AFF

# AT Terrorism

## 100k false positives

Timme Munk, University Illinois at Chicago, "100,000 false positives for every real terrorist: Why anti-terror algorithms don't work | First Monday", August 2017, <https://journals.uic.edu/ojs/index.php/fm/article/view/7126/6522>

Can terrorist attacks be predicted and prevented using classification algorithms? Can predictive analytics see the hidden patterns and data tracks in the planning of terrorist acts? According to a number of IT firms that now offer programs to predict terrorism using predictive analytics, the answer is yes. According to scientific and application-oriented literature, however, these programs raise a number of practical, statistical and recursive problems. In a literature review and discussion, this paper examines specific problems involved in predicting terrorism. **The problems include the opportunity cost of false positives/false negatives, the statistical quality of the prediction and the self-reinforcing, corrupting recursive effects of predictive analytics, since the method lacks an inner meta-model for its own learning- and pattern-dependent adaptation**. **The conclusion is algorithms don’t work for detecting terrorism and is ineffective, risky and inappropriate, with potentially 100,000 false positives for every real terrorist that the algorithm finds.**

## 

## Risky for resources and past ex have not used PP

Timme Munk, University Illinois at Chicago, "100,000 false positives for every real terrorist: Why anti-terror algorithms don't work | First Monday", August 2017, <https://journals.uic.edu/ojs/index.php/fm/article/view/7126/6522>

The current wave of Islamic terrorism in Europe has a greater political and social platform in ethnic religious extremist environments and among returning volunteers from the Syrian civil war (Bennhold, 2015). The group of possible potential terrorists is therefore large, but the group of actual terrorists small, which makes it difficult to apply the rule of limited police resources optimally. Across Europe, authorities find it difficult to predict and focus correctly on who will become terrorists from the large group of potential terrorists. It involves a necessary prioritization of monitoring and investigations which in some cases have been erroneous. The wrong people have been monitored, and the right people have gone free, simply because the number of potential terrorists is so vast. It is often mentioned after attacks that the now dead terrorists were known by the police but the police found that monitoring, investigating or arresting them was neither necessary nor possible. **This prioritization involves tremendous opportunity costs when you choose not to investigate terrorists due to limited resources and instead choose to investigate innocent people, violating their legal rights and wasting resources.** This is an insoluble practical problem, as the small selected target group versus the total group means more undiscovered terrorists and persecution of innocent people. This is why the extent and use of police resources is a large issue across Europe. Successful prediction and prevention of terrorist attacks often require resource-intensive and time-consuming traditional police work involving interrogations, searches and informants in the extremist environments and digital networks. It is therefore difficult to choose which persons to investigate, and the risk of failure is great. If you look [2] at all public sources on current counter-terrorism efforts, you find that, **in practice, the investigative breakthroughs in the prevention of terrorism reported in the media are entirely due to subject-based data mining** (Bennhold, 2015). The wanted terrorist Abdeslam Salah, who was partly responsible for the Paris attacks in 2015, was arrested because he used a monitored mobile phone. Others involved in the Paris attacks were located based on their relations to **and** contacts with family members (Taub, 2016). Therefore, these investigative breakthroughs **cannot be attributed to the use of predictive analytics**, which is a pattern-based experimental method (DeRosa, 2004; Horgan, 2008; Jensen, 2002; McMorrow, 2009; Schneier, 2006). As mentioned above, the subject-based method is a digital version of traditional police work rather than pattern recognition and prediction based on large amounts of data with an infinite number of possible correlations (DeRosa, 2004). The results of counter-terrorist investigations are therefore consequences of the digitization of the investigations — an efficiency gain — rather than proof that predictive analytics works. The effect of the pattern-recognizing, inductive method is strongly debated and assessed in the literature relationally as an experimental method that can only be used as a complement to other methods (DeRosa, 2004; Hayden, 2016; Jensen, 2002). The challenge is that the inductive method seeks to find emerging patterns in relational and conditional data in infinite dimensions rather than unconditional and unrelated data in finite dimensions, which increases the complexity of and noise in the data material (DeRosa, 2004). The traditional method, based on investigating already convicted or suspected persons (subject-based), limits the complexity and noise dramatically, making it even more efficient (Bouchard, 2015; Chivers, 2003; DeRosa, 2004; Jonas and Harper, 2006; Kaufmann, 2010; Lum, et al., 2008). This underlines the practical problem of finding patterns in complex, open social systems with potentially infinite dimensions for predictive analytics.

# 

# Privacy

## Surveillance bad bc profiling

E.L van Kooten, Tilburg Law School, "Predictive policing; An investigation into the use of the Crime Anticipation System by the Amsterdam police department and the safeguard against discrimination", May 2018, <http://arno.uvt.nl/show.cgi?fid=146478>

Is it possible to use the **Crime Anticipation System** without infringing rights? A framework will be given to see if the use of CAS is possible without infringing rights. The infringements discussed in the previous sub-question will be used for this. A possibility for police to prevent crime is to be present at locations **designated** as **High Impact Crime areas.** This presence will work preventively. When the police are present at those areas, it will probably not violate a citizen’s right per se, but **when they start undertaking action** it might be. **For example, when the police start with body searches, before a crime has occurred, a citizen’s privacy is violated**. Preventive searches can be done in the Netherlands in areas with a security risk and approval of the mayor.12 Will predictive policing make it possible for the police to start using preventive searches to prevent crimes?13 It is difficult to select random people from a flow of people that is larger than the processing capacity. Despite the fact that guidelines are explicitly directed at the random designation of persons, it is still a person who selects someone. This selection is based on the knowledge in his head that automatically starts to look at characteristics that are viewed as an increased risk. 14 A similar thing can occur in traffic controls. Without a suspicion, vehicles can be forced to stop, the driver's driving license may be asked for.15 The so-called rifle judgment16 makes it possible that, if an investigating officer encounters facts and circumstances that involve a reasonable suspicion of a criminal offense, the investigating officer may then apply investigative powers and, for example, can search a vehicle for the suspicion of drug possession. This is not based on an instrument that makes use of objectified knowledge. Furthermore, it is not the intention that biased choices are made, just as with preventive searches. But how random is random? Would it not be much better if the police could use objective criteria in a traffic control that have been tested and determined in advance. Selection based on gut feeling will be avoided.17 This brings a risk of ethnic profiling where skin colour and ethnicity are used as distinctive features to select from a population. It is frequently argued that this is in conflict with the nondiscrimination principle. 18 Unequal treatment based on personal characteristics such as age, religion, race, gender or religion, skin colour or origin is not permitted. The fact that crime is mainly committed by young men does not mean that it is lawful to place the focus on young men in a preventive search. Ethnic minorities, such as non-Western immigrants, are also overrepresented in crime statistics. If you extend this line, you could also question the selective surveillance in deprived neighbourhoods based on information.19 **Furthermore, with the use of big data a lot of data of innocent citizens are also collected.** The privacy of those citizens are less protected because of this under Article 8 of the European Convention of Human Rights (ECHR). There also needs to be looked into the so-called ‘chilling effect’ that predictive policing can have. The chilling effect comes into play when people know that they are watched or think that they might be watched. People will act differently because they are afraid of the potential negative consequences it might have. This chilling effect is mostly connected to the right freedom of speech, but Article 8 ECHR is also applicable in relation to discrimination or stigmatization of certain groups in society.20 Another important issue is the self-fulfilling prophecy. Primarily, the algorithms used for predictions may not take into account the inaccuracies reflected by historical data. In the data that is being used, information can be overrepresented or underrepresented which leads to biased statistics, which can lead to self-fulfilling prophecies. Furthermore, when police is more active at certain areas, there will be more arrests. 21 **Because more and more data is collected about citizens, governments and companies can develop profiles of citizens, divide them into different categories and then treat them differently.** This makes predictive policing mainly a privacy and discrimination issue. “Ethnicity does not play a role in the prediction, because that is ‘a politically incorrect variable’.” Inventor of Crime Anticipation System, Dick Willems As the police states themselves, they cannot profile based on ethnicity and emphasizes, apart from the multiple offenders, not to focus on people, but on tackling specific sorts of crimes.

