Algorithmic Governance in Law Enforcement Report:

The Case of Predictive Policing

Nora Povejsil

King's College, London

Table of Contents

1. Executive Summary

This report focuses on predictive policing, which refers to using algorithms to anticipate criminal activity and prevent it from occurring in the first place. Two case studies involving a United States predictive policing company called PredPol and a Chinese company called Megvii are used to illustrate the ethical issues of each, how they are received by the public, and how the government uses and attempts to regulate them. The report highlights the rapidly developing technical approaches used in the field which has so far outpaced government regulation. Additionally, the social implications of increasingly technocratic law enforcement strategies are explored. This report is intended for regulators and other interested parties to begin understanding the field of predictive policing by exploring how cases have unfolded in two countries with contrasting ethical and regulatory standards for tech companies and the use of citizens' personal data.

2. Introduction

There are three forms of predictive policing: person-based (who will commit the crime), area-based (where the crime will occur), and event-based (what the crime will be) (Hung). The goals of predictive policing are to reduce crime by preemptively dispatching police to hotspots, identifying potential perpetrators and intervening before they break the law, and detecting signs of social unrest to prevent escalations like rioting and looting. Critically, government and law enforcement officials must understand the benefits and limitations of predictive policing, as well as the public's perception of it, which is dependent on attitudes towards surveillance and technology more broadly. The ethical challenges of predictive policing include sacrifices of privacy, requiring trust in non-transparent technologies, and an acceptance of technological failures that result in extreme consequences for individuals, including false accusations and potential discrimination. By analyzing predictive policing as it has developed in the U.S. and China (as of 2022), this report aims to compare and contrast the relationships between technology companies, governments, and citizens in both countries ("citizen" will be used in the sense of "inhabitant" in this report as opposed the legal definition). Understanding these stakeholders' varying willingness to address crime and punishment with algorithmic governance illuminates the growing challenge of technological development outpacing policy and public awareness.

3. Background

3.1 AI Technology

Predictive policing lies on the premise that taking relevant data, feeding it into predictive or identity-matching algorithms, and outputting statistically risky people and areas will better inform law enforcement in distributing their resources and efforts. The types of models and data used to achieve this vary depending on a company's algorithm and the country it is deployed, which dictates privacy standards and practices. While some use biometric matching and video analytics from surveillance cameras to match suspected individuals (Noorden), others use statistical risk analyses to map crime similarly to patterned phenomena like contagions or the weather (Mohler). Data sources include past crime data (location, time of day, type of crime), environmental characteristics associated with crime (foreclosures, multi-family homes, drug use), social media, and personal identifying data (including digital and biometric data like facial recognition, fingerprints, or even gait) (Ferguson). Methods used to transform these data into actionable predictions include but are not limited to hot spot analysis, regression methods, data mining, near-repeat, spatiotemporal analysis, and risk terrain analysis (Perry). The resulting models allow law enforcement to target people and areas for crime reduction. How law enforcement agencies execute that goal varies greatly.

3.2 The Field of Predictive Policing

Predictive policing is a rapidly developing field that has only become fairly popular (implemented in 53 countries) in recent years, becoming a major topic in ethical literature (Feldstein). In the U.S., federal funding towards research and technological innovation for crime prevention, along with newly available and vast amounts of data, accelerated efforts towards predictive policing (Ferguson 2017). Additionally, the alluring promise that stopping crimes before they happen would save money, time, and resources justified predictive policing due to its monetary, not just moral, return on investment (Mohler). Critically, it can improve operational efficiency and outperform police officers' local knowledge (Mohler). However, in order to deliver on these benefits, to reduce crime, protect citizens, and assist the police, it must also inevitably infringe on citizens' privacy. The data used to train many predictive policing models

come from collection methods akin to surveillance strategies. From training facial recognition algorithms on citizens to scraping personal information from social media, this kind of data collection renders individuals, regardless of whether or not they have committed a crime, perpetual suspects under scrutiny. Inaccuracy or unfairness in the resulting model exacerbates this issue and introduces differential impacts for marginalized people; often models trained on historical data are biased toward classifying members of minority groups as more likely to commit a crime due to embedded systemic prejudice in law enforcement (Bhuiyan).

