# POLICING BY MACHINE

LIBERTY

# POLICING BY MACHINE

I.IBERTY

JANUARY 2019

# POLICING BY MACHINE

## PREDICTIVE POLICING AND THE THREAT TO OUR RIGHTS

**Author: Hannah Couchman**

Contributing researcher: Alessandra Prezepiorski Lemos


# CONTENTS


# EXECUTIVE SUMMARY

# EXECUTIVE SUMMARY

Police forces across the UK are using predictive policing programs to predict where and when crime will happen – and even who will commit it.

These opaque computer programs use algorithms to analyse hordes of biased police data, identifying patterns and embedding an approach to policing which relies on discriminatory profiling. An algorithm is a list of rules that a computer will follow to solve a certain problem – but they also "learn" and become more autonomous when making predictions, without having to be programmed.

Predictive policing programs entrench pre-existing inequalities while being disguised as cost-effective innovations in a time of austerity – and their use puts our rights at risk.

***Policing by machine*** focuses on two types of predictive policing program: (1) predictive mapping programs and (2) individual risk assessment programs.

## Predictive mapping programs

Predictive mapping programs evaluate police data about past crimes and identify "hot spots" or boxes of high risk on a map. Police officers are then directed to patrol these areas – which are often communities already experiencing "over-policing" (i.e. they are subject to policing interventions which are disproportionate to the level of crime in that area).

Like any data collected from society, the data used to drive predictive policing programs will be reflective of pre-existing patterns of





discrimination: *"to the extent that society contains inequality, exclusion or other traces of discrimination, so too will the data"*.[1] For example, people from black, Asian and minority ethnic (BAME) communities are disproportionately more likely to be arrested[2], leading the program to assume, wrongly, that the areas in which they live or spend time are the areas where there is more crime.[3]

One of the leading commercial predictive mapping programs is made by PredPol, a company based in the United States.[4] PredPol previously provided its program to Kent Police,[5] where it was used for five years before the force decided to look to develop an internal version of the program or purchase one at lower cost.

A wide range of private companies offer alternative predictive mapping programs – these include HunchLab, IBM, Microsoft, Hitachi, and Palantir. It is unlikely that police forces deploying these commercially available products will have access to, or an understanding of, how the programs work – the algorithms they rely on are considered trade secrets.

## Individual risk assessment programs

Individual risk assessment programs predict how people will behave, including whether they are likely to commit, or even be victims of, certain crimes.

For example, Durham Police have used a program called the Harm

1 *Goodman et al, 2016, European Union regulations on algorithmic decision-making and a "right to explanation", AI Magazine 38, Available at https://arxiv.org/abs/1606.08813 [Accessed November 2018]*

2 *GOV.UK Ethnicity Facts and Figures, 2017, Arrests 2016/17, Available at: https://www.ethnicity-facts-figures. service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest [Accessed November 2018]*

3 *In 2017, the percentage of defendants convicted out of all those prosecuted was lowest for Black and Mixed ethnic groups. See: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/courts-sentencing-and-tribunals/prosecutions-and-convictions/latest [Accessed January 2019]*

4 *See: www.PredPol.com*

5 *See page 53 for more information on Kent's use of PredPol*

Assessment Risk Tool (HART). The program uses machine learning to decide how likely a person is to commit an offence over the next two years. The program gives the person a risk "score" of low, medium or high, and is designed to over-estimate the risk that they pose.[6]

The program bases its prediction on 34 pieces of data, 29 of which relate to the person's past criminal history. The other pieces of data include personal characteristics such as postcode, which act as "proxies for race" by indirectly indicating a person's ethnicity and fuelling the same biases. This is why research on algorithms used in the criminal justice system in the United States showed that, even where race was not included in the data the algorithm used, the algorithm still learned characteristics in a way that is discriminatory[7] – because other pieces of data it did use correlated with race and led to inadvertent profiling by the algorithm.[8]

In April 2018, it was revealed that police data which was fed into the HART program was supplemented by an Experian[9] dataset called "Mosaic", produced through profiling each of the 50 million adults in the UK.[10] Mosaic profiles and classifies people into spurious groups – for example, a *"crowded kaleidoscope"* is a low-income, *"multi-cultural"* family working *"jobs with high turnover"* and living in *"cramped houses"* or *"overcrowded flats"*.[11] Mosaic even links

6 *Oswald et al, 2018, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality, Information & Communications Technology Law, Volume 27, 2018, pages 228-230, Available at: https://ssrn.com/abstract=3029345 [Accessed November 2016]*

7 *Ibid*

8 *Question 11, Science and Technology Committee Oral evidence: Algorithms in decision-making, HC 351, 14 November 2017*

9 *Experian is a consumer reporting agency. Consumer reporting agencies are companies that collect and sell personal information on consumers that is used to decide whether to provide consumers credit, insurance, medical care, housing, banking services, utilities, and employment.*

10 *Big Brother Watch, 2018, Police use Experian Marketing Data for AI Custody Decisions [Press release], 6 April, Available at: https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions [Accessed: November 2018]*

11 *Ibid*





names to stereotypes: for example, people called Stacey are likely to fall under *"families with needs"* who receive "*a range of benefits"*. According to Mosaic, Terrence and Denise are *"low income workers"* who have *"few qualifications"* and are *"heavy TV viewers"*.[12] Running this data through individual risk assessment programs inevitably encourages a discriminatory and offensive association between factors such as family circumstances, income, class and the propensity to commit crime.

Currently, HART is used to assess whether a person is eligible to be diverted to a rehabilitation program and avoid a formal court process.[13] This alone is a significant decision, and there is potential for these programs to be used in a much wider range of circumstances within the criminal justice sector.

Other police forces are developing similar capabilities. For example, Avon and Somerset Police use predictive policing programs for an extraordinary array of risk assessment activities – to decide a person's likelihood of being a victim of crime, experiencing a vulnerability or being reported missing, as well as their likelihood of perpetrating or being a victim of domestic violence or a sexual offence.[14]

Another trial of predictive policing, carried out by West Midlands police, "*combined data on crimes, custody, gangs and criminal records to identify 200 offenders who were getting others into a life on the wrong side of the law"*.[15]

In this report we highlight the ways in which our rights are fundamentally undermined by the use of predictive policing programs – programs which, far from being neutral, incorporate

12 *Ibid*

13 *People who are scored as "medium risk" are eligible to participate in the program, called "Checkpoint"*

14 *See page 46 for Avon and Somerset's response to Liberty's FOIA request on individual risk assessment programs*

15 *Beckford, 23 December 2018, 'Minority Report' police computer is being used to 'predict' who is likely to commit crimes amid ethical concerns over £48million project, the Mail on Sunday, Available at: https://www.dailymail.co.uk/news/article-6523997/Minority-Report-police-computer-predict-likely-commit-crimes.html [Accessed January 2019]*

human biases, exacerbate social inequalities and threaten our privacy and freedom of expression.

We also outline the results of 90 Freedom of Information Act (FOIA) requests[16] sent by Liberty to every police force in the UK to gain insight into these troubling practices. They reveal that 14 police forces have already rolled out predictive policing technologies or are planning to do so, without proper consideration of our rights and the discriminatory impact these technologies can have.

## Discrimination

Although predictive policing is simply reproducing and magnifying the same patterns of discrimination that policing has historically reflected, filtering this decision-making process through complex software that few people understand lends unwarranted legitimacy to biased policing strategies that disproportionately focus on BAME and lower income communities. Use of algorithms can and should be examined for the ways in which they can remove bias – but until the police demand and use fully tested programs that embed this by design, we should completely reassess the role algorithms play in policing.

The use of predictive policing by police forces also ignores what communities really want from their local police and undermines policing aims. Focusing on abstract data, isolated from its human context, is at the expense of building proper community trust and understanding. This is particularly important in relation to over-policed communities.

16 *Members of the public are entitled to request information from public authorities under the Freedom of Information Act 2000. For more information on this process, see: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/*





## Big data, privacy and freedom of expression

Predictive policing programs encourage reliance on “big data” – the enormous quantities of personal information accumulated about us in the digital age. A culture of big data allows the state to monitor us even more closely and build up intrusive profiles from thousands of pieces of information. This chills our freedom of expression, making us feel we are being watched and forcing us to self-censor.