## 

## Surveillance in Europe bc of PP

Vogiatzoglou, Plixavra. "Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity." European Journal of Law and Technology [Online], 10.1 (2019): n. pag. Web. <http://ejlt.org/article/view/669/901>

Serving this mentality of 'nice-to-have', **practices of mass surveillance increasingly become the most popular means used by both law enforcement and intelligence services in the fight against serious crime.** Interestingly, the defining contour of the concept of mass surveillance is not clear. While this term is being broadly used, it is not subject to a formal definition, but it is mainly linked to a number of characteristics.[21] Most importantly, the individuals subject to mass surveillance are not clearly defined in advance. In particular, mass surveillance is not directed against a specific individual or group of individuals, but it concerns large parts of the population or even the entire population. Furthermore, as opposed to targeted surveillance, which relates to a past crime, mass surveillance in its current dimension may also be used as a pre-emptive measure, aimed at the prevention of future criminal offences and threats to society at large.[22] Mass surveillance, hence, feeds from a pre-crime mentality that "in order for the suspect to emerge, everyone must be subject to surveillance". [23] Therefore, while practices of mass surveillance may serve a multitude of purposes including prevention, detection, investigation and prosecution of serious crime, as will be analysed further on, this paper seeks to focus only on this first purpose of prevention. Furthermore, modern practices of mass surveillance are developing **as the adoption of intelligence-led policing and predictive policing methods by a wide range of security actors ties in with the current phenomenon where massive amounts of data are produced and collected on a daily basis in the hands of the private sector.** Either willingly and intentionally or unconsciously, citizens give away large amounts of their personal data and information to companies that use them towards their own benefit.[24] Consequently, the private sector collects progressively larger amounts of varied data that are able to reveal important information concerning the personal lives and profiles of the individuals, forming a pool of information that the states aspire to dive into. **To that end, private companies are asked to participate in government surveillance through national and European regulatory frameworks that oblige them to collect, store and eventually hand in citizens' personal data to national and third country law enforcement authorities and/or intelligence services. In this way, the practices of mass surveillance in question facilitate** and support intelligence-led policing, including **predictive policing methods**, and the overarching concept of big data analytics, through the vast amplification of security actors' databases. At an EU level, a number of legal instruments establishes the transfers of personal data generated in the sectors of financial and travel information, to security actors both internally amongst Member States and externally to third countries.[25] Financial information contains personal data such as the names of the beneficiary and the ordering customer, while travel information, in this case Passenger Name Records (PNR) data, are the data required by an airline, in order for an airplane ticket to be bought and may include the passenger's full name, date of birth, address, as well as sensitive information, such as details of any special meal requirements. A third and most common category of private entities' bulk collection, retention and ultimately transfer of personal data to security actors for the purposes of mass surveillance, consists of electronic communications data. In particular, data generated or processed in the context of publicly available electronic communications services include both content data and metadata. Content data refer to the content of the communication, for instance a conversation, while metadata refer to technical, temporal and spatial elements, for instance the where, when and amongst who a conversation took place. The latter category of data is now being regulated at national level,[26] after the failed European attempt, which will be further analysed in the following section.[27] Several of these legal instruments regulating mass surveillance practices was placed under the scrutiny of the highest supranational Courts of Europe. This paper, therefore, focuses on the judicial regulation of modern manifestations of mass surveillance, as being carried out through the bulk access of security actors to personal data held by the private sector.

## Lack of legal FW in US allow abuse

Walter L. Perry et al, RAND, "The Role of Crime Forecasting in Law Enforcement Operations", 2013, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf>

Pitfall 4: Underemphasizing assessment and evaluation. During our interviews with practitioners, very few said that they had evaluated the effectiveness of the predictions they produced or the interventions developed in response to their predictions. The effectiveness of any analysis and interventions should be assessed as part of the overall effort to keep the data current. Measurements are key to identifying areas for improvement, modifying interventions, and distributing resources. Pitfall 5: Overlooking civil and privacy rights. The very act of labeling areas and people as worthy of further law enforcement attention inherently raises concerns about civil liberties and privacy rights . Labeling areas as “at-risk” appears to pose fewer problemsbecause, in that case, individuals are not being directly targeted. **The U.S. Supreme Court has ruled that standards for what constitutes reasonable suspicion are relaxed in “high-crime areas” (e.g., hot spots). However, what formally constitutes a “high-crime” area, and what measures may be taken in such areas under “relaxed” reasonable-suspicion rules, is an open question**

## 

## Lack of transparency = public mistrust

**Albert Meijer**, International Journal of Public Administration, "Predictive Policing: Review of Benefits and Drawbacks: International Journal of Public Administration: Vol 42, No 12", **Feb 12 2019**, <https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664>

Next, to the practical **issues** **that** are **accompany**ing the administration of **predictive algorithms**, **more fundamental concerns regarding privacy** and ethics are raised. Edwards and Urquhart (2016) review whether the usage of open source and social media data by law enforcement agencies should be permitted and to what extent the digital identity of citizens is protected. The authors raise the question to what extent the digital footprint of citizens (e.g. what citizens share on social media and the data that can be collected such as our movements with public transport) is private and whether it can be used unconditionally. De Hert and Lammerant (2016) discuss tensions between the profiling of individuals in society and legal safeguards, as these are often loosened to resolve these tensions. Even tough jurisprudence on privacy is very clear in the legal limits of predictive profiling, there remain little cases which makes it hard to set precise boundaries what is eligible. This conclusion is underlined by Costanzo, D’Onofrio, and Friedl (2015), as they argue that legislation is important to retain trust between citizens and governments as there should be a balance between the utilization of big data and the privacy of citizens. **If there are no clear boundaries citizens might develop a profound sense of mistrust towards governments as they are unaware whether, and to what extent, they are monitored** (Inayatullah, 2013; Schlehahn et al., 2015).

## 

## Predictive policing is incompatible with transparency and accountability

Moses and Chan 18

Lyria Bennett Moses and Janet Chan (both are Faculty of Law, UNSW Australia and Data

to Decisions Cooperative Research Centre, Sydney, Australia). “Algorithmic prediction

in policing: assumptions, evaluation, and accountability.” Policing and Society, VOL. 28,

NO. 7, 806–822. 2018.

**Transparency,** defined as ‘availability of information about an actor allowing other actors to monitor the workings and performance of this actor’ (Meijer 2014, p. 511), **is**

**closely related to accountability** (Pasquale 2015, p. 175). If there is comprehensible information as to the circumstances in which data are collected, the circumstances in which data may be altered (including data storage security protocols), the circumstances in which data are matched or combined (including statistical probabilities of incorrect

matches and any systemic bias), the algorithms and processes that are used on the data (the ‘source code’), as well as the assumptions and biases inherent in those, the output in its original form, and any limitations in the process by which any visualisations are rendered, then the person to whom the account is given has a comprehensive understanding of the reasons for any given decision. The decision, including reliance on the software, is then open to evaluation, critique, feedback, and formal sanction where relevant. **However**, for a range of reasons, such **full transparency and comprehensibility is rarely possible in predictive policing.** Software may be subject to commercial-in-confidence provisions in licensing contracts. **Even where the source code is available, there may be emergent properties of the algorithm** (particularly in the case of machine learning) **that cannot be anticipated.** **In addition, the person to whom an account is given may lack the expertise to deduce biases inherent in the choice of algorithm or process of analysis.** Other assumptions discussed above, such as those inherent in processes of data collection, may be poorly understood so that there is little evidence to confirm or counter the assumptions inherent in the process.

