decrease rates of detention; in fact, a recent survey by the Media Mobilizing Project and Media Justice found that only 17% of the jurisdictions they surveyed saw a reduction in detention when they implemented a risk assessment tool, while the rest saw an increase or no change.[53] Many risk assessment tools are developed by private companies, who have a profit interest in the development and implementation of the tools, and who work together with governmental users to keep the algorithm a black box by claiming it is "proprietary."[54] The lack of transparency,[55] and community input, into these tools makes it effectively impossible for the public to understand, evaluate, and challenge their design and implementation.[56]

HTTP://BIT.LY/PRETRIALRATGUIDE; EPIC.ORG, ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM, https://epic.org/algorithmic-transparency/crim-justice/ (last visited Feb. 4, 2020); Hannah Sassaman, *Pennsylvania's Proposed Risk-Assessment Algorithm Is Racist*, THE PHILADELPHIA ENQUIRER, Sept. 4, 2019, https://www.inquirer.com/opinion/commentary/pennsylvania-sentencing-commission-rat-risk-assessment-20190904.html;

[49] *See* PRETRIAL JUSTICE, THE USE OF PRETRIAL "RISK ASSESSMENT" INSTRUMENTS: A STATEMENT OF CIVIL RIGHTS CONCERNED, http://civilrightsdocs.info/pdf/criminal-justice/Pretrial-Risk-Assessment-Full.pdf.

[50] *See* Bernard E. Harcourt, *Risk As a Proxy for Race*, University of Chicago Public Law & Legal Theory Working Paper No. 323 (2010).

[51] See *Litigating Algorithms*, AI NOW INST. 13 (Sept. 24, 2018), https://ainowinstitute.org/litigatingalgorithms.pdf. *See also*, Ellora Thadaney Israni, *When An Algorithm Helps Send You to Prison*, N.Y. TIMES, Oct. 26, 2017, https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html

[52] Laurel Eckhouse, *Layers of Bias: A Unified Approach for Understanding Problems With Risk Assessment*, CRIMINAL JUSTICE AND BEHAVIOR (2018), https://doi.org/10.1177/0093854818811379

[53] @mediamobilizing, TWITTER (Feb. 4, 2020, 2:30 PM), https://twitter.com/mediamobilizing/status/1224777290262949888/photo/2; *supra* note 49.

[54] *Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools*, ELECTRONIC PRIVACY AND INFORMATION CENTER, https://epic.org/algorithmic-transparency/crim-justice/ (last visited Feb. 4, 2020); Kate Crawford and Jason Schultz, *AI Systems as State Actors*, 119 COLUMBIA L. REV. 1941 (2019).

[55] "While it is difficult to have accountability without transparency, transparency, in and of itself, does not guarantee that actors with power in the system will be held accountable for their actions and decisions. Even with adequate, or even excellent, transparency and access to the courts, violence and injustice within the criminal legal system continues." COMMUNITY JUSTICE EXCH., TRANSPARENCY IS NOT ENOUGH 4, https://www.communityjusticeexchange.org/resources.

[56] *Id.*

In addition, many tools are not designed for use in the specific context in which the courts deploy them.[57] In the pretrial context, for example, risk assessments are relied upon as a measure risk of danger to community safety and intentional flight, despite the fact that they are calibrated to calculate risk of rearrest and non-appearance, an entirely different set of metrics. Furthermore, many tools produce one "risk" score, combining rearrest and non-appearance as "risk," despite the fact that courts are required to make each inquiry separately.[58] Finally, risk assessment tools can drive automation bias, the idea that automated decision-making systems are *more* "neutral" than human decision-makers because they are scientific.[59] This bias carries with it the potential to further entrench the harms caused by faulty predictions produced by the tools, as actors are less likely to question whether those predictions are accurate or based on the unique circumstances and characteristics of the person standing before the court.

Crime Forecasting Technologies:

Proponents of crime forecasting technologies claim that it uses machine-learning algorithmic technologies to identify patterns in data collected from a variety of surveillance technology sources (for example, past arrest statistics, CCTV cameras and drones), in order to predict future crime and drive the allocation of law enforcement resources.[60]

Concerns with Crime Forecasting Technologies: Crime forecasting technologies are essentially risk assessment tools that label certain blocks or neighborhoods as "high risk." And like risk assessments, crime forecasting technologies rely on data points that often correlate with race - such as past police activity, income, arrests, to produce forecasts.[61] As a result, crime forecasting technologies not only reflect the behavior of law enforcement rather than people in the areas predicted to be "high crime," but they also create feedback loops that actually increase racialized targeting within the criminal punishment system.[62] The crime forecasting technologies use data that simply reflect the underlying racism in law enforcement behavior - such as data that shows predominantly Black neighborhoods have higher rates of arrest - in order to then justify additional law enforcement presence in those same neighborhoods, in turn creating *new* data points for that increased law enforcement presence in those same neighborhoods, that is then added to the set to justify ever increasing policing.[63] Finally, and perhaps most importantly, both individual risk assessments and crime forecasting technologies suggest that incarceration is appropriate if the state believes they may be "at risk": at risk of not showing up to court, or of using drugs, or of

---

[57] CENTER ON RACE, INEQUALITY AND THE LAW AND ACLU, WHAT DOES FAIRNESS LOOK LIKE? CONVERSATIONS ON RACE, RISK ASSESSMENT TOOLS, AND PRETRIAL JUSTICE 13 (Oct. 2018), http://www.law.nyu.edu/sites/default/files/Final%20Report--ACLU-NYU%20CRIL%20Convening%20on%20Race%20Risk%20Assessment%20%20Fairness.pdf

[58] Matt Henry, *Risk Assessment: Explained*, THE APPEAL, Mar. 25, 2019, https://theappeal.org/risk-assessment-explained/

[59] PARTNERSHIP ON AI, REPORT ON ALGORITHMIC RISK ASSESSMENT TOOLS IN THE U.S. CRIMINAL JUSTICE SYSTEM 23, https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/

[60] Companies and products include: ShotspotterMissions, PredPol, Crimescan and Palantir.

[61] *supra* note 48.

[62] Andrew Guthrie Ferguson, *The Truth About Predictive Policing and Race*, THE APPEAL, Dec. 7, 2017, https://theappeal.org/the-truth-about-predictive-policing-and-race-b87cf7c070b1/; Matt Stroud, The Minority Report: Chicago's New Police Computer Predicts Crimes, But is it Racist?, THE VERGE, Feb. 19, 2014, https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist

[63] *Id.*

being arrested, or of engaging in any number of criminalized behaviors, or of not paying a fine or fee they can't afford, such as for an electronic monitoring ankle bracelet. In response, broad coalitions of community-based organizations, advocates, bail funds, scholars, and have worked to challenge the narrative of "risk" altogether, putting forward a vision of public safety that focuses on meeting people's needs and resourcing every community.[64]

[64] For example, National Bail Out and Southerners on New Ground, organizers of the national Black-led Black Mama's Bail Out, have developed a sample "needs assessment" to use not to make decisions about anyone's freedom, but to provide supportive resources to people who are being bailed out. *Until Freedom Comes*, NATIONAL BAIL OUT, https://nationalbailout.org/untilfreedomcomes/ (last visited Feb. 5, 2020); NATIONAL BAIL OUT, UNTIL FREEDOM COMES: A COMPREHENSIVE BAIL OUT TOOLKIT 47, https://southernersonnewground.org/wp-content/uploads/2019/07/Until-Freedom-Comes-A-Comprehensive-Bailout-Toolkit.pdf