The ability to control what information is made available about us is integral to our lives. But a dangerous emerging narrative requires us to justify our desire for privacy, rather than requiring that the state – including the police – provide a sound legal basis for the interference.

## Human oversight

Requiring human oversight or intervention alongside such programs is not sufficient to meet the concerns highlighted in this report. The challenges in ensuring police officers don’t defer to the algorithm, known as "automation bias”, are so significant that they cannot be met in the short term by training or guidelines.

Enabling humans to work alongside algorithms requires in-depth and long-term research, analysis and testing – and there is no evidence, as yet, that automation bias can be sufficiently mitigated. As such, it is time to ask questions about whether these technologies have any place in our police forces.

## Transparency

Predictive policing programs are often referred to as “black boxes”, because they are so opaque – we can’t understand how they come to their decisions, and what role each piece of data

plays in the program's decision-making process. This means we can't hold the programs to account, or properly challenge the predictions they make about us or our communities. This is exacerbated by the fact that the police are not open about when they are using these programs.

## Conclusion

The disturbing consequences of relying on predictive policing programs go beyond increased profiling and include the inefficient use of police resources and deepening divisions between the police and local communities. These divisions can even lead to an increase in crime.[17]

While it may seem that predictive policing programs can discover new and useful trends in offending behaviour, many will simply restate pre-existing patterns of exclusion and inequality. Predictive policing programs are not offering a new insight into crime with greater utility for public safety – instead, they lead to a cycle of self-fulfilling prophecies that unfairly target over-policed communities and undermine community relations with the police.

From deciding if someone is likely to reoffend, through to which areas or neighbourhoods should be most frequently patrolled by police, these decisions are too important to hand over to a machine – and the risks to our civil liberties are too great. Any policing approach which relies on a combination of predictions, profiling and the idea of "pre-criminality" puts our rights are risk. In a democracy that should value policing by consent, it's time to draw some red lines about how we want our communities to be policed.

17 *Brennan 2018, Weapon-Carrying and the Reduction of Violent Harm, British Journal of Criminology, Available at: https://doi.org/10.1093/bjc/azy032 [Accessed November 2018]*





# RECOMMENDATIONS

Liberty opposes suspicion driven by big data and "data predictions", which feeds an opaque decision-making environment and risks putting discriminatory practices further out of view.

We recommend the following:

1. Police forces in the UK should end their use of predictive policing "mapping" programs, which rely on problematic historical arrest data and encourage the over-policing of marginalised communities.
2. Police forces in the UK should end their use of predictive policing "individual risk assessment" programs, which encourage discriminatory profiling and result in opaque decision-making that cannot be adequately overseen by police officers or effectively challenged by the people impacted by these decisions.
3. At the very least, and with a view to ending the use of these programs, police forces in the UK should fully disclose information about the use of predictive policing programs within their force. Where decision-making is informed by predictive policing programs or algorithms, this information needs to be communicated to those directly impacted by their use, and the public at large, in a transparent and accessible way.
4. Investment in digital solutions for policing should focus on the development of programs and algorithms that actively reduce biased approaches to policing, work towards addressing the issues outlined in this report and

are accompanied by concrete steps to address wider and underlying issues of bias that permeate the criminal justice system. The development and trial of any such programs should be overseen by independent experts, and the evaluation of trials should be conducted entirely independently, with the results made public. A human rights impact assessment should be developed in relation to the use of any new digital solutions, and this must also be made available to the public.

5. Police forces should examine more widely their use of data, to include a full review of the Gangs Matrix and similar databases. Police forces must, at the very least, introduce guidance requiring that police databases such as the Gangs Matrix set out targeted criteria for inclusion and removal, outline a process for challenging a person's inclusion, explain the sources used to populate the database, and establish safeguards to prevent discriminatory use of data. Similarly, and in line with commitments to an independent review into the "Prevent" strategy,[18] the police should review the way in which they hold and use data obtained under the "Prevent" scheme.

18 *See, for example: Liberty, 2018, Briefing on the Counter-Terrorism and Border Security Bill for Second Reading in the House of Lords, Available at https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20the%20Counter-Terrorism%20and%20Border%20Security%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Lords.pdf [Accessed Janaury 2019]*

# BIASED MACHINES

# BIASED MACHINES

Many uses of predictive policing compound the crisis of unfair treatment of marginalised communities. What's more, their use provides a front of allegedly "impartial" statistical evidence, putting a neutral technological veneer on pre-existing discriminatory policing practices.

Under the Human Rights Act, public authorities like the police must not discriminate against people when acting in a way which affects their human rights. Such discrimination includes – but is not limited to – sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or any other status.

There is a real risk that, when it comes to biased predictive policing tools, our rights to privacy, freedom of expression and even liberty and fair trial will not be evenly fulfilled. For example, BAME or low income communities are more likely to be unfairly targeted or assessed by a predictive policing program, and so are more likely to feel the need to self-censor.

## Bias and predictive mapping programs

Using historical crime data to make predictions is deeply problematic because the data collated by the police does not present an accurate picture of crime committed in a particular area – it simply presents a picture of how police responded to crime. For example, there will be crimes that were not reported to the police, for a wide range of reasons including a lack of confidence,[19] mistrust and fear. There

19 *For example, in 2018 and the four years prior, a smaller percentage of Black Caribbean people had confidence in their local police compared with White British people. See: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/confidence-in-the-local-police/latest*





will also be incidents that were reported but not followed up by the police, or areas where the police have been patrolling regularly and are therefore likely to encounter more offences.

Furthermore, arrest statistics could show that a particular number of people have been arrested in a certain area, but being arrested does not indicate that someone is guilty of an offence. In 2016/17, black people were over three times more likely to be arrested than white people, and people with a mixed ethnic background were over two times more likely to be arrested than white people, but without a corresponding rate of conviction.[20] In 2009, the Home Affairs Select Committee reported on developments since the Stephen Lawrence inquiry and noted that BAME people remain *"over-policed and under-protected within our criminal justice system."* [21]

As such, many predictive policing programs are better at predicting likely police involvement in a certain community – not potential crime. One study suggests that predictive mapping programs merely spark a "feedback loop" that leads to officers being repeatedly sent to certain neighbourhoods – typically ones with a higher percentage of residents who are BAME or on low income – regardless of the true crime rate in that area.[22] If an officer is sent to a neighbourhood and then makes an arrest, the software takes this as indicating a good chance of more crimes being committed in that area in future.

20 *See: GOV.UK Ethnicity Facts and Figures, 2017, Arrests 2016/17, Available at: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest [Accessed November 2018] In 2017, the percentage of defendants convicted out of all those prosecuted was lowest for Black and Mixed ethnic groups. See: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest [Accessed January 2019]*

21 *Home Affairs Select Committee, 2009, The Macpherson Report - Ten Years On, session 2008–09, Available at https://publications.parliament.uk/pa/cm200809/cmselect/cmhaff/427/427.pdf [Accessed November 2018] - The Macpherson Report, published on 24 February 1999, found that the police investigation into Stephen's murder was "marred by a combination of professional incompetence, institutional racism and a failure of leadership by senior officers. While the inquiry focused on the Metropolitan Police Service (MPS), the report concluded that "institutional racism affects the MPS, and police services elsewhere."*

22 *Ensign et al, 2017, Runaway feedback loops in predictive policing, Available at https://arxiv.org/abs/1706.09847 [Accessed November 2018]*

In 2016 researchers from the Human Rights Data Analysis Group released a landmark study that reconstructed and applied a predictive policing program to Oakland, California in the United States.[23] This study focused on the local police department's record of drug crimes from 2010.[24] They found that the system would have sent police officers *"almost exclusively to lower income, minority neighbourhoods"* [25] even though public health-based estimates suggested that drug use was widespread across the city. If these predictions had been used in active deployment, police would have patrolled areas where they were exacerbating pre-existing policing bias relating to both race and income.

