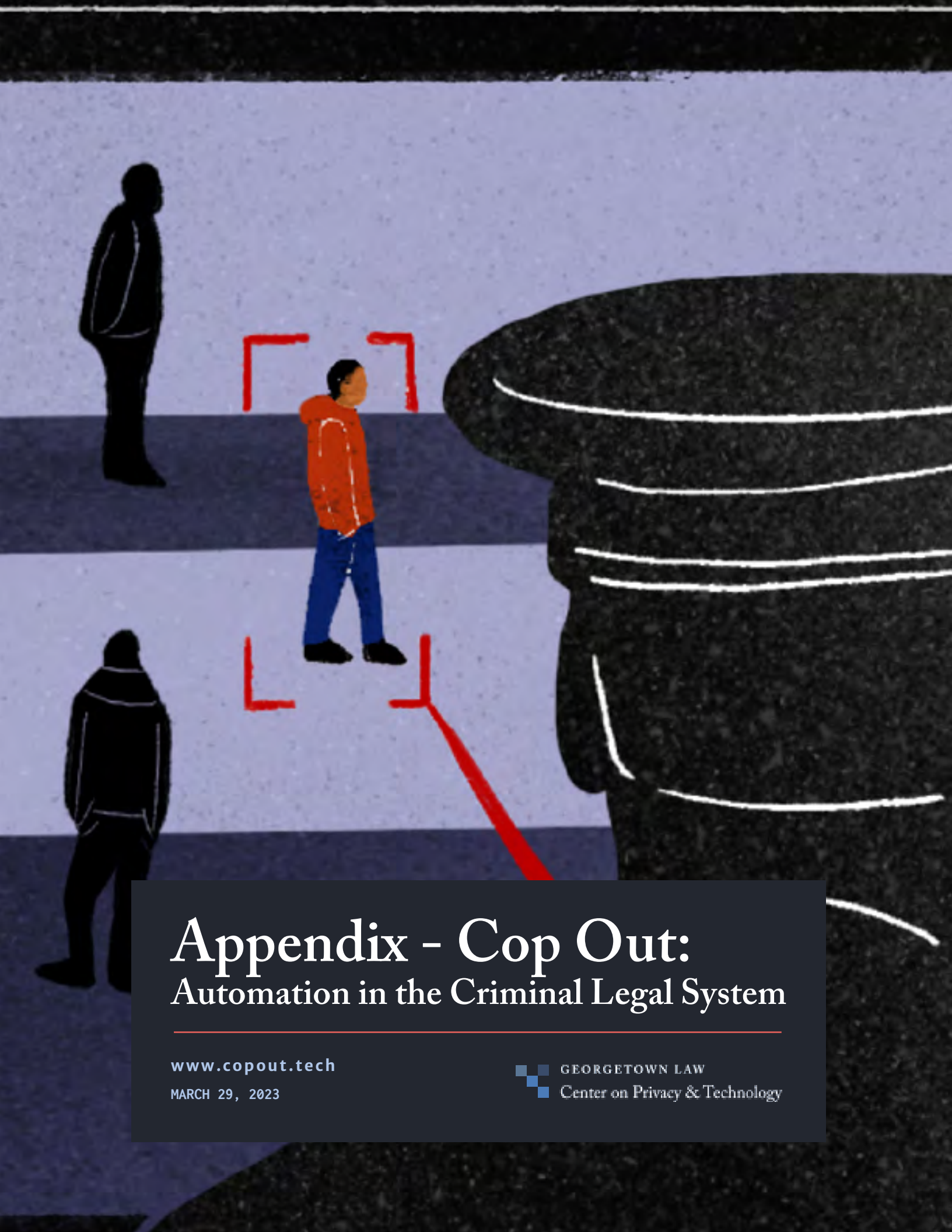

Appendix - Cop Out:
Automation in the Criminal Legal System

www.copout.tech

MARCH 29, 2023

GEORGETOWN LAW
Center on Privacy & Technology

Appendix - Cop Out: Automation in the Criminal Legal System

AUTHOR

Jameson Spivack, *Associate*

CONTACT

privacy@georgetown.edu / 202-662-9779

DESIGN

rootid
Cover Illustration by Lara Zigic, as part of a collaborative process,
larazigic.com

www.copout.tech
www.law.georgetown.edu/privacy-technology-center

March 29, 2023

TABLE OF CONTENTS

Crime forecasting

BASICS

"Crime forecasting" here refers to two separate but related processes: *predictive policing* and *data-driven prosecution.* Both processes involve using historical police data to calculate the probability of future police activity — arrests, reported crimes and other police-civilian interactions — in a given area in the future. Police use the algorithm's calculations as a basis for targeting particular neighborhoods or particular people. Prosecutors use the algorithm's calculation as a basis for charging decisions and sentencing recommendations. In both cases, the algorithm labels certain locations "at-risk" or certain people as "likely" to commit or be the victims of crime.