4. Case Examples

4.1 Megvii and Chinese Predictive Policing

Governments implement predictive policing strategies that often incorporate technologies from multiple companies that provide distinct services. Chinese and U.S. companies are leading these technological developments in predictive policing and have had their own local successes and pushbacks in their implementations, as have countries to which they export their algorithmic products. In China, companies focus on video surveillance, facial recognition, and general "smart-city" AI applications (Ekman). Megvii, one of these companies, describes itself as a general Internet of Things company that includes " 7/24 all-round automated supervision" for crime prevention (Megvii). It ingests data from video footage, photos, cases, and incident reports to parse and store information about faces, cars, names, and more (Mozur, Xiao). Megvii uses techniques including biometric recognition (including facial recognition), detection of illegal behaviours, and most controversially, group categorisation (Peterson, Mozur). Categorisation is a tool used by other Chinese AI companies, which has sparked outrage among the international community, especially its use in the Western region of Xinjiang and beyond to target the movements of the Uighurs, a largely Muslim subsect of the Chinese population (Mozur). Megvii claims to be "concerned about the well-being and safety of individual citizens, not about monitoring groups," however their technology is undeniably a critical part of China's surveillance architecture (Mozur).

4.2 PredPol and United States Predictive Policing

In the U.S. on the other hand, China's biggest AI technology rival, predictive policing has been adopted by local law enforcement agencies in a slightly less invasive, but still controversial, manner. Many companies have been a part of the localised patchwork of preventative crime

efforts in the U.S. One of the most well-known companies, PredPol, provides a service specifically designed for predictive policing. PredPol's machine learning algorithm predicts locations of future crimes based on past crime data combined with localised risk terrains. It was developed by researchers at UCLA with the Los Angeles Police Department (LAPD) according to the theory that, put succinctly, less extreme crimes lead to more extreme crimes happening later in the same area (Bhuiyan). Experts have classified PredPol's underlying mathematical model as relatively simplistic and often racially biased due to existing neighbourhood-level prejudices in law enforcement systems (Bhuiyan). Because it is place-based, it effectively only functions for one-off crimes specifically tied to an address or city block, such as burglary (Ferguson). Consequently, research has demonstrated that PredPol has had little effect on crime rates in the U.S. and the U.K. (Ferguson). Part of this has to do with the fact that PredPol is a tool to direct police to risky areas in the hopes that their presence will deter criminal behaviour, which does little to address the root causes of crime (Mohler). Regardless of the technology's simplicity, its novelty in the field and the often discriminatory impacts that it produced have made it a famous example of predictive policing software.

As the pace of development for predictive policing technology rapidly increases, both companies serve as notable examples in their respective countries and export their algorithms globally (Ekman). Megvii differs from PredPol in its ability to integrate surveillance systems and advanced Internet of Things-based data collection methods that can pinpoint specific individuals. PredPol stays away from biometric data to inform police surveillance, instead focusing on areas of crime risk rather than, for the most part, individuals. Both companies, however, aid in alleged discriminatory police practices and allow for unprecedented state surveillance power (Ferguson 2017). Through the "solutions" they provide, AI-based technology companies like Megvii and PredPol influence how governments' and citizens' attitudes towards the role of surveillance in society evolve in tandem with technology.