The research noted that increased scrutiny and surveillance resulting from the disproportionate patrolling of historically over-policed communities had been linked to worsening mental and physical health.[26] This is corroborated by other studies, which show that living in areas where pedestrian stops are more likely to become invasive is associated with worse health,[27] and that reports of trauma and anxiety from young men in New York City increased as the frequency of police contact rose, especially among those reporting intrusive and/or unfair police stops.[28] The increased police contact also created additional opportunities for police violence in over-policed areas.[29]

23 *Lum et al, 2016, To predict and serve?, Significance Magazine, Available at: https://rss.onlinelibrary.wiley.com/doi/abs/10.1111/j.1740-9713.2016.00960.x [Accessed November 2018]*

24 *Ibid*

25 *Ferguson, 2017, The Truth About Predictive Policing and Race, Available at: https://medium.com/in-justice-today/the-truth-about-predictive-policing-and-race-b87cf7c070b1 [Accessed November 2018]*

26 *Lum et al, 2016, To predict and serve?, Significance Magazine. Available at: https://rss.onlinelibrary.wiley.com/doi/abs/10.1111/j.1740-9713.2016.00960.x [Accessed November 2018]*

27 *See, for example: Sewell et al, 20106, Collateral damage: The health effects of invasive police encounters in New York City, Journal of Urban Health 93, Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4824697/ [Accessed November 2018]*

28 *Geller et al, 2014, Aggressive policing and the mental health of young urban men, Am J Public Health, Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4232139/ [Accessed December 2018]*

29 *Sewell et al, 2016, Collateral damage: The health effects of invasive police encounters in New York City, Journal of Urban Health 93, Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4824697/ [Accessed November 2018]*





Worryingly, the 2014 manual provided by mapping program PredPol[30] boasts that the PredPol program is comparable to the "broken windows" policing strategy, which saw stringent targeting of low-level crime based on the theory that visible signs of crime, anti-social behaviour and civil disorder create an environment that encourages further crime and disorder, including serious crimes. This strategy therefore encourages policing methods that target minor crimes such as vandalism and fare evasion to, in theory, create an atmosphere of order and lawfulness. The widely criticised strategy, now accepted as ineffective, was notorious for leading to the over-policing of BAME communities.[31] Kent Police have previously used PredPol technology – and other police forces use similar programs or have developed their own internal models. More information about which police forces are using mapping programs is included later in this report.

While human decision making in the criminal justice system is also intrinsically biased, the nature of decision making by machines means there is no option to challenge the process, or hold the system to account. Liberty strongly supports widespread calls for underlying issues of discrimination in the criminal justice system to be addressed, including an emphasis on unconscious bias training for criminal justice professionals – but the introduction of opaque decision-making algorithms is a completely inappropriate solution to human bias and fails to address the underlying, systemic issues.

30 *PredPol, 2014, Best Practices and Training Guide, Available at: https://www.muckrock.com/foi/elgin-7770/foia-elgin-police-dept-predpol-documents-51858/?utm_content=buffer6144c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#file-190432 [Accessed November 2018] Ibid, page 13*

31 *See: Harcourt et al, 2005, Broken Windows: New Evidence from New York City and a Five-City Social Experiment, University of Chicago Public Law & Legal Theory Working, Paper No. 93 Available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2473&context=journal_articles [Accessed November 2018]*

**Recommendation One:** Police forces in the UK should end their use of predictive policing "mapping" programs, which rely on problematic historical arrest data and encourage the over-policing of marginalised communities.

## Bias and individual risk assessment programs

There is also significant potential for discrimination in the use of individual risk assessment programs. A United States study conducted by ProPublica into the "COMPAS" risk assessment program found significant racial disparities in the way the program predicted risks of reoffending.[32]

The program incorrectly labelled black defendants as likely to commit further crimes at twice the rate of white defendants. Conversely, white defendants were mislabelled as low risk more often than black defendants.[33] While the software did not use race as an explicit category for risk scoring, it deployed a range of "proxies for race", such as neighbourhood and socio-economic measures, that disproportionately impacted on black defendants.

When conducting their research, ProPublica ran a test on the data that isolated the effect of race from criminal history and reoffending, as well as from defendants' age and gender.[34] Black defendants were still 77 per cent more likely to be labelled as at higher risk of committing a future violent crime and 45 per cent more likely to be predicted to commit a future crime of any kind.[35] This means that the disparity could not be explained by a defendant's prior crimes, or the type of crimes they were arrested for.

32 *Angwin et al, 2016, Machine Bias, ProPublica, Available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, [Accessed November 2018]*
33 *Ibid*
34 *Ibid*
35 *Ibid*





Northpointe, the company that produced the COMPAS program, disputed ProPublica's analysis, but declined to share its own calculations on the basis that these were a trade secret[36] – further demonstrating the lack of transparency that characterises these systems. However, Northpointe did disclose the fact that its formula included factors such as education levels and employment status, among the 137 questions that are either answered by defendants or taken from criminal records – data which may well be correlated to race.[37] The fact that this data was considered by the program at all suggests that factors such as level of education influenced the machine's assessment, entrenching prejudices in determining risk.

In the UK, the first academic review of Durham's HART program noted that postcode data could be related to *"community deprivation"*. If postcode data is relied upon for building future models of reoffending, then it could draw more attention to these neighbourhoods. These problems can be replicated in other individual risk assessment programs – you can read more about which police forces use these technologies later in this report.

While new technologies are often misconstrued – or even misrepresented – as objective, there are clearly real risks of biased and unfair decisions. This draws on and compounds wider issues of disproportionality across the criminal justice system. David Lammy MP, who led a review into the treatment of, and outcomes for, BAME people in the criminal justice system in 2016/17, found that: *"BAME individuals still face bias – including overt*

36 *Ibid*
37 *Ibid*

*discrimination – in parts of our justice system, which treats ethnic minorities more harshly than white [people].”*[38] For example, black people are eight times more likely to be stopped and searched by the police.[39]

This issue isn’t just about technology and algorithms – it goes much deeper to police strategy and the bias which permeates the criminal justice system in its entirety.

38 *Bowcott, 19 December 2017, Government accepts call to tackle racial bias in justice system, The Guardian,Available at: https://www.theguardian.com/uk-news/2017/dec/19/london-prosecutions-could-be-dropped-or-delayed-in-pilot-scheme [Accessed January 2019]*

39 *Home Office Policing Statistics, 2018, Stop and Search. Available at: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest [Accessed January 2019]*

# OUR PRIVACY UNDER THREAT

# OUR PRIVACY UNDER THREAT

Under Article 8 of the European Convention on Human Rights ("ECHR") – brought into our domestic law by the Human Rights Act 1998 – we have a right to respect for our privacy, which means we should be free from intrusion into our personal life – including unnecessary, heavy-handed state surveillance. Our right to privacy can only be interfered with when it is necessary and proportionate to do so in a democratic society.

There is a clear conflict between the state's drive to make use of an enormous range of data for policing purposes and our individual privacy and identity. The level of data required to operate algorithms presents a real risk to our privacy.

As the state amasses more and more information about us, we become more vulnerable to surveillance and profiling, as well as inappropriate or inaccurate determinations about who we are and what we are likely to say, do and even think. An approach to policing which suggests that all data can be relevant in assessing criminality casts the net of surveillance even wider.

There are an enormous number of reasonable and entirely legal reasons to keep information private – and choosing what we disclose is one of the key ways we express ourselves as humans. The desire to control what information is made available about us is integral to our lives.





But there is a dangerous emerging narrative that requires us to justify our desire for privacy, rather than requiring that the state provides a sound legal basis for the infringement.

Rather than looking to establish good practices around data minimisation, the police continue to collect enormous quantities of data and combine it with other datasets.  The use of commercial data by Durham police's aforementioned HART program, which profiles groups of people by ethnicity or spurious and offensive categorisations, demonstrates this risk. Other policing programs use similar, deeply intrusive personal data to make predictions.[40]

Collating and combining data on such significant swathes of the population allows for profiling and monitoring on an unprecedented scale, and places us all under suspicion and surveillance.

40 *See "Use of predictive policing programs in the UK, from page 43*


# THE CHILLING EFFECT

# THE CHILLING EFFECT

Our right to free speech, along with the right to form and join associations or groups, means that we're free to hold opinions and ideas and share them with others without the state interfering. These rights are protected by Article 10 and Article 11 ECHR.

This is a fundamental part of our democracy, and allows us to keep our government accountable and transparent. Information and ideas also help to inform our opinions and political debate. Our right to form and join associations or groups means that we can gather with other people and use public spaces to make our views known, and this includes our right to protest.

As with our right to privacy, these rights can be limited, including to protect the interests of others, but only where this is proportionate and necessary in a democratic society.