For more on the basics of crime forecasting, see:

National Institute of Justice Office of Justice Programs, "Predictive Policing," https://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx.

Andrew Ferguson, *Big Data Prosecution and* Brady, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397292.

Andrew J. Ferguson, *Predictive Policing Theory*, The Cambridge Handbook of Policing in the United States (ed. Tamara Rice Lave & Eric J. Miller), Cambridge Univ. Press (2019).

John S. Hollywood, Brian McInnis, Walter L. Perry, Carter C. Price, Susan C. Smith, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, available at https://ebookcentral.proquest.com/lib/georgetown/reader.action?docID=1437438 .

Sarah Brayne, *Big Data Surveillance: The Case of Policing*, https://doi.org/10.1177/0003122417725865.

WHAT CRIME FORECASTING TOOLS ARE BASED ON

There are two types of predictive policing tools: *place-based,* which map so-called "hot spot" areas based on historical police activity, and *person-based,* which use historical police data to generate lists of individuals supposedly at risk of committing or being victims of crime.

Place-based policing algorithms rely on police department data, including 911 calls and community or police reports of suspected crime. They may give weight to data points such as reports of property crime or vandalism, juvenile arrests, the presence of people on parole or probation, and disorderly conduct calls. Some algorithms even give weight in their calculations to things like weather patterns, the presence of liquor stores and population density.

Person-based algorithms rely on data collected about individual histories of interaction with the criminal legal system. Those tools create lists of names and assign accompanying risk scores based on data from arrest records, inclusion in gang databases, parole and probation records, and police reports.

Data-driven prosecution refers to a set of data analysis techniques that prosecutors use when making decisions about what charges to bring, what sentences to ask for and how to dispose of cases. As a process, it is relatively understudied, but in general it describes prosecutorial reliance on data from the criminal legal system, including law enforcement data about active cases, data about the locations of previously reported crimes, lists of individuals whom police have identified as priority offenders, and data about probationers and parolees. More research is necessary to understand what specific algorithmic products prosecutors are using; how they are using them; and what policies, if any, guide or constrain these practices.

For more on which data crime forecasting tools are based on, see:

Elizabeth Joh, *The Undue Influence of Surveillance Companies on Policing,* https://www.nyulawreview.org/online-features/the-undue-influence-of-surveillance-technology-companies-on-policing.

David Robinson and Logan Koepke, Upturn, *Stuck in a Pattern: Early evidence on "predictive policing" and civil rights,* https://www.upturn.org/reports/2016/stuck-in-a-pattern.

Andrew J. Ferguson, *Predictive Policing Theory,* The Cambridge Handbook of Policing in the United States (ed. Tamara Rice Lave & Eric J. Miller), Cambridge Univ. Press (2019).

Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273800.

Andrew Ferguson, *Big Data Prosecution and* Brady, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397292.

RISKS AND BIASES

Developers build crime forecasting algorithms with historical police data, meaning the algorithms' outputs will reflect inequities in the criminal legal system. That includes data from decades of documented policing practices that are biased, corrupt and even unlawful: falsifying crime records, planting evidence, targeting Black and Brown communities, and otherwise manipulating crime data. All of these biased decisions, originally made by humans, become part of the algorithms that corporations and law enforcement agencies claim can "predict" future crime. Police then spend disproportionate amounts of time targeting the same communities and individuals they have targeted in the past, creating a feedback loop.

Historical crime and arrest data don't give reliable information about where the most crime is happening but about where the most policing is happening. What gets measured and subsequently fed into policing algorithms are the incidents that are reported to police or that the police themselves report and the people police arrest. But the crime that is reported to police varies by community: White and wealthier communities are less likely to report crimes to the police. And even where the data shows that Black and white people are likely to commit certain offenses at the same rate — for example, offenses relating to drug use and sale — in many cases Black people are significantly more likely than white people to be arrested or incarcerated. Crime forecasting tools take the data from that kind of biased policing and represent it as objective evidence of where future offenses will be committed and by whom.

For more information on the risks and biases of crime forecasting and historial police data, see:

Rashida Richardson, Jason M. Schultz, Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice.

Kristian Lum, William Isaac, *To predict and serve?*, https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x.

Bernard E. Harcourt, "Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age."

Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273800.

Matt Shroud, "Heat Listed," https://www.theverge.com/22444020/chicago-pd-predictive-policing-heat-list.