## Terrorist justification enables surveillance

Brian Lozada, Abacus, "The Emerging Technology of Predictive Analytics: Implications for Homeland Security", 2014 <http://abacusgroupllc.com/static/pdf/TheEmergingTechnologyofPredictiveAnalytics-BrianLozada.pdf>

Emerging Technologies and Privacy Concerns As emerging technologies have developed in recent years in response to the need for advanced counterterrorism initiatives, the dual responsibility of gathering information to support such initiatives while protecting the civil liberties and legal rights of individuals as a result of increased information access continues to remain a priority. Yet despite privacy concerns, **the trend of extensive data collection to track individuals’ behavior seems to continue to be on the rise. In 2012, U.S. Attorney General Holder signed off on revised rules regarding government data sharing which would allow for the National Counterterrorism Center within the Department of Homeland Security the ability to analyze existing government records collected about citizens for suspicious patterns of behavior concerning domestic terrorist-related threats** (Howard, 2013). According to Howard (2013), this action can be justified for counter-terrorism initiatives, as there are advanced persistent threats; the goal of such data collection and analysis is to find and detect terrorism plots before they occur. However, these rules seem to override the mission of the Federal Privacy Act of 1974 that protected individuals’ civil liberties (Howard, 2013). Therefore, emerging technologies, such as predictive analytics and active intelligence engines, may result in public controversy should the public believe that infringement on personal liberties exceeds the perceived security benefit. In order to continue to maintain the delicate balance between developing new technologies while, at the same time, ensuring the protection of civil liberties, it is necessary that the nation adheres to homeland security policies that were instated to protect such liberties. In addition, it is necessary that all technologies are safeguarded against the potential threat of vulnerability amongst intelligence sources and methods utilized for information sharing to further increase the public’s confidence in counterterrorism measures.

# 

# Feedback Loop

**Danielle Ensign**, Sorelle A. Friedler, Scott Neville, Carlos Scheidegger, and Suresh Venkatasubramanian. **2017**. Runaway Feedback Loops in Predictive Policing. **Cornell** <http://arxiv.org/abs/1706.09847>

“Predictive policing systems are increasingly used to determine how to allocate police across a city in order to best prevent crime. Discovered crime data (e.g., arrest counts) are used to help update the model, and the process is repeated. **Such systems have been empirically shown to be susceptible to runaway feedback loops, where police are repeatedly sent back to the same neighborhoods regardless of the true crime rate.** In response, we develop a mathematical model of predictive policing that proves why this feedback loop occurs, show empirically that this model exhibits such problems, and demonstrate how to change the inputs to a predictive policing system (in a black-box manner) so the runaway feedback loop does not occur, allowing the true crime rate to be learned. Our results are quantitative: we can establish a link (in our model) between the degree to which runaway feedback causes problems and the disparity in crime rates between areas. Moreover, we can also demonstrate the way in which \emph{reported} incidents of crime (those reported by residents) and \emph{discovered} incidents of crime (i.e. those directly observed by police officers dispatched as a result of the predictive policing algorithm) interact: in brief, while reported incidents can attenuate the degree of runaway feedback, they cannot entirely remove it without the interventions we suggest.”

# 

# AT Tech Neutral

Perry et al 13

Walter L. Perry, Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood (Researchers at RAND Corporation). “Predictive Policing: Forecasting Crime for Law Enforcement.” Santa Monica, CA: RAND Corporation, 2013.

<https://www.rand.org/pubs/research_briefs/RB9735.html>.

While predictive policing has much promise and has received much attention, there are myths to be aware of and pitfalls to avoid when adopting these approaches. Many of the myths stem from unrealistic expectations: Predictive policing has been so hyped that the reality cannot match the hyperbole. There are four common myths when it comes to predictive policing:• The computer actually knows the future. Although much news coverage promotes the meme that predictive policing is a ”crystal ball,” the resulting algorithms predict the risk of future events, not actual events. Computers can dramatically simplify the search for patterns, but their predictions will be only as good as the data used to make them. The computer will do everything for you. On the contrary, even with the most complete software suites**, humans must find the relevant data, process these data**

**for analysis, design and conduct analyses** in response to ever-changing crime characteristics, review and interpret analysis findings (and exclude erroneous findings), recommend interventions, **and take action to exploit the findings** and assess the impact of interventions. • You need a high-powered (and expensive) model. In fact, most departments do not need the most sophisticated software packages or computers to launch a predictive policing program. In several of the case studies, simple heuristics were nearly as good as analytic software in performing some tasks for predictive policing. While complex models can offer increased predictive power, there may be diminishing returns. • Predictions automatically lead to major crime reductions. Predictions are just that. Actual decreases in crime require taking action based on predictions. Predictive policing is part of an end-to-end process.

# Predictive Policing includes the implementation

Walter L. Perry et al, RAND, "The Role of Crime Forecasting in Law Enforcement Operations", 2013, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf>

**Making “predictions” is only half of prediction-led policing; the other half is carrying out interventions,** acting on the predictions that lead to reduced crime (or at least solve crimes). What we have found in this study is that predictive policing is best thought of as part of a comprehensive business process.

# 

# Other countries prove PP is bad

## India:

### CRIME IN INDIA WENT UP FOR THE PAST 3 YEARS

National Crime Records Bureau, "Crime in India – 2018", <http://ncrb.gov.in/StatPublications/CII/CII2018/pdfs/CII%202018%20SNAPSHOTS%20STATES.pdf>

A total of **50,74,634 cognizable crimes** comprising 31,32,954 Indian Penal Code (IPC) crimes and 19,41,680 Special & Local Laws (SLL) crimes were registered **in 2018.** Though it shows **an increase of 1.3% in registration of cases over 2017** (50,07,044 cases), however, crime rate per lakh population has come down from 388.6 in 2017 to 383.5 in 2018. [Table –1.1] ii. During 2018, registration of cases under IPC have increased by 2.3% whereas SLL crimes have declined by 0.1% over 2017. [Table – 1.1] iii. Percentage share of IPC was 61.7% while percentage share of SLL cases was 38.3% of total cognizable crimes during 2018.[Table – 1.1]

National Crime Records Bureau, "Crime in India—2017", <http://ncrb.gov.in/StatPublications/CII/CII2017/pdfs/CII2017-Snapshots-State-UT.pdf>

A total of **50,07,044 cognizable crimes** comprising 30,62,579 Indian Penal Code (IPC) crimes and 19,44,465 Special & Local Laws (SLL) crimes were registered **in 2017, showing an increase of 3.6% in registration of cases over 2016** (48,31,515 cases). [Table –1.1] ii. During 2017, registration of cases under IPC have increased by 2.9% and SLL crimes by 4.8% over 2016. [Table – 1.1] iii. Percentage share of IPC was 61.2% while percentage share of SLL cases was 38.8% of total cognizable crimes during 2017.[Table – 1.1]

National Crime Records Bureau, "Crime in India—2016", <http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/9%20%20Snapshots%20All%20India%202016.pdf>

A total of **48,31,515 cognizable crimes** comprising 29,75,711 Indian Penal Code (IPC) crimes and 18,55,804 Special & Local Laws (SLL) crimes were reported **in 2016, showing an increase of 2.6% over 2015** (47,10,676 cases). [Table – 1.1]

## 

### Why CMAPS is really bad

Vidushi Marda and Shivangi Narayan, Association for Computing Machinery, "Data in New Delhi's predictive policing system", January 2020, <https://dl.acm.org/doi/pdf/10.1145/3351095.3372865>