Predictive policing programs, along with the associated use of data and increased surveillance, have the potential to interfere with these rights.

As we normalise predictive policing, we may begin to self-police to avoid unwarranted suspicion. We may become afraid of the level of data being gathered about us, what it is used for, how it is shared and what predictions might be made about us as a result – and this may have a chilling effect on what we choose to say, where we choose to go and who we choose to associate with.





The data utilised by these programs may draw upon many variables over which we have no control – such as local area offending rates, convictions in our family – and then lead to significant consequences for our life and liberty. This is another form of guilt by association.

Studies have shown that people censor what they post on social media or what they look up online when they are aware they are being surveilled by the state.[41] The research showed that women and young people were more likely to self-censor as a result of surveillance.[42]

As reliance on data increases, information relating to innocuous actions could be combined and analysed to detect trends which in some way indicate an alleged propensity to commit crime.

Making connections between data points, like where someone lives and who they associate with, to predict whether they will commit a crime will again have a chilling effect – and one that will be most keenly felt by over-policed communities.

41 *Stoycheff, 2016, Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring, Journalism & Mass Communication Quarterly, Available at https://journals.sagepub.com/doi/pdf/10.1177/1077699016630255 [Accessed January 2019] and Penny, 2016, Chilling Effects: Online Surveillance and Wikipedia Use, Berkeley Technology Law Journal, Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645## [Accessed January 2019]*

42 *Ibid*


HUMAN v MACHINE
REGIONLT7:Criminal DatabaseTP:AA4152540186
Print Preview
Clear Markers
LT/TP Analysis
Transaction Queue
DELL

# HUMAN v MACHINE

Police forces generally claim that humans have oversight of predictive policing programs and are charged with making final decisions. While the idea of having human involvement or oversight of an algorithmic decision-making process may sound reassuring, there is a lack of evidence as to our ability as humans to provide meaningful intervention over algorithms and decisions made by machines.

Section 49 of the Data Protection Act 2018 states that individuals must not be subjected to solely automated decision-making in a law enforcement context – but this protection does not go far enough. For example, decision making as to the risk posed by a person detained in police custody may not be fully automated (or so the police will claim), but the role of the human officer may be extremely limited, and the potential impact of the decision significant.

Relatedly, it is difficult to assess the degree to which a human has really made a decision – how do we separate out what is a genuine assessment on the part of a police officer or criminal justice professional and what is simply down to the output of the algorithm?

In the United States, programs such as the aforementioned COMPAS risk assessment system calculate a score that predicts the likelihood of an individual committing a future crime. Even though the final decision is formally made by a judge, the automated decision made by a program can be decisive, especially if judges rely on it exclusively or have not received warnings about the risks of doing so (such as inaccuracy, discrimination and unfair decisions).[43]

43 *Citron, 2016, (Un)Fairness of Risk Scores in Criminal Sentencing, Forbes13, Available at: https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/#146a-7f514ad2, [Accessed November 2018]*





In sectors where use of algorithmic decision making is well-established, such as the aviation industry, the risk of "automation bias" – humans simply deferring to the machine – is accepted as significant.[44] Automation bias means that a human decision-maker may disregard or fail to search for contradictory information in light of a computer-generated solution, which is simply accepted as correct.

Humans in high-risk situations may feel that they should not question the indecipherable recommendation of the algorithm. A police officer may be hesitant to overrule an algorithm which indicates that someone is high risk, just in case that person goes on to commit a crime and responsibility for this falls to them – they simply fear getting it wrong. It is incredibly difficult to design a process of human reasoning that can meaningfully run alongside a deeply complex mathematical process.

One inspector attached to Avon and Somerset Police commented in relation to their use of predictive policing[45] that *"there are still some people in the organisation who believe it is the be-all-and-end-all and professional judgement isn't quite as important. So there will be people who say...that is what we must do"*.[46] They went on to say that *"[If] we do something with person B and we don't do something with person A and then person A the goes on to kill someone or seriously injure them, where is the defenceability [sic] around that? So I can understand people's thinking in that sense, I really can"*.[47]

44 *See: Cummings, 2004, Automation bias in intelligent time critical decision support systems, Paper presented to the American Institute for Aeronautics and Astronautics First Intelligent Systems Technical Conference, Reston, VA, Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.91.2634 [Accessed November 2018]. See also: Parasuraman et al, 2010, Complacency and Bias in Human Use of Automation: An Attentional Integration, The Journal of the Human Factors and Ergonomics Society 52, Available at https://www.researchgate.net/publication/47792928_Complacency_and_Bias_in_Human_Use_of_Automation_An_Attentional_Integration [Accessed November 2018].*

45 *See "Avon and Somerset" section in "Current Use in the UK"*

46 *Dencik et al, 2018, Data Scores as Governance: Investigating uses of citizen scoring in public services, Available at: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report.pdf [Accessed December 2018]*

47 *Ibid*

Research by the Data Justice Lab noted that, in the context of Avon and Somerset's use of algorithms, *"the onus then falls on the frontline staff to record or explain any decision they make that might be at odds with what the system is telling them"*.[48] A policing coordinator commented that *"you can become too dependent on technology sometimes."* [49]

There is therefore a risk that police officers or criminal justice professionals – either consciously or unconsciously – will abdicate responsibility for significant decisions to the algorithm. We have seen this pattern of behaviour elsewhere in the public sector where algorithms are deployed. Philip Alston, the United Nations Special Rapporteur[50] on extreme poverty and human rights, has said of the Department of Work and Pensions (DWP): *"Because the default position of DWP is to give the automated system the benefit of the doubt, claimants often have to wait for weeks to get paid the proper amount, even when they have written proof that the system was wrong. An old-fashioned pay slip is deemed irrelevant when the information on the computer is different"*.[51]

He added that *"the presumption of innocence is turned on its head when everyone applying for a benefit is screened for potential wrongdoing in a system of total surveillance. And in the absence of transparency about the existence and workings of automated systems, the rights to contest an adverse decision, and to seek a meaningful remedy, are illusory."* [52]

48 *Ibid*
49 *Ibid*
50 *Special Rapporteurs are independent experts appointed by the UN Human Rights Council with the mandate to monitor, advise and publicly report on human rights situations, either in specific countries or worldwide.*
51 *Alston, 2018, Statement on Visit to the United Kingdom, United Nations Special Rapporteur on extreme poverty and human rights, Available at: https://www.ohchr.org/Documents/Issues/Poverty/EOM_GB_16Nov2018.pdf [Accessed November 2018]*
52 *Ibid*





This chimes with our concern that police officers will defer to the machine in contexts where they should be providing human oversight and overriding the algorithm based on other evidence.