5. Ethical Issues

The main ethical issues that arise from predictive policing include technological failures (i.e. incorrect predictions), accountability, privacy, safety, and discrimination. First,

technological failures are inevitable, as most predictive policing efforts rely on probabilistic inferences (never with 100% certainty) to predict where and when crime will happen and who will commit it (Hung). Instances of stopping innocent people occur both with and without the help of predictive policing. However, algorithmic decision-making in policing reduces accountability, as a computer program cannot be held "responsible" in the same way that a human can be (Hung). Thus, technological failures in conjunction with the lack of accountability and recourse for inanimate algorithms create a situation rife with ethical problems; when it comes to questions of due process or invasions of privacy or discrimination, there is no clear precedent for taking a proprietary black box algorithm and its developers to task (Ferguson).

Governments tend to argue that privacy is the tradeoff for public safety, and hence increased surveillance as a result of predictive policing is justified because of its crime reduction impacts. Citizens' rights are prioritised such that when one's right to life is at stake, privacy falls down the list of priorities (Hung). For example, the marketing of Chinese smart cities by both the government and involved technology companies tends to highlight the values of community safety over all else (Mozur, Xiao). To the Chinese government, social stability is the paramount priority, and predictive policing serves to combat any threat to it before it arises (Mozure, Xiao). Similarly, in the post 9/11 era in the U.S., more targeted surveillance on "at-risk" groups, in addition to "dragnet" surveillance on the whole population, gained major traction in a nation that prioritises privacy to a greater extent than most other nations (Brayne). However, the U.S. differs from China in its relative restraint in using advanced technologies for surveillance on a population-wide scale, with less emphasis on individual identities until someone becomes "high-risk."

Discrimination in predictive policing is at the forefront of international debate. The example of China's "anti-terrorism" efforts in Xinjiang, which some countries have characterised as genocide, has been in large part aided by AI technology companies such as Megvii (BBC). The government used facial recognition to identify Uighurs, collected DNA samples, and employed a variety of other AI-powered surveillance strategies to facilitate the "crackdown" on terrorism (Mozur). The Chinese government has been known to preemptively detain civilians and forcefully squash civil unrest (Mozur, Xiao). Chinese companies like Megvii have faced

difficulty in exporting their software to the U.S. and Europe after being blacklisted for their involvement in authoritarian political operations in Xinjiang and elsewhere in China (predictive policing technologies and biometric data collection are now common in 16 different provinces and regions across China as of 2018) (Ekman, Mozur). Other countries, whose governments' values on safety over privacy that China exhibits, what some would call "AI totalitarianism," for example Serbia, have adopted Chinese predictive policing technologies (Hung, Ekman). The success that China has found in their global exports is limited by the number of countries that share their attitudes towards surveillance and government power.

Similarly, PredPol has garnered its fair share of criticism for perpetuating discrimination against minorities and for increasing surveillance in already disproportionately-policed neighbourhoods. In Los Angeles, the LAPD's implementation of PredPol only deepened existing, mutual distrust between police and civilians, especially in communities of colour (Bhuiyan). Because it uses data from already biased police databases, PredPol's algorithm to some extent inherits and perpetuates systemic racial disparities (Feldstein). At a time when police violence and prejudice have been top of mind for many Americans, the public has been quick to raise an eyebrow at supposedly "neutral" algorithmic solutions (Metz). As a result, some cities, like Los Angeles, terminated their contracts with PredPol but continued to use big data analytics and predictive policing under rebranded "community policing" efforts (Bhuiyan). Ultimately, the scepticism that predictive policing garners in the U.S. has only sometimes resulted in its removal from law enforcement. Largely, public outcries have only driven law enforcement to become more secretive about the data and algorithms used in their work. Much of the government surveillance apparatus is invisible yet in plain sight, as police monitor citizens' online behaviour. PredPol and Megvii are two examples of predictive policing companies among many others, along with governmental agencies, that use data from social media (Binder), banking information, emails, medical care records, phone calls, car travel, and internet search histories to trace individuals' behaviour, potential criminal activity, and social movements like protests (Brayne). As these data sources create banks of evidence for law enforcement agencies to use to identify and prevent crime, they also open up the most intimate facets of life to government surveillance.