5.1.1Historical bias... While gathering information is an age old practice within policing, from compiling “badmash registers” in colonial India to maintaining a list of criminals by birth to keep track of criminal tribes [27], the act of gathering information has always been a selective one; with greater surveillance often befalling axes of disadvantage, i.e. caste, gender, class, and religious minority. It is not simply a case of more crime occurring in poorer parts of Delhi, or in places where minorities and migrants live - an additional layer of complication is introduced when a human is tasked with choosing which area or under which crime a certain call should be led. **A general apathy towards individuals living in slums, and more forgiving outlooks with respect to individuals living in posh parts of Delhi was apparent from conversations across the Call Centre. This, combined with the fact that policing as an institution has a controversial record around discrimination, brutality, and illegal practices with vulnerable individuals [11] means that historical bias is not only embedded, but actively formalised and introduced into data.** 5.1.2Representation bias... Given that input data for CMAPSconsists of calls to the Dial 100 call centre and a national database used to track crime and criminals, there is a significant underrepresentation of individuals from privileged socio-economic backgrounds, and also of upscale areas in the data. This is because the sampling methods, i.e. **calls to an emergency helpline or existing records in a criminal database (not conviction database) lend themselves more readily to some areas of the city and sections of society.** The DMD receives around 20000 calls a day, and in the course of our research some employees said that people from posh areas “hardly called”, and that an overwhelming majority of these calls were from slums. **This means that the probability of crime will be marked higher in hotspot areas where quantity of engagement is higher, leading to a vicious circle of heightened scrutiny for the most marginalised,** eventually leading to more arrests and reports coming out of these areas. 5.1.3**Measurement bias... Occurs** in DMD and CMAPS for a few reasons. **Given** that **the** spatial distribution of Delhi is less accurate among temporary settlements, and there is **greater nuance in data arising from privileged neighbourhoods in Delhi**, the clusters of information tend to be less quantitatively overwhelming, thus attracting less future scrutiny. This bias arises not just because of systemic blind spots, but also because of vulnerable individuals inability to engage with the system as well as others. For example, we learnt from a call taker that some people do not know their addresses even if they have been living at that place all their lives and an overwhelming majority of such people have always been women. She said women mostly stay inside the house and are not very aware of their surroundings or the exact address (name of mohalla/colony) of their location. In most cases they Wouldnt even know the nearest police station by which the call taker could identify the caller’s address. In such cases the call takers have no choice but to ask callers to call again once they know their address. They encourage them to ask a passerby to tell them about the landmarks of their location, a thana, police chowki or another famous place to get their address. 5.2 Disparate impact, or indirect discrimination Disparate impact refers to a situation where a prima facie neutral policy has a disproportionate and disadvantageous impact on a protected class [1]. Findings from our research indicate that data collection and creation within Delhi Police has a disproportionate impact on historically marginalized and vulnerable groups, which we can logically extend to decision making that is informed by such data [22]. Crimes are more likely to be recorded when they come from organised colonies, with specific details and granular information relating to actual addresses, **whereas crimes from shanty settlements are plotted at the same spot due to lack of accurate information, leading to an imbalance in what is classified as a "hotspot" of crime. There is also widespread selective enforcement and individual officer discretion that works against the interests of these communities.** This in turn leads to over-policing areas inhabited by individuals from vulnerable groups, and also creates a cycle of confirmation bias within an institution that is already embedded with societal, cultural, gender and caste biases [11]. Article 15 of the Indian Constitution prohibits discrimination on the grounds of race, religion, caste, sex, and place of origin. While the status of disparate impact under Article 15 has been the subject of some legal debate [2], the Delhi High Court in 2018 recognised indirect discrimination [10], a.k.a disparate impact, as one that qualifies as discrimination under the Indian Constitution. Reiterating the rationale underlying Article 15, the Court stated that it existed be-cause women and other vulnerable groups, “have been subjected to historic discrimination that makes a classification which disproportionately affects them as a class constitutionally untenable.” Given our findings in this paper, thus, current data practices within the Delhi Police can attract Article 15 of the Indian Constitution. 5.3 Direct discrimination The design of ‘layers’ in CMAPS software can be used to filter immigrant colonies and minority settlement areas, extending from the belief that crime rises due to the de facto existence of these areas, and the people who live in them. The observable variable that is used at the time of analysis and filtering is not merely a proxy for a protected attribute, it is the protected attribute itself, under Article 15(1) of the Indian Constitution. It is also reasonable to state that the use of such infrastructure can attract Article 14of the Indian Constitution, which contemplates the fundamental right to equality and equal protection of laws. According to the Supreme Court of India, “equality” must necessarily be substantive, i.e. must consider whether a provision or executive act “contributes to the subordination of a disadvantaged group of individuals.” [5] The use of opaque technical systems like CMAPS currently afford a veneer of objectivity and shield against scrutiny in the process, but a challenge to this usage is both possible and crucial.

#### 

#### Explanation of CMAPS

Vidushi Marda and Shivangi Narayan, Association for Computing Machinery, "Data in New Delhi's predictive policing system", January 2020, <https://dl.acm.org/doi/pdf/10.1145/3351095.3372865>

**CMAPS was announced in 2015 as a partnership with the Indian Space Research Organisation. Under this partnership, Delhi Police claimed it would use "space technology for effective governance" explaining that CMAPS would be capable of geographic and environment profiling of crime, would rank districts on the basis of crime reported, numbers of people affected, and produce predictive models based on these trends to assist officers to plan and deploy police forces [21]. The input data of this system is from the Dial 100 emergency call centre (the equivalent of 911 in the United States or 999 in the United Kingdom), and from First Information Report (FIR) data stored in the Crime and Criminal Tracking Network Systems (CCTNS) in New Delhi.**

### 

#### Methodology of Study

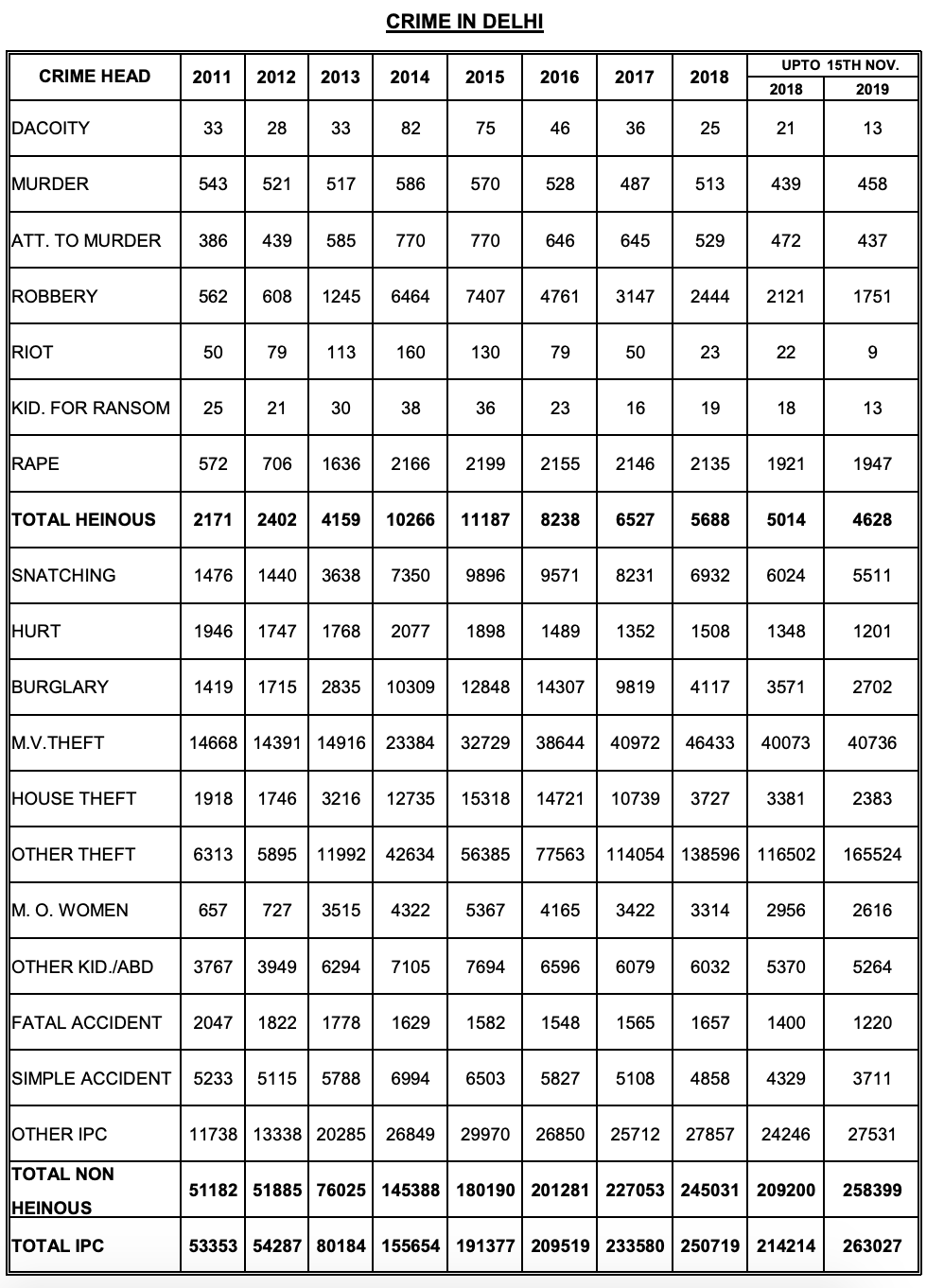
Vidushi Marda and Shivangi Narayan, Association for Computing Machinery, "Data in New Delhi's predictive policing system", January 2020, <https://dl.acm.org/doi/pdf/10.1145/3351095.3372865>