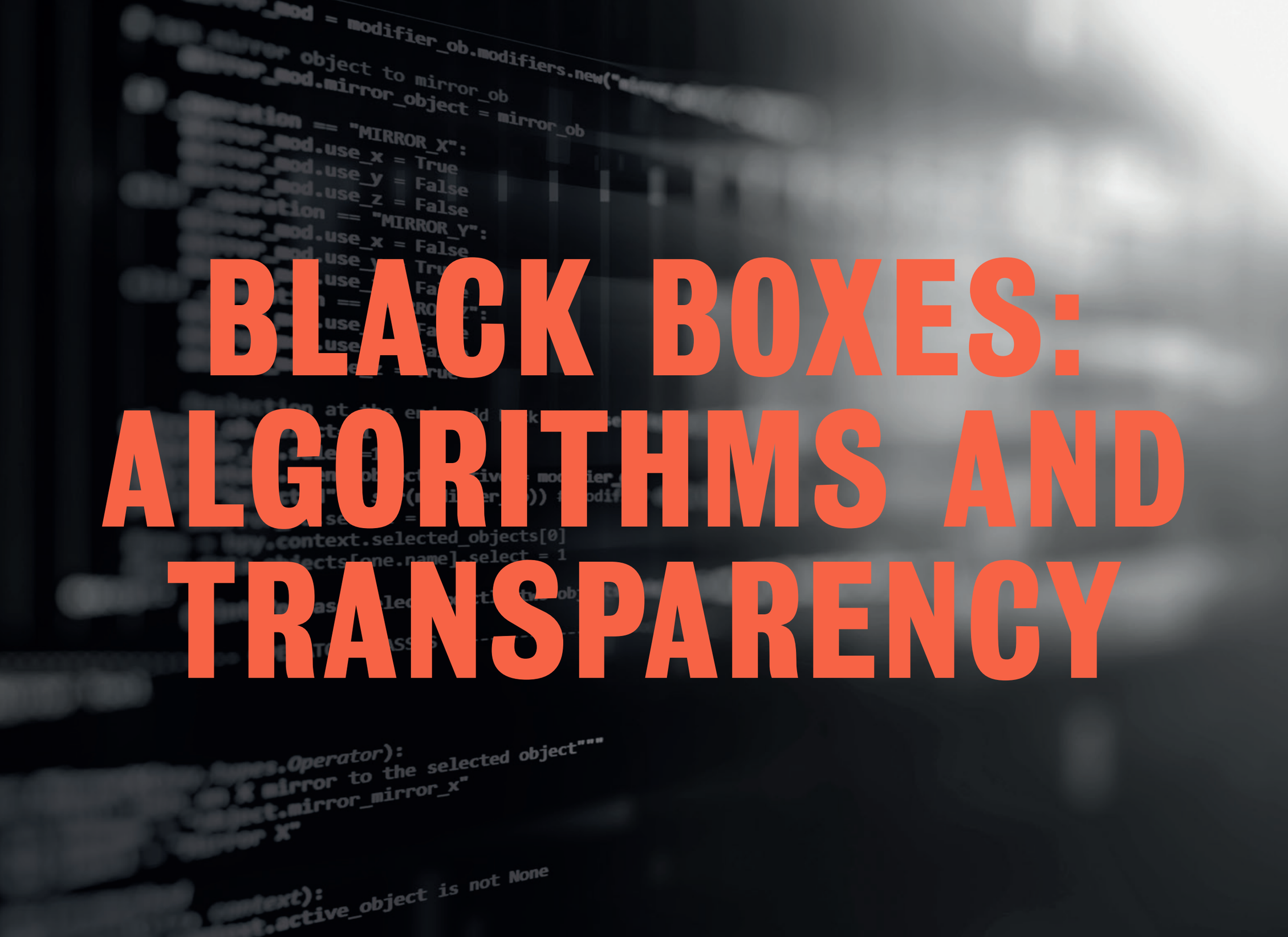
This is particularly important given that research on Durham's HART program showed a *"clear difference of opinion between human and algorithmic forecasts"*.[53] During initial trials of the algorithm, members of the police force were asked to mimic its outcomes by predicting whether a person would be of a low, moderate or high risk of reoffending. The model and the officers agreed only 56.2 per cent of the time.[54]

As use of these algorithmic processes becomes normalised, and as the technology develops and provides quicker and easier answers to complex policing questions, there is evidence that police officers may even become deskilled and less able to make those decisions themselves – making it even less likely that they will override the judgement of the computer.[55]

It is unacceptable for policing decisions which have a significant impact on people's lives – such as who will be able to avoid formal prosecution in court or which communities will be more heavily policed – to simply be handed over to machines.

**Recommendation Two:** Police forces in the UK should end their use of predictive policing "individual risk assessment" programs, which encourage discriminatory profiling and result in opaque decision-making that cannot be adequately overseen by police officers or effectively challenged by the people impacted by these decisions.

53 *Oswald et al, 2018, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality, Information & Communications Technology Law, Volume 27, 2018, pages 228-230, Available at: https://ssrn.com/abstract=3029345 [Accessed November 2018]*
54 *Ibid*
55 *Hildebrandt, 2017, Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics. University of Toronto Law Journal 68, Available at: https://ssrn.com/abstract=2983045 [Accessed November 2018]*


BLACK BOXES:
ALGORITHMS AND
TRANSPARENCY

# BLACK BOXES: ALGORITHMS AND TRANSPARENCY

Using predictive policing programs to allocate police attention or make decisions about people who have been detained by the police will shift accountability from human decision makers to computers. While police officers should be expected to justify why they have made a certain decision, and have their reasoning open to scrutiny and challenge, there is a much more complex process at play when a predictive policing program has been used.

Any sort of policing intervention amounts to an interference with our rights – it must not be arbitrary. Predictive policing methods, as compared with other policing interventions, are not sufficiently transparent and accountable to meet this standard.

Where a police officer or criminal justice professional makes a decision about someone who has been detained in police custody (for example, a decision as to whether to grant them bail), it's possible for the detained person, or their lawyer, to ask questions and make representations to the officer. This is nearly impossible when faced with the recommendation of a computer algorithm. While we may be able to question the officer overseeing the algorithm, the officer themselves may not understand the algorithm or feel accountable for the decision.

Another example might be around patrolling decisions. Where a police officer makes a decision to pay particular attention to a





specific area, the local community can ask questions and hold them to account for their strategy. When the decision has been made by a predictive policing program, this open dialogue and debate is very difficult.

In many cases where black box technologies are deployed, even the police officers involved in operating the programs won't have any insight into how the algorithm works. In fact, the private companies that develop these programs may refuse to reveal the algorithm used because it is a trade secret.[56]

In any case, algorithms will often use machine learning to change and adapt as they attempt to predict outcomes – without having to be programmed by a human. For instance, an algorithm will learn to correlate a number of different factors with a particular output – but the developers may not know what factors are given what weight.

When Liberty submitted FOIA requests to police forces across the UK, some refused to answer questions[57] about their use of algorithms. There is a serious risk that the public will face impossible barriers to holding their police forces accountable.

Some police forces avoid commercial products and develop their own predictive policing programs internally. In these circumstances, it is likely that the force itself will have a greater degree of insight into how the program works, but there is little external transparency as to how these programs are developed, and understanding of how they work among front line police officers will still be low.

56 *This raises an important question as to whether public authorities should be required to include appropriate information about the use of algorithmic decision-making tools in order to encourage such information to be provided publicly and proactively – and set expectations for the private companies that provide these programs. See: Brauneis and Goodman, 2017, Algorithmic Transparency for the Smart City, Yale Journal of Law & Technology 103, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3012499 [Accessed November 2018]*

57 *See, for example, Avon and Somerset and Northamptonshire in the "Current Use in the UK" section below.*

Even for the most well-informed computer programmers, algorithmic decision making can be difficult to decipher – so simply having access to the algorithm used does not mean there will be a greater degree of transparency. Explaining how this data is then used and how the algorithm works remain incredibly difficult questions.

If no one can explain how a decision about you has been made, it is impossible to challenge it properly. The House of Lords Select Committee on Artificial Intelligence concluded that *"achieving full technical transparency is difficult, and possibly even impossible, for certain kinds of AI [artificial intelligence] systems in use today... We believe it is not acceptable to deploy any artificial intelligence system which could have a substantial impact on an individual's life, unless it can generate a full and satisfactory explanation for the decisions it will take."* [58]

This is a significant problem given that, where the state infringes on a person's rights, there needs to be a legal basis for that infringement. This is to protect people from being treated differently based on arbitrary or illogical factors such as where they live. Police practices may fall foul of this essential standard as a result of the use of predictive policing programs.