Aaron Sankin, Dhruv Mehrotra, Surya Mattu, Annie Gilbertson, "Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them," https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

United States v. Curry, 4th Cir. 2020, https://www.ca4.uscourts.gov/opinions/184233A.P.pdf.

Face recognition technology

BASICS

Face recognition technology, also called facial recognition, is a biometric tool used to determine the likelihood two images are both representations of the same person's face. Law enforcement agencies use face recognition software to attempt to identify people in photos or video footage. There are generally two types of face recognition: one-to-one matching, which compares two photos to one another to verify they're the same person, and one-to-many matching, which compares one photo to a database to identify someone. In the latter, officers upload a probe photo of a face to be identified and an algorithm analyzes its features, compares it to a database of face photos and then issues a list of potential matches along with a numerical confidence score for each.

During a face recognition search, an algorithm detects the presence of a face in the probe photo. Then it scales and rotates the image so it is in a standard position for comparison. Next, it creates a face "template" by extracting facial features like eyes and nose from the image. Finally, it compares this template to the template of another face photo, assigning a score based on the likelihood the two templates represent the same face.

For more on the basics of face recognition technology, see:

Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, https://www.perpetuallineup.org.

Stan Z. Li, Anil K. Jain, "The Handbook of Face Recognition," Second Edition, https://www.researchgate.net/publication/235709405_Handbook_of_Face_Recognition_the_second_edition.

WHAT FACE RECOGNITION TOOLS ARE BASED ON

Face recognition tools have two constituent parts: an algorithm applied to a face photo and a database to which analyzed face photos are compared. The algorithm, which is typically shielded from public view by copyright law, is created by "machine learning" — training on vast sets of labeled data. The more data the algorithm processes, the better it gets at matching. The algorithm detects patterns in facial features and applies those patterns to novel images.

The database is the collection of face photos to which face recognition users (in this case police) compare the result of the algorithm's analysis. It is the pool of people from which a match can be detected; only images within the database can be returned as a potential match. In many jurisdictions, police use mugshot photos as a database; in other jurisdictions, they also have access to driver's license photos. The company Clearview AI built a database with photos from the internet, which it assembled by scraping data from multiple internet platforms

in violation of their terms of service.

For more on what face recognition is based on, see:

Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, https://www.perpetuallineup.org.

Stan Z. Li, Anil K. Jain, "The Handbook of Face Recognition," Second Edition, https://www.researchgate.net/publication/235709405_Handbook_of_Face_Recognition_the_second_edition.

HOW FACE RECOGNITION TOOLS ARE USED

Law enforcement agencies use face recognition for two primary purposes: to verify an individual's identity and to identify an unknown individual. Verification uses one-to-one matching, whereas identification uses one-to-many. Officers use face recognition to try to identify people in the field, after they've been arrested, in a photo or video during an investigation, or on real-time video surveillance. As of 2016, around one-quarter of all 18,000 law enforcement agencies in the United States have access to face recognition. That means over half of all American adults have their face in a face recognition database, either at the local, state or federal level.

For more on how police use face recognition, see:

Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, https://forensicwithoutscience.org.

Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, https://www.perpetuallineup.org.

Andrew G. Ferguson, *Facial Recognition and the Fourth Amendment*, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=4252&context=mlr.

Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

BIASES

Bias can exist at a number of key points in a face recognition system: the algorithm, the database of faces and the human implementation of the technology. The algorithm can be biased if it's trained on data that favors lighter-skinned men — as many commercially available algorithms are — and performs worse on ethnic, racial and gender minorities. Like all other algorithmic tools, face recognition depends on training data, and if the data is low quality or incomplete, the results will also be low quality or incomplete. The comparison database can be biased if people of certain demographic groups are overrepresented.

Because low-income, Black communities and other communities of color are subject to greater levels of law enforcement, they are overrepresented in mugshot photo databases; when such a comparison database is used, those same people are more likely to be identified or misidentified.

Finally, face recognition can be implemented in harmful ways that reinforce bias. Officers can manipulate the probe photos they submit for searches: copying features from one face and pasting them onto another, heavily editing photos, or submitting composite sketches or celebrity lookalikes. Even in the absence of photo manipulation, investigating officers' implicit bias impacts their ability to analyze the results of face recognition searches; research indicates that most people are much worse at identifying faces than they believe, particularly people of different races.

For more on bias in face recognition, see:

Patrick Grother, Mei Ngan, Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology*, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, https://www.flawedfacedata.com.

Alex Najibi, "Racial Discrimination in Face Recognition Technology," https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology.

David White, James D. Dunn, Alexandra C. Schmid, Richard I. Kemp, *Error Rates in Users of Automatic Face Recognition Software*, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0139827.

Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

Christian A. Meissner, John C. Brigham, *Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review*, https://psycnet.apa.org/record/2001-14540-001.

IMPACTS OF INCREASED SURVEILLANCE

Face recognition alters the balance of power between people and governments, giving government agents the ability to identify and track people in secret. By virtue of being enrolled in a face recognition database, people are part of a perpetual lineup, always a potential suspect in a criminal investigation. The fear of government surveillance has chilling effects. It makes people less likely to attend protests or engage in political speech for fear of being watched. Typically when police want to identify someone, they need to do so manually, and when they want to search or track someone — including their location over time — they need to get a warrant. Face recognition allows police to bypass both of those mechanisms.

For more on face recognition's impact on surveillance, see:

Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, https://www.perpetuallineup.org.

Clare Garvie, Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, https://www.americaunderwatch.com.

Clare Garvie, "Public Protest, Face Recognition, and the Shield of Anonymity," https://medium.com/center-on-privacy-technology/public-protest-face-recognition-and-the-shield-of-anonymity-44daa8ad1e80.

Marketplace Tech, "Police can track protesters even after the demonstrations end," https://www.marketplace.org/shows/marketplace-tech/police-protesters-surveillance-tracking-facial-recognition.

Tawana Petty, Logic Magazine, "Safe or Just Surveilled?: Tawana Petty on the Fight Against Facial Recognition Surveillance," https://logicmag.io/security/safe-or-just-surveilled-tawana-petty-on-facial-recognition.

International Justice and Public Safety Network, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field,* June 30, 2011, pg. 2, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

Risk assessment tools (RATs)

BASICS

Risk assessment technologies (RATs) are a general class of algorithms that calculate the probability, based on past law enforcement data, that a person will have a particular interaction or outcome in the criminal legal system, such as being arrested or missing a court hearing. Typically, judges and corrections officials consult RATs when making decisions about the level of state control or supervision a person will receive — for example, how to set bail, how long a criminal sentence will be or whether to grant parole.

Criminal legal system officials rely on RAT scores when making decisions about bail; sentencing; case management in jail, prison, and during parole; discretionary release/parole; and conditions of probation. Depending on the jurisdiction, officials may use the same RAT product at several decision points (for example, in decisions about both sentencing and parole), or they may use different RAT products marketed for a specialized purpose (for example, "predictive policing").

For more on the basics of risk assessment tools, see:

"Public Safety Risk Assessment Clearinghouse," Bureau of Justice Assistance, US Department of Justice, https://psrac.bja.ojp.gov.

"Use of Valid Actuarial Assessments of Risks and Needs," National Parole Resource Center, https://nationalparoleresourcecenter.org/action-guide-use-of-valid-actuarial-assessments-of-risks-and-needs/selecting-and-validating-an-assessment-instrument.htm.

Keith Porcaro, "Detain/Release: simulating algorithmic risk assessments at pretrial," https://medium.com/berkman-klein-center/detain-release-simulating-algorithmic-risk-assessments-at-pretrial-375270657819.

Alex Chohlas-Wood, "Understanding risk assessment instruments in criminal justice," https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice.

WHAT RATS ARE BASED ON

RATs give predictive weight to correlations between previous defendants' characteristics and their outcomes in the criminal legal system. Prior criminal history is by far the most common factor used in RATs: a person with an extensive history of contact with the criminal legal system, for example, is likely to be classified by an RAT

as high risk. RATs also take into account data from law enforcement about an individual's drug use, family and social support, community or neighborhood, and employment status.

When RATs receive data about a new person, they will give a score reflecting the individual's supposed risk, as the algorithm calculates, based on these factors.

For more on what risk assessment tools are based on, see:

"Public Safety Risk Assessment Clearinghouse," Bureau of Justice Assistance, US Department of Justice, https://psrac.bja.ojp.gov.

Melissa Hamilton, *Back to the Future: The Influence of Criminal History on Risk Assessment*, https://www.researchgate.net/publication/310326909_Back_to_the_Future_The_Influence_of_Criminal_History_on_Risk_Assessment.

Stanford Pretrial Risk Assessment Tools Factsheet Project, https://law.stanford.edu/pretrial-risk-assessment-tools-factsheet-project.

Laurel Eckhouse, Kristian Lum, Cynthia Conti-Cook, Julie Ciccolini, *Layers of Bias: A Unified Approach for Understanding Problems With Risk Assessment*, https://journals.sagepub.com/doi/abs/10.1177/0093854818811379.

COMPAS PRRS-II Risk Assessment Factsheet, https://www-cdn.law.stanford.edu/wp-content/uploads/2019/06/COMPAS-PRRS-II-Factsheet-Final-6.20.pdf.