**This paper reports findings from a larger ethnographic study of predictive policing in Delhi conducted over 2 years** **(from February 2017 to March 2019)**. Initially, our research questions centred around the technical systems alone and the way in which they might be aiding decision making within Delhi Police. As we spent more time at the Delhi Police Headquarters (PHQ), our concerns changed in two important ways. First, we realized that the human and institutional actors surrounding CMAPS and the processes that preceded it, substantially informed and influenced its form and use. Second, we learned that the process of data collection and creation within the PHQ was carried out in the absence of explicitly articulated standard operating procedures and auditing mechanisms. Thus, we realized that we first needed to understand the link between individual arbitrariness and institutional standardization in context of CMAPS. That motivated us to specifically conduct an institutional study of the data creation processes within policing in order to understand the eventual impact of CMAPS**. We collected data through marginal and participant observation with Call Takers, including those who handle emergencies, Dispatchers, Digital Mapping Division Map Plotters, and officers in the communications wing.** W**e also conducted unstructured interviews with approximately 20 individuals to uncover the qualitative ways in which value-laden decisions are taken by officers in the PHQ.** Observation and interviews were conducted in parallel. The former helped us understand established processes of data collection and creation, and gave rise to specific questions which we followed up through interviews. We gained access to the PHQ as academic researchers interested in studying the technical turn to policing in India’s capital. During our time there, access to documents related to mapping and predictive policing were limited due to security reasons. Access to the Call Centre and the Dispatch Command Room was considerably tougher than the DMD. We were not allowed to carry notebooks or any recording device inside the Call Centre. However, access to documents displayed publicly on the notice boards of CallCentre, and DMD was provided. To supplement the gaps in our observations and interviews and to verify some information from our interviews, we also led two requests under India’s Right to Information (RTI) Act, to illuminate the extent to which CMAPSis currently used, how the system was designed, developed and audited before deployment, how personnel operating CMAPS are trained and what the parameters of their training are, funding for CMAPS, among others. We received 13 replies to our RTI but given wide exceptions for law enforcement under the RTI Act, and a governance vacuum around the use of technology in the public sector, we were unable to furnish any information through this route. In March 2019, our access to DMD and other processes within DelhiPolice were cut o due to security reason

## 

### Crime in Delhi Went up

National Informatics Centre, "Crime in Delhi", November 15, 2019, <https://www.delhipolice.nic.in/PDF/CID.pdf>



# 

### Muslims are oppressed

Saurav Datta, Catch News, "Delhi Police to go high-tech with predictive policing: Here's why it's a bad idea | Catch

News", Feb 10, 2017, <http://www.catchnews.com/india-news/delhi-police-to-go-high-tech-with-predictive-policing-here-s-why-it-s-a-bad-idea-1467027497.html>

An article in Columbia Journalism Review alleges that a predictive policing model leads to what is commonly termed as the 'machine bias'. "Algorithms can be especially susceptible to perpetuating bias for two reasons. First, algorithms can encode human bias, whether intentionally or otherwise. This happens by using historical data or classifiers that reflect bias (such as labeling gay households separately, etc.). This is especially true for machine-learning algorithms that learn from users' input," says the article titled Investigating the Algorithms that Govern our Lives. **Especially in India, given the enforced ghettoisation of Indian Muslims and communalisation of police and paramilitary forces, this system can potentially derail criminal justice**. One only has to visit certain localities like Juhapura in Ahmedabad, Mohammad Ali Road in Mumbai and Mumbra in its suburbs, or Calcutta's Topsia, Tiljala and Metiabruz localities to gauge the extent of the problem. When the chances of 'calculated' bias is both perpetrated and perpetuated, very little remains of justice and, civil liberties and democratic rights. ISSUES UP CLOSE Based entirely upon computer algorithms which have no concern for either human differences nor racial and ethnic sensibilities, the COMPAS, on which CMAPS is based on, tries to map out if more crimes are going to be committed in a certain area as compared to another. For example: COMPAS tries to predict if more crimes will be committed n in New York's Bronx or in the Harlem area. The algorithms study previous crime rates, based on mainly quantitative, not qualitative statistics, and thereafter enables what experts call 'crime forecasting'. Two studies by the RAND Corporation, Evaluation of the Shreveport Predictive Policing Experiment and Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations provides an insight into how correlation and not causation can affect criminal justice. According to these reports, statistics are, more often than not, misleading unless a lot more data is available. While almost all police departments that have used predictive policing admit that it definitely is an optimisation of resources, in certain cases it has helped improve community relations, but it is at the end of the day a prediction that isolates one area/person as being more prone to crime than another. According to Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, 'the operational value of predictive policing tools is in their contribution to broader law enforcement strategies that use the tools' risk assessments to inform resource allocation and problem-solving decisions.' 'To be effective, predictive policing must include interventions based on analytical findings. Successful interventions typically have top-level support, sufficient resources, automated systems providing needed information, and assigned personnel with both the freedom to resolve crime problems and accountability for doing so,' the report adds. But in the case of India, chances are that these interventions, or more in-depth data simply might not exist. THE INDIAN ISSUE The 2002 Steven Spielberg movie Minority Report showed a Pre-Crime Captain from a Special Police Unit, armed with the 'smartest' tech to apprehend future murderers, turning into a murder accused because of a statistical analysis gone awry. When we are dealing with computer predictions, especially in the case of crime, there are chances that wrong areas and wrong people might be brought under scrutiny because of pre-conceived notions and socio-religious biases. **For India, besides the obvious machine bias, the minority bias will also be affecting the computer algorithms. With the heightened fear of 'terror attacks' and the vague (and legally indefensible) definition of 'radicalisation' (as applied to Muslims), the adoption of predictive policing methods may well have a crushing effect on civil liberties and democratic rights of Indian citizens**. Truth, and nothing but the whole truth, as determined and conclusively established by law, should form the basis of criminal justice and not algorithm-based suspicions. Especially in a country reeling under the effects of Hindu majoritarianism where members of a particular minority community are more likely to be falsely implicated in criminal cases.

