Now is the time to regulate AI in law enforcement;

Presented to The Department of Justice

Student ID: 1223546 October 28th, 2020

Executive Summary

Artificial Intelligence (AI) in policing presents an emerging threat to free society. The Constitutional guarantee of fair and equal application of the law is incompatible with the shrouded secrecy of AI techniques proliferating in precincts across the country. The Department of Justice (DOJ) must act to create a robust legal structure to regulate how Federal, state, and local law enforcement use AI to execute their duties in service of the public. To ensure equal protection under the law, the DOJ should publish guidance for law enforcement agencies' use of AI and any related technology. If a citizen can be suspected, accused, questioned, detained, tried, convicted, or imprisoned based on the output of an algorithm, then the technical details of that algorithm and all supporting technology, institutional practices, and specialized knowledge about that algorithm must be subpoenable. Holding law enforcement accountable to basic evidentiary standards will require that technological methods be accessible to the accused, and over time, legal precedent will encourage police to make their data and methods open source by default.

Background

The expansion of AI and large scale data analysis represents a major inflection point in the power of local police departments. All government agencies are motivated to increase effectiveness while reducing costs. Integrating technology into local law enforcement saves time and money by making administration more efficient, thereby saving labor hours which is effectively the same as hiring more officers. AI technologies deploy algorithms on massive datasets produced by police actions like arrests to generate predictive models of crime patterns in communities. These predictive metrics allow police departments to strategically allocate resources with the intent of crime reduction or even prevention. If a precinct commander can predict with reasonable accuracy where and when a crime is most likely to occur, then they can assign more officers to the beat, or, as was the case in Chicago, intervene directly with persons determined to have a high propensity for crime[1].

From a strictly financial and efficiency perspective, the case in favor of predictive policing appears conclusive at first blush. However, AI's unintended consequences erode the

core tenets of the American legal system. New York City's now infamous 'stop and frisk' policy of aggressively enforcing low-level crimes resulted in racial profiling and the broad targetting of whole communities by police. By the same measure, if an algorithm deems a certain region in a city to have higher propensity for crime, extra police attention drawn to that area will result in more arrests and crime reports which, in turn, supply the training data for the algorithm. A negative feedback loop confirms the algorithm's initial bias. Police agencies will defend their discriminatory practices because they derive from the judgements of an ostensibly impartial AI.

Further downstream from arrests are parole and sentencing hearings where AI generated 'risk assessments' have become commonplace determinants of people's freedom. Risk assessments apply the tools of actuarial analysis that calculate the probability of an insurance claim. For instance, how prone someone is to illness determines how much they may pay for health insurance. Criminal risk assessment produces similar scores for defendants' likelihood of skipping bail or recidivism upon release. Again, there is an input problem and a false assuredness of impartiality. The training data fed into risk assessment algorithms are primarily past incidence of contact with the legal system, which is more likely among heavily policed areas. The vicious cycle then becomes amplified into a higher orbit as parents are removed from their children's lives by the state. Instead of ameliorating implicit bias in the judicial system, we amplify the effects of structural racism because poverty and racial factors are overrepresented in criminal risk models[2,3].

Policy Recommendations

The harms caused by the deployment of AI in law enforcement, either knowingly or by circumstance of technology or institutional practice, stem from a vacuum of governance. Currently, most police AI systems are protected as proprietary methods and copyrights of private companies, and Freedom of Information Act (FOIA) requests are routinely denied on these grounds[4]. Without open access to the tools governing our society, citizens are alienated from their right to monitor their government, much less hold it accountable. Secondly, law enforcement algorithms are diverse in scope and application across jurisdictions. Each contract between state or local agencies and AI companies is designed to suit the needs of the signatories, not necessarily the interests of the public. Lastly, no federal mandate exists to govern the management of police data. To address these issues, I recommend the following policies:

1) All data, methods, and technical details of AI products used by law enforcement agencies, as well as any related technology, should be subpoenable without exception.

2) Going forward, all procurement contracts between law enforcement agencies and AI companies must include end-to-end open source architecture.

3) The Department of Justice must publish guidance on data provenance modeled after New York City's recent law that requires annual reports of all surveillance technology used by the NYPD[5].

Conclusion

Last year, President Trump issued an Executive Order on AI regulation that mostly admonishes against Federal intervention: "Where a uniform national standard for a specific aspect related to AI is not essential, however, agencies should consider forgoing regulatory action."[6] No sector is in more urgent need for national standards than AI in law enforcement. Leaving open this vacuum of governance and allowing each jurisdiction to decide their own rules undermines American's Constitutional rights to equal protection under the law. Even more fundamentally, the ability to challenge one's own imprisonment and mount an effective defense are being eroded by AI. Sacrificing *habeas corpus* to secure the profits of surveillance companies is an unwise bargain. Leaving this debate for a more convenient season will condemn another generation of our most vulnerable citizens to the brutal realities of structural racism. Surely, limiting the growth of technology and innovation will make the police's job more difficult. But, to quote Orson Welles' film *Touch of Evil*, "A policeman's job is only easy in a police state."

References:

1. Saunders, Jessica, et al. Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. J Exp Criminol 12, 347–371 (2016). https://doi.org/10.1007/s11292-016-9272-0.
2. Harcourt, Bernard E. Risk as a Proxy for Race: The Dangers of Risk Assessment. Columbia Law School Scholarship Archive (2015). https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3568&context=faculty_scholarship.
3. Angwin, Julia, et al. Machine Bias. ProPublica (2016). https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing .
4. Heilweil, Rebecca. Why we don't know as much as we should about police surveillance technology. Recode (2020). https://www.vox.com/recode/2020/2/5/21120404/police-departments-artificial-intelligence-public-records.
5. Granicus, Inc. 2020. " The New York City Council - File #: Int 0487-2018 ". Legistar.Council.Nyc.Gov. https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=&Search=.
6. 2020. Whitehouse.Gov. https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.