Public Safety Assessment, https://advancingpretrial.org/psa/factors.

RISKS AND BIASES

While originally marketed as a way to reduce mass incarceration, reform the bail process, combat bias in judicial decisions and more efficiently allocate scarce resources, RATs can actually fuel inequities. The problems with RATs can be broken down into six main issues:

1. There is no consensus on what makes an RAT algorithm fair.
2. RATs use real-life data, reflecting an inequitable and biased criminal legal system.
3. Because of existing inequities in the criminal legal system and society more broadly, data that is on its face race-neutral, such as ZIP codes, can be used as a proxy for race.
4. Judges' interpretations of risk scores vary greatly, and there is no established criteria for distinguishing levels of risk in the first place.
5. Many algorithms are developed by private actors and hidden from outside inspection, making them impossible to audit.

6. RATs base their calculations of individual behavior on data about group behavior, which may have constitutional equal protection implications under the 14th Amendment.

Competing notions of "fairness" in algorithms

RAT models vary based on the variables developers choose and how they're weighed. A developer's goal is to make an algorithm whose outputs most closely match the outcomes in the data on which the algorithm is trained. Beyond that, there's the question of whether an algorithm is "fair," but there are conflicting, incompatible notions of "fairness" in algorithms.

Biased criminal legal system data

Not only are RATs built on data that reflects biased criminal legal system practices, but the outcomes they purport to predict — probability of rearrest, for instance — are also impacted by those biases. Black people and other people of color are more likely to be stopped and searched by police; be arrested and convicted for drug possession; be surveilled in their neighborhoods; prosecuted; receive harsher sentences; and be excluded from pretrial counseling and support programs. An algorithm that calculates a probability an individual will be rearrested, for example, includes in that calculation future biased policing. Rearrest is not a neutral, objective measure; because police disproportionately target Black people, arrest rates reflect not criminal activity but law enforcement behavior.

Use of proxy variables masks discrimination

Even though characteristics like race and class are not explicitly factored into RATs, other variables can act as proxies, meaning seemingly innocuous categories can mask discrimination. For example, because of racial disparities in policing and sentencing, "risk" — and by extension criminal history — act, in essence, as a proxy for race. Variables like ZIP code, income and education level also function as proxies for race and class because of segregation and other existing social disparities.

Varying judicial interpretations of risk scores

Most RATs present risk scores as numbers on a scale or a low-medium-high spectrum, and it's not clear how judges are supposed to translate these scores when making decisions. Nor are there criteria for determining how to categorize risk scores in the first place, with labels like "high risk" and "low risk" applied arbitrarily. It is up to the judges using these tools, who don't understand how they work, to interpret them.

Secretive nature of algorithmic models

Because many RATs are proprietary, the algorithms that power them are often hidden from public view. The public has general ideas about the factors they do and don't consider, but their exact nature and the weights

given to each is often unknown. That makes it impossible to audit the tools, and judges who rely on the scores don't understand how they work.

Judgment of individuals based on group behavior

The calculations RATs make about individuals are based on data about the behavior of other people with similar characteristics. That is potentially in tension with the constitutional law principle that people have the right to be judged based on their individual behavior, not as part of groups. The level of "risk" assigned to an individual, whether it's risk of missing a trial or committing another crime, is based on whether people with similar traits did so. This would be true even if it were possible to create a perfectly statistically "fair" and unbiased RAT.

For more on the risks and biases of risk assessment tools, see:

John L. Koepke, David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041622.

NYCLU, *The Problem with Pretrial Risk Assessment Tools*, https://www.nyclu.org/en/publications/problems-pretrial-risk-assessment-tools.

Laurel Eckhouse, Kristian Lum, Cynthia Conti-Cook, Julie Ciccolini, *Layers of Bias: A Unified Approach for Understanding Problems With Risk Assessment*, https://journals.sagepub.com/doi/abs/10.1177/0093854818811379.

Andrea Bonezzi, Massimiliano Ostinelli, *Can algorithms legitimize discrimination?*, https://psycnet.apa.org/record/2021-28943-001.

Alexandra Chouldechova, *Fair prediction with disparate impact: A study of bias in recidivism prediction instruments*, https://arxiv.org/abs/1610.07524.

Movement Alliance Project, MediaJustice, Mapping Pretrial Injustice, https://pretrialrisk.com.

Bernard E. Harcourt, R*isk as a Proxy for Race: The Dangers of Risk Assessment*, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3568&context=faculty_scholarship.

David A. Harris, *The Reality of Racial Disparity in Criminal Justice: The Significance of Data Collection*, https://scholarship.law.duke.edu/lcp/vol66/iss3/4.