## China:

<https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region#>

(New York) – **Chinese authorities are building and deploying a predictive policing program based on big data analysis in Xinjiang, Human Rights Watch said today.** The program aggregates data about people – often without their knowledge – and flags those it deems potentially threatening to officials. According to interviewees,some of those targeted are detained and sent to extralegal “political education centers” where they are held indefinitely without charge or trial, and can be subject to abuse. “For the first time, we are able to demonstrate that the Chinese government’s use of big data and predictive policing not only blatantly violates privacy rights, but also enables officials to arbitrarily detain people,” said Maya Wang, senior China researcher at Human Rights Watch. “People in Xinjiang can’t resist or challenge the increasingly intrusive scrutiny of their daily lives because most don’t even know about this ‘black box’ program or how it works.” **Human Rights Watch said Xinjiang authorities in recent years have increased mass surveillance measures across the region, augmenting existing tactics with the latest technologies. Since around April 2016, Human Rights Watch estimates, Xinjiang authorities have sent tens of thousands of Uyghurs and other ethnic minorities to “political education centers.”**

## Australia:

Johnny Lieu, Mashable, "Australian police use a secret algorithm and blacklist to target children suspected of future offending", October 26, 2017, <https://mashable.com/2017/10/26/children-predictive-policing-australia/>

**A new report by the Youth Justice Coalition examined the use of New South Wales Police's Suspect Targeting Management Plan (STMP),** which is being used to mark people as young as 11. The STMP is a risk-assessment tool and a policing program used to prevent future crimes by focusing on repeat offenders, or those suspected to potentially commit one. For a person to be entered into the STMP, they need to be nominated by police. A "targeting team" assesses the nomination, based on intelligence around suspected or historical criminal activity, or other information. The system uses an algorithm to calculate how likely a person is going to offend, and classes them into the categories of extreme risk, high risk, medium risk, or low risk. Just what criteria on what makes a person fit into these categories, or makes them nominees for the STMP, is not publicly available. **Those entered into the STMP "experience a pattern of constant harassment" by police, despite some having minor, non-violent convictions, or no convictions but frequent contact with law enforcemen**t. What's concerning, however, is that the **STMP is skewed towards young people, Indigenous Australians (44 percent of STMP nominees), and is being used by police as a substitute for having "reasonable grounds to suspect" a person has committed an offence.** In one case study, police records justified the stop and search of a 16-year-old boy, because "young people who get on the last carriage of a train and wear Nautica are known to commit criminal damages (graffiti)."

## 

# 

# LA Predictive Policing Bad

Beryl Lipton, MuckRock, "Eight years in, LAPD can’t measure PredPol’s effect on crime • MuckRock", March 2019, <https://www.muckrock.com/news/archives/2019/mar/12/algorithms-lapd-predpol/>

The Los Angeles Police Department, an early adopter of data-driven policing, needs tougher standards for data collection, recordkeeping, and communicating its policies to the public to guard against targeting minorities and certain neighborhoods, a new report from the department’s inspector general said. The 48-page report from the office of **Inspector General Mark Smith**, issued on March 8, **said data tracked by the department is inadequate for determining the impact of specific programs on crime.** The report, reviewed on March 12 by the Board of Police Commissioners, examined databases, software, and crime statistics used in three specific programs. It found that data on **“dosage,” the time an officer spends in an area deemed to be of interest, was too vague.** One critic of the LAPD’s predictive policing systems said that the report itself fell short by not accounting for the harm to targeted individuals and their communities from the department’s targeted policing practices and policies. Over the past decade, LAPD has used several predictive policing systems, combining strategies that target individuals and locations. In 2009, the department began development of the L.A. Strategic Extraction and Restoration (LASER) Program, using nearly $1 million in grants from the federal Bureau of Justice Assistance, designed to identify for removal particular “high risk” individuals. Two years later, it began to employ the predictive policing software PredPol, which uses historical data to create daily reports on anticipated crime “hotspots.” And the agency recently began testing ELUCD, a platform to survey community sentiment. The IG’s report specifically reviewed LASER, PredPol, and ELUCD, noting use of a platform developed by data analytics firm Palantir to streamline information used in both the LASER and PredPol programs. The 9000-member department has had a long history of controversy in which local groups have questioned its ability to overcome bias in policing. Stop LAPD Spying Coalition released a report in May 2018 critical of the department’s predictive policing and asked the inspector general’s office to conduct its own review. At a special July 2018 police commissioners meeting on data-driven policing, representatives from the American Civil Liberties Union of Southern California, **Stop LAPD Spying Coalition, and the community testified in opposition to the department’s use of predictive technology - including the audited programs, automated license plate readers and video recording systems - to drive decision making and to identify individuals for warrantless surveillance.** The five-member commission, following a request from Stop LAPD Spying Coalition, asked in August 2018 that the IG examine the agency’s existing data-informed strategies. The IG report offered new information about the department’s use of technology, noting that in August the department had suspended use of the LASER system. Jamie Garcia, a Stop LAPD organizer, told MuckRock that the program’s suspension was news to her and had been done without public notice. However, the temporary suspension, she said, will not enable the department to compensate for its shortcomings. **“This isn’t a new program that just got started and it’s going to have some bumps,”** Garcia told MuckRock. **“This is a program that has been in effect for 10 years.** This is 10 years of people’s lives that they have been screwing with. **The LASER program relied on the identification of “Chronic Offenders” to be monitored for removal from the community. It also highlighted areas, referred to as “LASER Zones” or “hotspot corridors,” for increased officer attention.** According to the report, the department is working to revise the program and plans to continue using it. Garcia was also disappointed that the report included no mention of the community request for the investigation or the human and civil rights impact these programs have had, and instead ignored potential victims of the program and the activists who have worked to bring to light problems. Stop LAPD released a response to the audit in which they call on the LAPD to “stop legitimizing harmful predictive policing programs by attempting to ‘reform’ them.” LAPD has been employing PredPol since 2011. The software intends to help police departments target high-risk crime zones and is used by an estimated 50 police departments. However, activists and academics throughout the country, such as the ACLU, are worried that the reliance on old data generated by previous LAPD policing or arrest patterns will perpetuate existing biases in deployment of officers and investigative resources. The department has begun to rethink some of its predictive policing methods, the IG report said. “[S]ome of the proposed changes for a revised offender-based program include more narrowly constraining the selection process, incorporating disclosure and appeal processes, and developing a centralized oversight component,” the report said. “The Department also expects to implement additional technology to assist in more accurately tracking data related to officers’ activities in the field, including those related to data-driven policing strategies.” The LAPD did not provide comment by publication time. **Garcia, however, believes any reform that cannot properly address concerns that LASER, PredPol, or other predictive systems are inherently unjust. “To even think about bringing something back that violates human rights, to me, is completely, completely unacceptable,” Garcia said. “How do you even talk about bringing back a program that has unjustly targeted and stalked people?”**

# 

# Police stopped using PP

## Palo Alto and Mountain View

Mark Puente, LA Times, "LAPD pioneered predicting crime with data. Many police don’t think it works - Los Angeles Times", July 2019, <https://www.latimes.com/local/lanow/la-me-lapd-precision-policing-data-20190703-story.html>

The Los Angeles Police Department took a revolutionary leap in 2010 when it became one of the first to employ data technology and information about past crimes to predict future unlawful activity. Other departments around the nation soon adopted predictive policing techniques. But the widely hailed tool the LAPD helped create has come under fire in the last 18 months, with **numerous departments dumping the software because it did not help them reduce crime and essentially provided information already being gathered by officers patrolling the streets. After three years, “we didn’t find it effective,” Palo Alto police spokeswoman Janine De la Vega said. “We didn’t get any value out of it. It didn’t help us solve crime.”** **The Mountain View, Calif., Police Department** spent more than $60,000 on the program between 2013 and 2018. “We tested the software and eventually subscribed to the service for a few years, but ultimately the results were mixed and we **discontinued the service in June 2018,”** spokeswoman Katie Nelson said in a statement. The program was designed to predict where and when crimes were likely to occur over the next 12 hours.