Durham Police have attempted to get around this lack of transparency by creating a framework for when algorithmic assessment tools should be used by police. Called ALGO-CARE, the model requires – among other things – that algorithms be lawful, accurate, challengeable, responsible and explainable.[59] However, it

58 *Ibid*

59 *Oswald and Urwin, 2018, Written evidence submitted to the House of Lords Select Committee on Artificial Intelligence, Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69002.html [Accessed November 2018]*



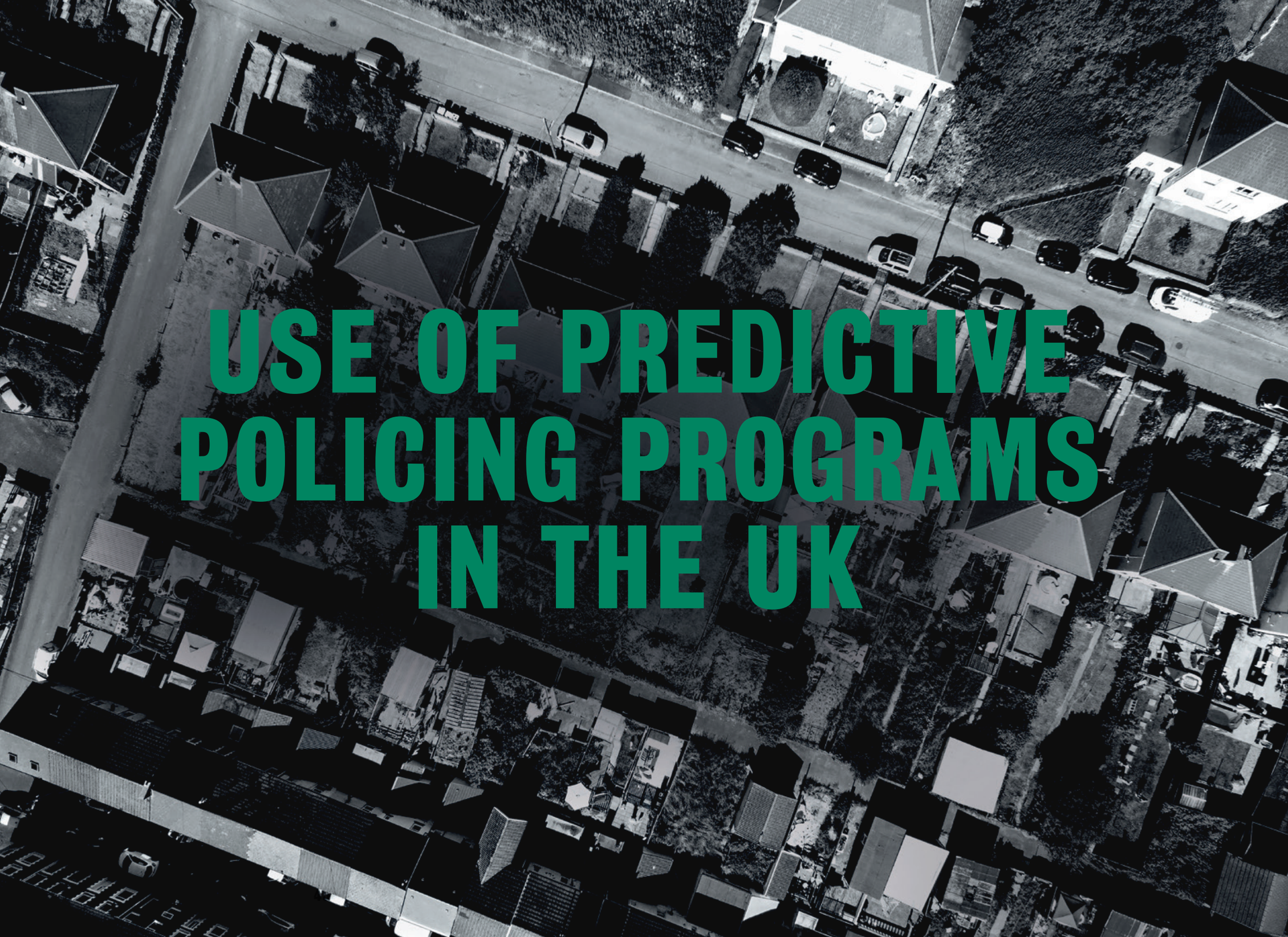


has been argued that *"accountability can never just be a checklist"* and, while police forces might develop frameworks for these programs, they should also consider whether it is appropriate to use these algorithms in the first place.[60] Using frameworks such as ALGO-CARE will not render the HART tool explainable – because even the highly skilled technologists behind the development of the algorithm will struggle to fully articulate how it works to a lay person.

**Recommendation Three:** At the very least, and with a view to ending the use of these programs, police forces in the UK should fully disclose information about the use of predictive policing programs within their force. Where decision-making is informed by predictive policing programs or algorithms, this information needs to be communicated to those directly impacted by their use, and the public at large, in a transparent and accessible way.

**Recommendation Four:** Investment in digital solutions for policing should focus on the development of programs and algorithms that actively reduce biased approaches to policing, work towards addressing the issues outlined in this report and are accompanied by concrete steps to address wider and underlying issues of bias that permeate the criminal justice system. The development and trial of any such programs should be overseen by independent experts, and the evaluation of trials should be conducted entirely independently, with the results made public. A human rights impact assessment should be developed in relation to the use of any new digital solutions, and this must also be made available to the public.

60 *Reisman, technical fellow at the AI Now Institute, quoted in Burgess, 2018, UK police are using AI to inform custodial decisions – but it could be discriminating against the poor, Available at: https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit [Accessed November 2018]*



# USE OF PREDICTIVE POLICING PROGRAMS IN THE UK

# USE OF PREDICTIVE POLICING PROGRAMS IN THE UK

Liberty sent 90 Freedom of Information Act (FOIA) requests[61] throughout 2018, asking UK police forces about their use of different predictive policing programs. The responses show that at least 14 police forces in the UK are currently using predictive policing programs, have previously used them or are engaged in relevant research or trials.[62]

| Police Force | Using or trialling – or planning to use or trial – predictive mapping programs? | Using individual risk assessment programs? |
|---|---|---|
| Avon and Somerset | ✓ | ✓ |
| Cheshire | ✓ | |
| Durham | | ✓ |
| Dyfed Powys | ✓ (In development) | |
| Greater Manchester Police | ✓ | |
| Kent | ✓ | |
| Lancashire | ✓ | |
| Merseyside | ✓ | |
| The Met | ✓ | |
| Norfolk | ✓ Uses a "solvability" algorithm (see below) | |
| Northamptonshire | ✓ | |
| Warwickshire and West Mercia | ✓ (In development) | |
| West Midlands | ✓ | ✓ |
| West Yorkshire | ✓ | |

61 *Members of the public are entitled to request information from public authorities under the Freedom of Information Act 2000. Failure to respond to our requests constitutes a breach of the Act. Public authorities are required to respond to the request within 20 days.*

62 *The appendices included at the end of this report (see pages 79-83) outline the police forces which did not use the predictive policing programs considered in this report, as well as those which did not respond to requests.*





## Avon and Somerset

Avon and Somerset are currently using a mapping program[63], but they told Liberty that they held no information in relation to guidance documents about the program, and that a University of the West of England student is being funded to evaluate the approach and will provide an independent assessment of the technique.

Avon and Somerset Police stated that they had *"given consideration"* to removing certain information from the process to avoid bias and the exacerbation of pre-existing inequalities. However, no further information was provided as to what information, if any, had been excluded from the process for this reason.

The force also uses an alarmingly broad variety of individual risk assessment programs, each of which uses machine learning. They use these risk assessment programs to assess a person's:

- Likelihood of re-offending
- Likelihood of victimisation and vulnerability
- Likelihood of being reported missing
- Likelihood of perpetrating a "serious domestic violence or sexual violent offence"
- Likelihood of being the victim of a "serious domestic violence or sexual violent offence"
- Likelihood of perpetrating a burglary offence
- Likelihood of perpetrating a stalking and harassment offence

63 *Avon and Somerset Freedom of Information response to. Received 18 July 2018. The program is based on a modeler made by multinational tech company IBM – see: https://www.ibm.com/uk-en/marketplace/spss-modeler*

- Likelihood of being the victim of a stalking and harassment offence
- Likelihood of a staff member having a stress-related period of sickness

This use of risk assessment algorithms forms part of Avon and Somerset's use of a program called "Qlik Sense", which has 30 applications across various police teams.[64]

The variety of ways in which Avon and Somerset Police use predictive policing is astonishing, and the assessment of victimhood is a highly controversial development.