RAT: BAIL (PRETRIAL)

Defendants often first encounter RATs before trial during their bail hearing. Here, judges use RATs in one of two ways: to gauge the likelihood of an individual's failure to appear at their trial or to assess their likelihood of being rearrested before trial. Over time, bail has shifted from the former, a means of ensuring court appearances, to the latter, a mechanism for withholding an individual's liberty on the basis of their supposed "dangerousness" to the community. This question has become a major point of deliberation for judges making decisions about bail, for which they consult RATs.

RAT: JAIL CASE MANAGEMENT, PLANNING AND SUPERVISION

In jail, case managers use RATs to supplement the process by which they evaluate incarcerated peoples' supposed risk of being rearrested in the future and what resources may reduce that supposed risk.

When case managers estimate whether a person is at risk of being charged with misconduct while incarcerated or rearrested after leaving jail, they consider factors such as physical and mental health, records of substance abuse, education, housing situation and employment history. Some case managers rely on RAT risk scores to make those judgments.

RAT: SENTENCING

Judges use RATs to inform sentencing decisions. RATs calculate the probability that a person will be arrested again in the future. Judges may rely on that calculation in making a judgment about that person's supposed "dangerousness." In contrast to pretrial RATs, which make binary recommendations about whether to detain or release someone, judges use sentencing RATs in complex decisions about the nature, duration and severity of punishment.

RAT: PRISON CASE MANAGEMENT, PLANNING, AND SUPERVISION

In prison, case managers use RATs when evaluating incarcerated peoples' needs and risks and in making decisions related to supervision and rehabilitation. When case managers estimate whether a person is at risk of being charged with misconduct while incarcerated or rearrested after leaving prison, they consider factors such as physical and mental health, records of substance abuse, education, housing situation and employment history.

RAT: DISCRETIONARY RELEASE/PAROLE

When deciding whether to release an incarcerated person early on parole (also known as discretionary release), parole boards may use RAT scores in determining whether a person is likely to be arrested again. RATs generate these scores using algorithms trained to detect statistical relationships within massive datasets drawn from historical criminal legal system records. That may include data about type of conviction, length of incarceration, behavior while incarcerated, record of criminal legal system involvement, mental health records, gender, education level and age.

RAT: PAROLE CASE MANAGEMENT

Once a person is on parole, a parole officer uses RAT scores to make decisions about what level of supervision the individual receives or what interventions — such as substance abuse rehabilitation or behavioral therapy — they are recommended for.

There is little research documenting the ways parole officers use the information from RATs when making those decisions or investigating the extent to which parole officers receive training or are subject to internal policies and guidance when using RATs.

RAT: PROBATION

Probation officers use RATs to make decisions about supervision levels, service and treatment interventions, and pretrial decisions for individuals on probation. Probation is an alternative to incarceration, occurring instead of or following incarceration.

For more on how risk assessment technologies are used at different stages of the criminal legal system, see:

"Public Safety Risk Assessment Clearinghouse," Bureau of Justice Assistance, U.S. Department of Justice, https://psrac.bja.ojp.gov.

John L. Koepke, David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041622.

Movement Alliance Project, MediaJustice, Mapping Pretrial Injustice, https://pretrialrisk.com.

Megan T. Stevenson, *Assessing Risk Assessment in Action*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3016088.

Danielle Kehl, Priscilla Guo, Samuel Kessler, *Algorithms in the Criminal Justice System: Risk Assessments in Sentencing*, https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf.

"Use of Valid Actuarial Assessments of Risks and Needs," National Parole Resource Center, https://nationalparoleresourcecenter.org/action-guide-use-of-valid-actuarial-assessments-of-risks-and-needs/selecting-and-validating-an-assessment-instrument.htm.

Other algorithmic criminal legal system technologies

Image analysis and recognition

Face recognition is just one example of image analysis technologies, which law enforcement uses to attempt to classify or identify people or objects based on an image. Iris recognition, for example, detects unique patterns of a person's iris and calculates the likelihood that two irises are from the same person. Police use tattoo analysis not only to attempt to identify people but to infer other information such as political beliefs, religious practices or associations with others. While not a biometric technology, object recognition functions similarly in that police use it to attempt to classify or identify objects based on its features.

For more on image analysis and recognition, see:

Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

John Daugman, *How Iris Recognition Works*, https://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf.

Electronic Frontier Foundation, "Tattoo Recognition," https://www.eff.org/pages/tattoo-recognition.

MathWorks, "Object Recognition: 3 things you need to know," https://www.mathworks.com/solutions/image-video-processing/object-recognition.html.