# Drug laws that affected PP

## Crack vs powder example

<https://issues.org/the-effects-of-mass-incarceration-on-communities-of-color/>

Although the United States has made some progress, it remains a substantially racially segregated nation residentially. And, the country stays very economically segregated as well. It is not surprising that poor people of color have been incarcerated disproportionately during the massive increase in imprisonment that has occurred in the nation since the early 1980s. **It is from poor communities of color that a very large number of felons are removed, and to these same neighborhoods that they return when their sentences end.** **This population churning has been called “coercive mobility” by criminologists**. Although it is the intent of legislatures, judges, police, and prosecutors to protect citizens and communities, there is reason to believe that coercive mobility has the unintended consequence of actually increasing crime and victimization. Some of the changes during this period of increased incarceration that disadvantaged people of color coming into the justice system were implemented with the help and support of African American political leadership, with the express purpose of protecting black and brown communities. **Perhaps the best example of this is the initial federal sentences for crack cocaine offenses: conviction for crack selling (more heavily sold and used by people of color) resulting in a sentence 100 times more severe than for selling the same amount of powder cocaine (more heavily sold and used by whites).**

## Marijuana

Kade Crockford (Director, Technology for Liberty Project, ACLU of Massachusetts).

“What’s Predictive Policing?” Privacy SOS. 2011. JDN. <https://privacysos.org/predictive/>

As Ronald Bailey wrote for Reason, “The accuracy of predictive policing programs depends on the accuracy of the information they are fed.” Many crimes aren’t reported at

all, and when it comes to the drug war, we know for certain that police don’t enforce the law equally. Take marijuana arrests as an example. **We know that black people and Latinos are arrested, prosecuted and convicted for marijuana offenses at rates astronomically higher than their white counterparts, even if we adjust for income and geography. We also know that whites smoke marijuana at about the same rate as blacks and Latinos.** Therefore we know that marijuana laws are not applied equally across the board: Blacks and Latinos are disproportionately targeted for associated arrests, while whites are arrested at much lower rates for smoking or selling small amounts of marijuana. Now consider that these arrest data are put into computer programs instructed to spit out

information to officers about where to target police patrols — what’s called predictive policing. The returned intelligence telling police departments where to target their patrols is supposedly accurate because arrest data fed into a computer algorithm produced it. But if historical arrest data shows that the majority of arrests for marijuana crimes in a city are made in a predominately black area, instead of in a predominately white area, predictive policing algorithms working off of this problematic data will recommend that officers deploy resources to the predominately black area — even if there is other information to show that people in the white area violate marijuana laws at about the same rate as their black counterparts. If an algorithm is only fed unjust arrest data, it will simply repeat the injustice by advising the police to send yet more officers to patrol the black area. In that way, predictive policing creates a feedback loop of injustice.

# 

# AT: Nola 4 life

## Unsustainable

Jonathan Bullington, Nola, "Cantrell should replace failing NOLA for Life, her transition group says | Local Politics | nola.com", May 4, 2018, <https://www.nola.com/news/politics/article_09e3fc1b-eba0-5a88-8a09-5b5dd01aa23d.html>

"NOLA for Life's success in 2013 and 2014 showed that City policy could indeed drive down gun violence in New Orleans, yet **the program's lack of sustainable results is evidence that a different model is needed**," wrote the transition team's subcommittee on violence reduction strategies.

## Opaque

Ali Winston, The Verge, "Palantir has secretly been using New Orleans to test its predictive policing technology - The Verge", Feb 27, 2018, <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>

Predictive policing technology has proven highly controversial wherever it is implemented, but in New Orleans, **the program escaped public notice, partly because Palantir established it as a philanthropic relationship with the city through Mayor Mitch Landrieu’s signature NOLA For Life program.** Thanks to its philanthropic status, as well as New Orleans’ “strong mayor” model of government, the agreement never passed through a public procurement process. In fact, key city council members and attorneys contacted by The Verge had no idea that the city had any sort of relationship with Palantir, nor were they aware that Palantir used its program in New Orleans to market its services to another law enforcement agency for a multimillion-dollar contract. Even James Carville, the political operative instrumental in bringing about Palantir’s collaboration with NOPD, said that the program was not public knowledge. “No one in New Orleans even knows about this, to my knowledge,” Carville said.

# 

# NYC Murder Rate up

Anna Hopkins, Fox, "Murder rate rises 55 percent in New York City, NYPD statistics say | Fox News", Feb 21, 2019, <https://www.foxnews.com/us/murder-rate-rises-55-in-new-york-city>

**Murder rates in New York City are up 55 percent in 2019** compared to the same time frame in 2018, according to NYPD statistics. From the start of 2019 through Sunday, there have been 48 murders in New York City, compared to 31 in the same seven-week time frame in 2018, the New York Daily News reported.

# AT Deterrence (Baltimore)

Thompson, Maxfield, Analyzing the Efficacy of Predictive Policing in Law Enforcement (May 1, 2016). <http://dx.doi.org/10.2139/ssrn.2891544>

These paroling officers were sent to high visibility spots within the various hot spots. The visibility of the police alone helped reduce crime, however; **police soon realized the crime was being displaced to other places in the city.** When this shift occurred, the CCP was seen as going into phase two (Perry 72). **Phase two consisted of a more aggressive policing strategy the high risk areas.** Now instead of scaring off crime, the Baltimore police shifted their focus to catching criminals. **During this activation period, total stops were greatly increased in the high risk zones.**

# Heat List

Andrew Ferguson, Time, "Police Are Using Algorithms to Tell Them If You're a Threat | Time", October 3, 2017, <https://time.com/4966125/police-departments-algorithms-chicago/>

In Chicago, Illinois, an algorithm rates every person arrested with a numerical threat score from 1 to 500-plus. **The process has been going on for four years, and almost 400,000 Chicago citizens now have an official police risk score**. **This algorithm — still secret and publicly unaccountable — shapes policing strategy, the use of force, and threatens to alter suspicion on the streets.** It is also the future of big data policing in America — and depending on how you see it, either an innovative approach to violence reduction or a terrifying example of data-driven social control. **In practical effect, the personalized threat score automatically displays on police computer dashboards so an officer can know the relative risk of the suspect being stopped. The predictive score also shapes who gets targeted for proactive police intervention.** These interventions can range from a home visit by police officers, to additional police surveillance, to an invitation to a community meeting — all of which convey the same clear message: law enforcement is watching. And while Chicago is in the vanguard of predictive policing, it is not alone; other cities like New York and Los Angeles are considering how to use big data policing to target at-risk individuals. Person-based predictive policing began in 2009 as an attempt to apply a public health approach to violence. Just as epidemiological patterns reveal environmental toxins that can increase health risks (like getting cancer), criminal patterns can increase life risks (like getting shot). The key is to identify the predictive risk factors and try to remedy the underlying environmental causes. Researchers at Chicago ITT developed an algorithm for the police to prioritize those most at risk by analyzing: past arrests for violent crime, weapons offenses or narcotics; age at the most recent arrest (the younger the age, the higher the score); incidents where the individual was a victim of a shooting or assault; and the trend line of criminal activity (whether the rate is increasing or decreasing). A computer then crunches the variables and spits out a relative threat score to determine a likelihood of either shooting someone or getting shot. This is the risk score that places someone on the Strategic Subjects List (colloquially known as “the heat list”). Police claim the targeting mechanism works by pointing to a high percentage of shooting victims as being accurately predicted by the heat list. **Critics have pointed out that the targeting is overbroad and ineffective, including tens of thousands of people with high scores but no history of prior arrest for violent crimes.** But, whether it works or not, three bigger unanswered questions exist about this use of a predictive risk score for everyone: Is it fair? Is it biased? And is it the future we want for policing? Fairness involves both how people get scored and how police treat those with threat scores. Relying on a black-box computer algorithm to rank threats in a society obviously creates its own risks. Society needs to be able to trust the data, to approve the inputs and to evaluate the outputs. **Currently, there is no public oversight of the police data, inputs or outputs, so communities are left in the dark unable to audit or challenge any individual threat score. Equally troubling, the threat scores impact the fairness of how police interact with people on the streets.** High-risk scores guide violence-interruption strategies, influencing who police contact and who falls under their heightened surveillance. But the threat scores also distort the day-to-day police decisions about use of force and reasonable suspicion. After all, once police have information that a person has a high threat score**, this knowledge will color criminal suspicion and increase perceived danger, resulting in more frequent and more aggressive interactions with people the algorithm deems “high risk.”**