Research undertaken by the Data Justice Lab into the use of data analytics in public services in the UK revealed that the technology was developed in part *"as a response to on-going austerity measures"*.[65] A chief inspector commented that *"...it's really the data help [sic] around which everything revolves"*. A former employee told researchers that *"they do use some social demographic information, like Acorn type information[66] that comes in"*, but another practitioner denied this in their interview.[67]

The interviews with practitioners also revealed the gravity of the outcomes based on the risk assessment algorithms, with one policing coordinator commenting that the system *"highlights it to you that you need to get this person into custody sooner rather than later."* This is particularly concerning given one coordinator's

64 *Dencik et al, 2018, Data Scores as Governance: Investigating uses of citizen scoring in public services, Available at: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report.pdf [Accessed December 2018]*
65 *Ibid*
66 *Acorn is a tool which categorises the UK's population into demographic types*
67 *Dencik et al, 2018, Data Scores as Governance: Investigating uses of citizen scoring in public services, Available at: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report.pdf [Accessed December 2018]*





admission that the data *"isn't always"* correct and a data quality issue may occur where *"someone is identified as high risk because they were previously linked to a murder or attempted murder and actually they were eliminated from that murder"*.[68]

According to Avon and Somerset Police, they use these predictive policing programs to *"support the organisation's assessment of risk at an individual person level"* [69] and that *"this technique is required to help understand risk and demand within the massive volumes of data collected on a daily basis"*.[70] They said that decisions made about action are entirely based on professional judgement, and that these programs *"triangulate with other sources, for example, intelligence reports [and] partnership referrals"*.[71]

Avon and Somerset told us that no ethnicity data is used, but that the process *"primarily focuses on crime incidents, demographic data (excluding ethnicity) and command and control incident data"*.[72] This response suggests that, while ethnicity is excluded from the inputted demographic data, it could include data which is a proxy for race.

Avon and Somerset originally refused to respond to our FOIA request. They tried to argue that releasing this information could increase criminal activity in areas perceived as more vulnerable to crime, or inform criminals of police tactics, thus enabling them to take measures to avoid detection.

Liberty asked for an internal review of this decision. We argued that the disclosure of information concerning how predictive policing programs work – in terms of, for example, the data points

68 *Ibid*
69 *Avon and Somerset Freedom of Information response to internal review. Received 3 October 2018.*
70 *Ibid*
71 *Ibid*
72 *Ibid*

used and whether the programme utilises algorithms or artificial intelligence – is paramount for policing transparency and assists us to understand otherwise impenetrable technologies that the public will struggle to hold to account.

Furthermore, the information requested would not amount to sufficient insight to inform people of police tactics, or indicate geographical areas which may be vulnerable – even if combined with the same information from other forces. Following the internal review process, Avon and Somerset agreed to disclose the information above.

## Cheshire

Cheshire Police used a mapping program called *"Operation Forewarn"* between January 2015 and November 2015. The data used for the mapping program related to *"all serious acquisitive crime with the exception of robbery, theft or vehicle registration plates and theft of fuel and criminal damage to a point of entry"*.[73]

Cheshire stated that this use of data required no algorithms or artificial intelligence. However, the program was clearly intended to be predictive in nature and is therefore subject to many of the concerns highlighted above concerning bias and discrimination.

Regarding potential bias, Cheshire Police stated that this was *"not applicable as no algorithm based software was used and only reported offences were mapped"*. However, as discussed throughout this report, any data on past crimes would contain intrinsic bias.

When asked about guidance, research or testing, Cheshire would neither confirm nor deny the existence of any relevant documents.

73 *Cheshire Freedom of Information response. Received 6 July 2018.*





## Durham

Durham Police use an individual risk assessment program called the Harm Assessment Risk Tool (HART).[74]

HART was produced following a partnership between the Department of Criminology at the University of Cambridge and Durham Constabulary, and used for the first time in April 2016.[75]

Durham refers to the use of HART as *"an ongoing experimental research program",*[76] intended to *"support custody officers in identifying offenders who could be eligible for deferred prosecution and inclusion onto a diversionary scheme"*.[77]

The original HART model was fed with historical data from 104,000 custody events that occurred in Durham Constabulary from 2008 to 2012. However, the model has been fed more historical data as part of the ongoing research programme.[78]

According to Durham Police, the model uses 34 predictors: 29 are taken from the detained person's offending behaviour plus age, gender, two forms of post code ("outward code only" – the first part of the post code) and *"a count of intelligence reports related to the detained person"*.[79] Durham Police have been heavily criticised for using postcodes as part of this process. Information such as postcodes and socio-demographic data can reinforce existing biases in policing decisions and the criminal justice system more broadly.[80]

74 *See pages 4-6 for discussion of the HART program.*
75 *Durham Freedom of Information response. Received 18 July 2018*
76 *Outlined in a request to Durham Constabulary under the Freedom of Information Act, dated 19 February 2018.*
77 *Ibid*
78 *Durham Freedom of Information response . Received 18 July 2018*
79 *Ibid*
80 *See page 5 for discussion of proxies for race in predictive policing programs.*

In their FOIA response to Liberty, Durham confirmed that the software does not use financial data, and that they had not purchased any data from external companies. However, Sheena Urwin, head of criminal justice at Durham Constabulary, had previously accepted that Durham Police had worked with credit data company Experian *"to improve its understanding of local communities"*.[81]

Durham stated that it is the custody officer who will make a final decision, but that they do not have guidance documents – only *"verbal briefings"* [82] Durham referred to a "Script for Custody Officers", which Liberty requested sight of, but this was refused on the basis that it was now no longer in use, despite it being specifically referenced in the initial response provided by Durham Police.

When asked about bias or the exacerbation of pre-existing inequalities, the alarming response was that "*no accuracy comparisons have yet been made between different demographic groups"* but that *"in the Durham Constabulary area over 90 [per cent] of the custody population describe[s] themselves as 'White British'"*. This is a deeply concerning response – the fact that Durham is not a diverse area with a low percentage of BAME residents does not negate the need for careful consideration and mitigation of potential bias in relation to race and other inequalities based on characteristics such as income.

## Dyfed Powys

In response to Liberty's request about predictive mapping programs, Dyfed Powys Police stated that they are currently

81 *BBC News, 2018, Durham police criticised over 'crude' profiling [Online], 9 April 2018, Available at: https://www.bbc.co.uk/news/technology-43428266 [Accessed November 2018]*

82 *Durham Freedom of Information response . Received 18 July 2018*





engaging with academics in the development of a potential algorithm for predictive policing, which they described as a *"work in progress"*. No more information was given.

## Greater Manchester Police

While Greater Manchester Police stated that *"no specialist software"* has been developed in terms of predictive policing programs, they also noted that they use a *"mostly"* simple mapping technique, so the only data used are burglary dwelling crime records containing date, time and location (Easting and Northing) information". The technique was first used in May 2010 and is *"still in occasional use"*.

Greater Manchester Police stated that *"the technique does not use algorithms or artificial intelligence"* because the maps *"are produced and interpreted by an Analyst or Researcher"*. They claimed that *"the technique is solely concerned with temporal and location information relating to domestic burglaries so potential bias should not be an issue".*

While this program may not automatically generate patrol maps based off algorithms, data is nonetheless used to make predictions about where crime may take place. It also bears one of the hallmarks of police use of predictive policing – a lack of awareness around the feedback loops which may result from their use and the impact this has on over-policed communities.

## Kent

Kent Police hit headlines[83] with its use of PredPol, the brand name of a mapping program used widely in the United States. However, the force has recently revealed that, as of 31 March 2018, it no longer uses this program – but it will be looking to develop an internal program or invest in similar predictive policing programs available at a lower cost.[84]

Kent Police started using PredPol in 2013. They released initial findings[85] relating to its use in the same year, ostensibly ahead of a final report – but this never materialised. Kent Police were unable to provide any information as to why a final report was not produced.

When asked about bias in relation to their use of PredPol, Kent Police asserted that the *"input data was limited to crime type, time and location of incident/crime, and does not include characteristics of persons"*. While this may be the case, this response fails to take account of the ways in which predictive mapping programs can nonetheless be biased (outlined above at pages 13-21) and lead to the over-policing of certain communities.

83 *See: Dearden, 2017, How technology is allowing police to predict where and when crime will happen, The Independent, Available at: https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html [Accessed November 2018]*

84 *Kent Freedom of Information response. Received 29 October 2018.*

85 *Kent Police, 2013, PredPol operational review -initial findings, Available at http://www.statewatch.org/docbin/uk-2013-11-kent-police-pp-report.pdf [Accessed November 2018]*





## Lancashire

Lancashire Police confirmed that they have trained analysts and specialist investigators who have predictive analysis and crime mapping capabilities.[86]

They stated that the methods employed use a variety of software, but declined to give any further information. This leaves unanswered questions about the sort of technology used, what data is relied upon and how they respond to the issue of potential bias. This lack of transparency about their practices means the public cannot hold them to account and question what role technology plays in the way the people of Lancashire are policed.