Joy Buolamwini, "Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces," https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

Behavior analysis and recognition

Law enforcement uses a range of technologies besides face analysis and recognition to attempt to identify, or make inferences about, people based on aspects of their physical person. They use gait analysis, for instance, to detect patterns in the particularities of how individuals walk, either to identify suspects, or to make inferences about their mood and internal emotional state. They use voice and speech analysis to attempt to identify or verify speakers or attempt to infer certain characteristics of the speaker such as gender, age and emotional state (*see* Communication analysis technologies).

For more on behavior analysis and recognition, see:

Ashish Badiye, Prachi Kathane, Kewal Krishan, *Forensic Gait Analysis*, https://www.ncbi.nlm.nih.gov/books/NBK557684.

Alka Agrawal, Raees Ahmad Khan, Nilu Singh, *Voice Biometric: A Technology for Voice Based Authentication*, Advanced Science, Engineering and Medicine, July 2018, Vol. 10, No. 7, pg. 1-2, available at https://www.researchgate.net/publication/324031666_Voice_Biometric_A_Technology_for_Voice_Based_Authentication.

Summer Allen, *Giving Voice to Emotion: Voice Analysis Technology Uncovering Mental States is Playing a Growing Role in Medicine, Business, and Law Enforcement*, IEEE Pulse Vol. 7, Issue 3, May-June 2016, available at https://pubmed.ncbi.nlm.nih.gov/27187541.

Automated license plate readers (ALPRs)

ALPRs (also sometimes called automatic number-plate recognition) use cameras to capture license plate numbers, then digitize those images and upload them into a database that law enforcement can search and share. Police and other law enforcement agencies use them to track a vehicle's travel patterns. ALPRs are a form of dragnet surveillance that records the license plate — as well as time and place — of every car that passes within a particular camera's frame. The data from ALPRs is stored for long periods of time, usually by private contractors, allowing law enforcement to track individuals' locations and movement. According to vendors, that information can tell police where a plate has been, identify travel patterns and link vehicles to one another.

For more on ALPRs, see:

Electronic Frontier Foundation, "Automated License Plate Readers (ALPRs)," https://www.eff.org/pages/automated-license-plate-readers-alpr.

Dave Maas, "Data Driven 2: California Dragnet—New Data Set Shows Scale of Vehicle Surveillance in the Golden State," https://www.eff.org/deeplinks/2021/04/data-driven-2-california-dragnet-new-dataset-shows-scale-vehicle-surveillance.

Automated police databases and alert systems

Police have begun shifting away from query-based police databases and toward alert-based systems. Query-based systems require police to manually run searches on individuals, whereas alert-based systems notify police in real time when certain variables are present. For example, an officer can set up a geofence around a particular area, or for a specific individual, and receive alerts whenever a warrant is issued inside the geofence or on the individual. Algorithms within these systems also compare data across cases and highlight potential links between them. But even the results of queries and alerts become data points: Because the tool tracks searches, an individual coming up consistently is marked, by virtue of repeated searches, as suspicious.

For more on automated police databases and alert systems, see:

Sarah Brayne, *Big Data Surveillance: The Case of Policing*, American Sociological Review, Vol. 82(5) 977-1008 (2017).

Gunshot detection

Gunshot detectors use sensors to detect a gunshot sound and triangulate the approximate location. However, because they are essentially microphones, there is concern they could be used for more general mass surveillance.

For more on gunshot detection, see:

ACLU, Community Control Over Police Surveillance: Technology 101, pg. 5, available at https://www.aclu.org/report/community-control-over-police-surveillance-technology-101.

MacArthur Justice Center, End Police Surveillance, https://endpolicesurveillance.com.

"Smart" city infrastructure

"Smart" cities refers to the use of sensors embedded in city infrastructure to inform the management and administration of daily city functions. These sensors collect data on everyday operations of the city and its occupants — on things such as energy use, package delivery, street lighting and parking — and city officials analyze that data to make decisions about resource use. This infrastructure expands surveillance of city inhabitants and provides increasing amounts of data for police to map and analyze people's behaviors within the city.

For more on "smart" city infrastructure, see:

Ida B. Wells Just Data Lab, "Smart Cities," https://www.thejustdatalab.com/tools-1/smart-cities-5hdnl.

Elizabeth Joh, *Policing the Smart City*, https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/policing-the-smart-city/D107A5808D6561101FE1C54550AF2D95.

Elizabeth Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing,* Harvard Law & Policy Review, Vol. 10, 2016, pg. 15-16, available at https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/harlpolrv10&id=20&men_tab=srchresults.