Public debate in the West (Hung) on predictive policing particularly emphasises how

governments politicise surveillance and justify it via security concerns to expand their capacities (Binder). American researchers suggest that the right to know, informed consent, privacy rights, and freedom of expression are key protections in ethical predictive policing implementation. Conversely, existing ethical standards for technology companies such as Megvii in China emphasize political compliance and state security as aspects of corporate social responsibility (Cave). Pushback against surveillance and discrimination exists within China, but much of it is silenced (Khatchadourian). As such, external and foreign criticism plays a large part in academic literature regarding the country's predictive policing practices.

6. Aspects of Regulation

In the U.S., the main legal hurdle in predictive policing programs is upholding the Fourth Amendment, which requires reasonable suspicion for stop-and-searches (Barrett). Algorithms and humans have different mechanisms by which they judge reasonable suspicion, and as such, a legal problem emerges when law enforcement relies on algorithms to justify a search (Hung). Furthermore, policies aimed at non-discriminatory prediction may be difficult to translate and incorporate into the algorithms themselves (Barrett). Additionally, from a logistical standpoint, laws in the U.S. on policing practices vary from locality to locality, leaving a patchwork of different policies with no central regulation, let alone AI regulation. In certain cities like Santa Cruz, California, predictive policing has been banned altogether (Kerber). In New York City, a Community Control Over Police Surveillance law was introduced in 2020, and in that same year, the LAPD stopped using PredPol as their predictive policing service (Kerber).

Predictive policing in China, especially in Xinjiang, infringes far more on personal privacy than in the U.S. However, there are regulations set in place such as the Data Security Law (2021), the Intelligence Law (2017), the Cyber Security Law (2016), and the State Security Law (2015), that stipulate appropriate uses of personal data by the government (Peterson). These laws protect against data collection and use by Chinese technology companies and law enforcement but are far less effective at curbing surveillance than in most Western countries (Peterson). Lawful versus unlawful behaviour can be vague in China, and as such there are more opportunities for law enforcement agencies to obtain access to personal data (Peterson).

7. Summary

Due to the speed and recency of predictive policing developments, regulation on the practice has lagged. In both the U.S. and China, despite their contrasting understandings of privacy and public safety, the same ethical issues arise in their approaches to predictive policing. In both countries, minority populations face discriminatory over-policing aided by predictive policing companies. While the approach of PredPol in the U.S. takes a more simplistic algorithmic approach than the Chinese company Megvii, it still produces similar ethical issues. Ethical norms in each country vary greatly, influencing efforts to regulate artificial intelligence in law enforcement. However, no specific and robust regulations on this issue exist in these countries at this time. Additionally, public opinion influences government action more in the U.S. than in China, meaning the adoption of predictive policing in the States has advanced only to backtrack after public outcry. In China, it has continuously expanded.

8. Recommendations

Predictive policing comes at a high price to personal privacy and can have potentially discriminatory impacts on minority populations who have been unfairly criminalised. To combat those harmful effects while retaining the potential benefit to public safety, there must be transparency in both the architecture of algorithms and in the surveillance efforts employed to collect the data. In other words, citizens should know how and where they are surveilled within their own country. Additionally, there must be regulation outlining the accountability of programmers in furthering discriminatory practices, which is an admittedly difficult task, as they are not fully responsible for what machine learning algorithms spit out. Finally, on a fundamental note, policies should be made to protect citizens; even though a technology designed to "prevent" crime exists (more to "interfere" with crime via police action), it could still do more social harm than good.

References

Barrett, L. (2018). Reasonably suspicious algorithms: Predictive policing at the United States border. [Online]. 23 January 2018. N.Y.U. Review of Law & Social Change. Available at:https://socialchangenyu.com/review/reasonably-suspicious-algorithms-predictive-policing-at-the-united-states-border/#iv-predictive-policings-pitfalls. [Accessed: 17 January 2023].