**Explanation of China’s policy**

Alexandra Ma, Business Insider, "How IJOP works, China surveillance app to monitor oppressed Muslims - Business Insider", May 11, 2019, <https://www.businessinsider.com/how-ijop-works-china-surveillance-app-for-muslim-uighurs-2019-5>

Officials in Xinjiang, China's most oppressed region, **use** **an** **intrusive**, all-seeing **smartphone app to monitor, track, and flag citizens for investigation or punishment.** A new report gives a glimpse into how it works, and allows the Chinese state **a vast array of** deeply personal **information** on its oppressed citizens, **like** their **blood type**, **how much gas they use,** **and whether they are on birth control.** Xinjiang has in recent years come under an unprecedented amount of scrutiny because of the country's crackdown on the Uighurs, a majority-Muslim ethnic minority concentrated there. Uighurs often refers to the region as East Turkestan. Officials in the region have installed hundreds of thousands of facial recognition cameras, **forced Uighurs to download software that would crawl their phone**s, and held at least 1 million Muslims in prison-like detention centers**. Beijing justifies its crackdown by calling Uighurs a national-security threat, and has routinely tried to stoke Islamophobia to justify its controversial policies in the region. Authorities** are also required to use a mobile app to log citizens' personal data, track citizens' activity, and flag "dangerous" individuals for investigation or punishment, Human Rights Watch (HRW) said in a report published last week. The app is connected to the Integrated Joint Operations Platform (IJOP) — a centralized data system that stores data about all of Xinjiang's residents. HRW researchers were able to crack into it by reverse-engineering its source code. Here's how the app works. Hoovering up whereabouts, blood types, and birth control methods The app asks Xinjiang authorities to grill citizens and log via their phones an array of information, including their height, blood type, and vehicle registration number, HRW reported. It also asks officials to glean intrusive personal information from citizens, including political views, whether they communicate with relatives abroad, and even their use of birth control, the researchers said. **Many Uighurs have been disappeared and detained for bizarre reasons, including setting clocks to a different time zone** than Beijing's, **wearing veils,** **and** **communicating with people who have gone abroad.** Xinjiang authorities currently have the right to stop any Uighur citizens in the region, question them, search their phones, and detain them if necessary.

# 

# LAPD Faking data → PP promotes malpractice

Mark Puente and Richard Winton. “LAPD's Data-Driven Culture under Scrutiny amid Scandal over Fake Gang Identifications.” *Los Angeles Times*, Los Angeles Times, 21 Jan. 2020, [www.latimes.com/california/story/2020-01-21/lapd-measured-the-number-of-gang-members-its-metro-officers-interviewed](http://www.latimes.com/california/story/2020-01-21/lapd-measured-the-number-of-gang-members-its-metro-officers-interviewed).

**The Los Angeles Police Department** has long been at the forefront of using data to help fight crime, even pioneering a program that uses statistics to predict where criminal activity is likely to occur. But now, that data-driven culture **is under scrutiny in the wake of a scandal in which 20 officers are unde**r investigation followin**g accusations of falsifying field interview cards to label individuals as gang members in an effort to boost statistics and populate a statewide gang database. The Times obtained a Metro Division platoon recap sheet, which shows that officers were measured daily in 16 categories** such as guns, citations and arrests. **Field interviews of gang members were among the categories used to measure productivity.** A source familiar with the internal investigation said that **Metro’s work emphasized guns and gangs and that its officers felt pressure to produce statistics in a results-driven departmen**t. The source spoke to The Times anonymously because the case is ongoing. **Los Angeles police officials said the recap sheets are one tool used to evaluate officers but stressed that such pressures were not an excuse to engage in misconduct.** “It doesn’t give someone the right to make it up,” LAPD spokesman Josh Rubenstein said. “It is one measure of productivity we look at. It is not the end-all, be-all. It is one of many.” Data analysis has become a central tool used by police departments to better target resources and to monitor officer conduct. Some experts — and even some community groups — have praised the tactic for helping understand crime patterns and also providing red flags to potential bias and ineffective policing. At the LAPD, station captains are grilled by higher-ups at weekly meetings about how to reduce crime, and crime statistics for each station are updated online every few weeks.

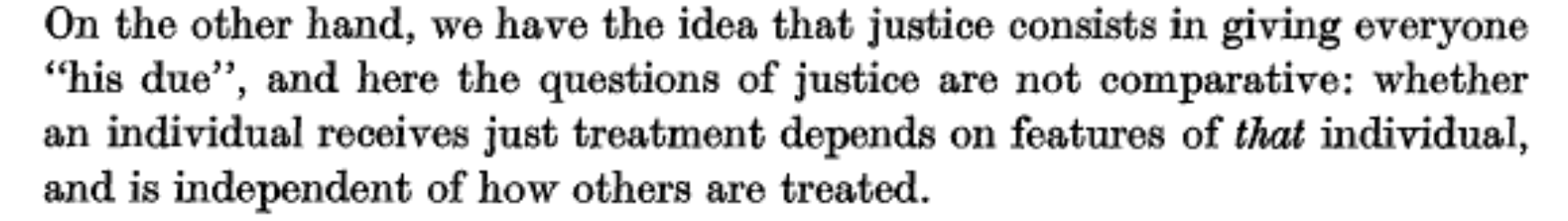
## Definition of PP

ACLU, "What's Predictive Policing? | Privacy SOS", March 21, 2019, <https://privacysos.org/predictive/>

**Predictive policing, with roots in business analytics, relies on using advanced technological tools and data analysis to take proactive measures to “pre-empt” crime.**

## Justice Definition

Montague, Phillip. “Comparative and Non-Comparative Justice.” *The Philosophical Quarterly (1950-)*, vol. 30, no. 119, 1980, pp. 131–140. *JSTOR*, [www.jstor.org/stable/2219277](http://www.jstor.org/stable/2219277)



## Structural Violence Definition

Adam Burtle, "structural violence | Structural Violence", 2010-2013, <http://www.structuralviolence.org/structural-violence/>

**Structural violence refers to systematic ways in which social structures harm or otherwise disadvantage individuals.**

* <https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist>
* <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/chicago-police-heat-list-renews-old-fears-about>
* <https://www.latimes.com/opinion/editorials/la-ed-lapd-predictive-policing-20190316-story.html>
* <https://thenextweb.com/artificial-intelligence/2019/02/21/predictive-policing-is-a-scam-that-perpetuates-systemic-bias/>
* <https://www.aclu.org/blog/criminal-law-reform/reforming-police/predictive-policing-software-more-accurate-predicting>
* <https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf>
* Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine Bias. ProPublica, May 23, 2016.

<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [accessed July 21, 2018].

<https://www.vice.com/en_us/article/ezp8zp/minority-retort-why-oakland-police-turned-down-predictive-policing>