Probabilistic genotyping

Probabilistic genotyping is a method of analyzing genetic material from crime scenes to determine whether it matches a suspect's DNA. In this method, software calculates the probability that a particular piece of DNA matches that of a person of interest.

For more on probabilistic genotyping, see:

Government Accountability Office, "Science & Tech Spotlight: Probabilistic Genotyping Software," https://www.gao.gov/assets/gao-19-707sp.pdf.

AI Now Institute, *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems,* https://ainowinstitute.org/litigatingalgorithms.pdf.

Communication analysis technologies

Police and corrections officials increasingly use algorithms to analyze written and spoken communications. These algorithms label a person's emotional state based on things like the words they use, how their voice sounds and their body language. While there is no information about how widespread these technologies are, they can be used at various parts of systems of policing and punishment.

Prison officials use sentiment analysis technology to search people's phone calls and letters for supposed evidence of crime or possible suicide attempts; police investigators use it when monitoring social media to understand public opinion and search for apparent signs of crime; and attorneys use it to evaluate and select jurors. These algorithms are trained on text or speech data to identify language that the developers label as positive, negative or neutral in tone. Some algorithms go beyond this binary to calculate the supposed probability a given piece of communication exhibits other emotions and sentiments, as determined by developers.

For example, prison officials can use this technique to search inmates' recorded phone conversations for certain keywords. That includes an algorithm that converts the inmates' voice to text and then flags specific words or phrases of interest within the text. If officials are looking for signs of possible suicide attempts among inmates, for instance, they can automatically flag conversations containing words that developers have associated with suicide or self-harm based on training data (*see* Behavior analysis and recognition).

For more on communication analysis technologies, see:

David Sherfinski, Avi Asher-Schapiro, "'Scary and chilling': AI surveillance takes U.S. prisons by storm," Reuters, https://www.reuters.com/article/usa-prisons-surveillance-idUSL8N2RP5LL.

David Sherfinski, Avi Asher-Schapiro, "U.S. prisons mull AI to analyze inmate phone calls," Reuters, https://www.reuters.com/article/us-usa-tech-prison/u-s-prisons-mull-ai-to-analyze-inmate-phone-calls-idUSKBN2FA0OO.

Sidney Fussell, "This AI Helps Police Monitor Social Media. Does It Go Too Far?," WIRED, https://www.wired.com/story/ai-helps-police-monitor-social-media-go-too-far.

Todd Feathers, "This Company Is Using Racially-Biased Algorithms to Select Jurors," Vice, https://www.vice.com/en/article/epgmbw/this-company-is-using-racially-biased-algorithms-to-select-jurors.

Beyond the legal system: the integration of law enforcement and non-law enforcement data

Digital technologies facilitate the increasing production and collection of data, which in turn further fuel the development of algorithmic technologies. Collection of personal data has proliferated in both the public and private sector, creating opportunities to target individuals for purposes of persuasion or social control. This new surveillance landscape has two complementary effects on the criminal legal system: 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. The former renders increasing amounts of personal data subject to law enforcement surveillance and scrutiny; the latter further extends the label of "criminal" beyond the legal system further into the personal realm.

The aforementioned technologies are just a portion of all algorithmic tools available to law enforcement, which in turn are just a segment of all surveillance technologies. Still more are in development or being planned for the future.

For more on the mixing of law enforcement and non-law enforcement data and how algorithmic tools are increasingly used to police people beyond the criminal legal system, see:

Sarah Brayne, *Big Data Surveillance: The Case of Policing*, *American* Sociological Review, Vol. 82(5) 977-1008 (2017).

Zeynep Tufekci, *Engineering the public: Big data, surveillance and computational politics*, https://journals.uic.edu/ojs/index.php/fm/article/download/4901/4097.

Shoshanna Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power."

Elizabeth E. Joh, "Increasing Automation in Policing," https://cacm.acm.org/magazines/2020/1/241710-increasing-automation-in-policing/fulltext.

Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers.

Ifeoma Ajunwa, *The Modern Day Scarlet Letter*, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5110&context=flr.

The Sentencing Project, "Collateral Consequences," http://www.sentencingproject.org/template/page.cfm?id=143.

Dara Lee Luca, T*he Digital Scarlet Letter: The Effect of Online Criminal Records on Crime,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1939589.

Miranda Bogen, "All the Ways Hiring Algorithms Can Introduce Bias," https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

Latanya Sweeney, *Discrimination in Online Ad Delivery*, https://arxiv.org/abs/1301.6822.

Virginia Eubanks, "Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor."

Danielle K. Citron, Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4796&context=wlr.

Safiya Umoja Noble, "Algorithms of Oppression: How Search Engines Reinforce Racism."


GEORGETOWN LAW
Center on Privacy & Technology