BBC News. (2022). Who are the Uyghurs and why is China being accused of genocide? [Online]. 24 May 2022. BBC News. Available at: https://www.bbc.com/news/world-asia-china-22278037. [Accessed: 17 January 2023].

Bhuiyan, J. (2021). LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws. [Online]. 8 November 2021. The Guardian. Available at: https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform. [Accessed: 17 January 2023].

Binder, C. (2016). Happenings Foreseen: Social Media and the Predictive Policing of Riots. *Sicherheit Und Frieden (S+F) / Security and Peace*, *34*(4), 242–247. http://www.jstor.org/stable/26429017

Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, *82*(5), 977–1008. http://www.jstor.org/stable/26426413

Cave, D., Hoffman, S., Ryan, F., and Thomas, E. (2019). Mapping more of China's technology giants. [Online]. 2019. Available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-12/Mapping%20more%20of%20Chinas%20tech%20giants.pdf?VersionId=wpDVHlKgXJHzeK8rZ.kmy0Ei63RxXMO. [Accessed: 18 January 2023].

Ekman, A., & de Esperanza Picardo, C. (2020). TOWARDS URBAN DECOUPLING?: China's smart city ambitions at the time of Covid-19. *European Union Institute for Security Studies (EUISS)*. http://www.jstor.org/stable/resrep25030

Feldstein, S. (2019). Types of AI Surveillance. In *The Global Expansion of AI Surveillance* (pp. 16–21). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep20995.8

Ferguson, A. G. (2017). Where We Police: Place-Based Predictive Policing. In *The Rise of Big*

Data Policing: Surveillance, Race, and the Future of Law Enforcement (pp. 20–33). NYU Press. https://doi.org/10.2307/j.ctt1pwtb27.5

Hung, TW., Yen, CP. On the person-based predictive policing of AI. *Ethics Inf Technol* 23, 165–176 (2021). https://doi.org/10.1007/s10676-020-09539-x

Kerber, V. (2022). A short history of predictive policing in the United States. [Online]. 30 May 2022. Medium. Available at: https://medium.com/@Vera_Kerber/a-brief-history-of-predictive-policing-in-the-united-states-ec3568e5c42c. [Accessed: 17 January 2023].

Khatchadourian, R. (2021). Surviving the crackdown in Xinjiang. [Online]. 5 April 2021. The New Yorker. Available at: https://www.newyorker.com/magazine/2021/04/12/surviving-the-crackdown-in-xinjiang. [Accessed: 17 January 2023].

Megvii. Available at: https://en.megvii.com/. [Accessed: 17 January 2023].

Metz, C. and Satariano, A. (2020). An algorithm that grants freedom, or takes it away. [Online]. 6 February 2020. The New York Times. Available at: https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html. [Accessed: 17 January 2023].

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., & Brantingham, P. J. (2015). Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, *110*(512), 1399–1411. http://www.jstor.org/stable/24740149

Mozur, P. (2019). One month, 500,000 face scans: How China is using A.I. to profile a minority. [Online]. 14 April 2019. The New York Times. Available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html. [Accessed: 17 January 2023].

Mozur, P., Xiao, M., & Liu, J. (2022). 'An Invisible Cage': How China is policing the future. The New York Times. Retrieved January 4, 2023, from https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Making Predictions About Potential Crimes. In *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (pp. 17–56). RAND Corporation.

http://www.jstor.org/stable/10.7249/j.ctt4cgdcz.10

Peterson, D., Hoffman, S. (2022). Geopolitical Implications of AI and Digital Surveillance Adoption. *Foreign Policy at Brookings*.

Van Noorden, R. (2020). *The ethical questions that haunt Facial-Recognition Research*. [Online]. 18 November 2020. Nature News. Available at: https://www.nature.com/articles/d41586-020-03187-3. [Accessed: 17 January 2023].