## Merseyside

Merseyside Police stated that they currently use *"predictive techniques"* [87] based on historical data. The program was written by Merseyside Police employees and is run on shared servers using data held in the police force's "data warehouse".[88]

On the subject of bias, they stated that *"the predictive policing techniques used by Merseyside Police relate to statistical information concerning crimes and incidents that have occurred and not about the people involved in them"*.[89] Again, this response shows a lack of awareness around the way predictive mapping programs have been found to initiate "feedback loops" which see the police constantly return to already over-policed communities.

86 *Lancashire Freedom of Information response. Received 21 August 2018.*

87 *Merseyside Freedom of Information response. Received 25 June 2018.*

88 *Ibid Data warehouses are large stores of data accumulated from a wide range of sources. They are designed to give a long-range view of data over time.*

89 *ibid*

## Metropolitan Police

The Metropolitan Police (the Met) conducted a number of trials of commercial products for 12 months, from May 2014 to April 2015. The products trialled included PredPol, Azavea and Palantir predictive mapping programs. At the same time as trialling these products, they utilised a predictive mapping program which was developed internally by the Met.

At the end of the trials, the decision was taken that the cost of implementing the commercial products was too great, but the internal program remains in place.

This internal product looks at the location of previous offences, the proximity to other similar offences and to the time that has elapsed since an offence was committed.

It uses reported crime data, including the location, date and time of the offence, and uses an algorithm. It runs automatically, but the response to the output was said to be *"subject to local interpretation"* by police officers when tasked to action this information. The Met accepted that the program was used to inform preventive policing, such as *"hotspot patrolling"*.[90]

The Met stated that there was no testing or research that could be provided in relation to their use of predictive policing programs. In light of the concerns described above regarding bias, this is clearly problematic.

They refused to disclose any guidance documents provided to the police on their use of the mapping program, stating that disclosure could result in crime evasion.

90 *Metropolitan Police Freedom of Information response. Received 11 October 2018.*





## Norfolk

While Norfolk Police said they didn't use and have never used technology to assess risk posed by people detained in custody, they are *"currently trialling an algorithm to assist in deciding whether burglary investigations should be allocated for further investigation"*.[91] The algorithm was developed by the University of Cambridge and uses data from Norfolk Police.

According to a historical FOIA request referred to by Norfolk Police, *"all cases of burglary are run through the algorithm before the Investigation Management Unit (IMU) decided whether or not to assign each case for investigation"*.[92]

According to Norfolk Police, all decisions made by the algorithm are reviewed by a member of staff, who can override any decision made, but no further information was given as to how this process works, what training members of staff receive to carry out this task or how automation bias is avoided.[93]

John Apter, Chairman of the Police Federation, criticised the use of this program and warned that the introduction of such systems represented a slippery slope which threatened to erode the trust that exists between the public and the police: *"I think we should always encourage officers to work effectively with new technology where appropriate...But my concern is that we can sometimes rely too heavily on technology, especially algorithm based technology."* [94]

91 Norfolk Freedom of Information response. Received 9 July 2018.
92 Ibid
93 See ours concerns in the "Human v Machine" section of this report, from page 31
94 *Evans, 2018, Police criticised for using computer to work out whether to send officers to burglaries, The Telegraph, Available at: https://www.telegraph.co.uk/news/2018/09/02/police-criticised-using-computer-work-whether-send-officers/ [Accessed December 2018]*

## Northamptonshire

Northamptonshire Police responded to our request for information about predictive mapping programs by confirming that they have used a predictive policing program. It was first used in 2015, but they failed to respond to questions as to whether it was still in use. They also refused to respond to any other questions about the program on the basis of the law enforcement exemption contained within the Freedom of Information Act 2000. They argued that telling the public what data is used by the program or the guidance that officers receive on its use would compromise their current or future law enforcement role. This is clearly unacceptable given the rights impact of these technologies – we need transparency to better understand these programs and have an informed debate about the role they should play in our society.

The force accepted that disclosure of this information could aid public debate and awareness of the technology and software that they employ. They also recognised that the public are entitled to know how public funds are spent, and how the police deploy resources within their force areas. However, the reasons for their refusal to disclose information were that *"the security of the country is of paramount importance, and the Police service as a whole is charged with preventing and detecting crime and protecting the communities they serve. As part of that policing purpose, various tactical tools may be utilised on an ongoing basis. The police service will not divulge information held, if to do so would place an individual, or community as a whole, at risk."* [95]

They stated that *"the comparative arguments in favour of non-disclosure, which in this case is our ability to prevent and detect*

95 *Warwickshire and West Mercia Freedom of Information response. Received 27 June 2018. Previous request referred to dated 5 October 2017.*





*crime, by far outweigh [the arguments for disclosure]"*.[96]

## Warwickshire and West Mercia

Warwickshire and West Mercia form a "police alliance", and the response provided applies to both forces. They informed us that an FOIA response they provided to a separate request in 2017 still applied, and that there had been no update since that time. This FOIA response stated that mapping software was trialled in one policing area but was not procured, but that they are *"about to introduce other software systems that may enhance our capability or will at least need to be considered regards interoperability*".[97]

## West Midlands

### MapInfo

West Midlands Police use a program called MapInfo. This uses crime and incident data to map hotspots of incidents that have already happened. A time-based analysis is carried out to analyse when crimes occur, including seasonality, days of the week and times of day. The data used includes crime data – but also anti-social behaviour incidents – reported to West Midlands Police over the two years prior.

According to West Midlands Police, no predictive analysis takes place other than *"assuming that long term hotspots will continue*

96 *Northamptonshire's response arrived at Liberty 124 working days after we had sent our request – 104 days over the limit outlined in the Freedom of Information Act. Liberty therefore did not appeal Northamptonshire's refusal to disclose information, which would have delayed the release of our report. As such, it was not subject to appeal in the same way as initial responses from Avon and Somerset, Lincolnshire and Merseyside were.*

97 *ibid*

*to be hotspots unless some preventative action is taken in these areas"*.[98] However, it is precisely this assumption which can lead to the discriminatory patterns of policing discussed above, especially with the inclusion of anti-social behaviour incidents. For example, a recent study showed that young black men in London are disproportionately more likely than white people to be prosecuted for breaking public dispersal orders available to police as part of a range of measures to crack down on antisocial behaviour.[99]

Human oversight is *"required to evaluate if the data used is of quality and if the outputs are reasonable"*.[100] No further information was provided as to how a police officer can assess the quality of the data inputted or the reasonability of the outputs, when these very outputs are so opaque.

When asked about bias, West Midlands Police were the only police force to accept that the software does not take into account under-reporting or non-reporting of crimes, since its database is limited to crimes/incidents reported to West Midlands Police. However, no reference was made to the issues that this can give rise to or how these risks were mitigated, if at all.

### West Midlands Police Data Driven Insights project

Separate to the use of MapInfo is the West Midlands Police Data Driven Insights project. The Data Driven Insights project consists of three different strands – Insight Search, Business Insight and the Insight Lab. Of these three strands, the Insight Lab is the most relevant to predictive policing because it *"will use advanced statistical analysis to better predict risk and gain a deeper*

98 *West Midlands Freedom of Information response. Received 2 July 2018.*
99 *Mills et al, 2018, Anti-social behaviour powers and young adults: The data, Available at: https://www.crimeandjustice.org.uk/publications/anti-social-behaviour-powers-and-young-adults-data [Accessed November 2018]*
100 *West Midlands Freedom of Information response. Received 2 July 2018.*





*understanding of complex policing problems"*.[101]

West Midlands Police also stated that they are *"in the process of developing [our] own data science capability and may well in the future look to develop algorithm assisted decision making to make an assessment of the risk posed by a detained person. This would most likely be a much broader evaluation of risk"*.[102]

West Midlands Police stated their plans to use algorithmic assisted decision making in the near future, although said that they have not yet developed and deployed any models. However, recent reports reveal that they are leading on a Home Office funded £48 million project called "National Analytics Solution". The program analyses vast quantities of data from force databases, social services, the NHS and schools to calculate where officers can be most effectively deployed – and an initial trial *"combined data on crimes, custody, gangs and criminal records to identify 200 offenders who were getting others into a life on the wrong side of the law"*.[103]

## West Yorkshire

West Yorkshire Police are currently working with University College London on an algorithm to predict areas at highest risk of crime. The project was started in December 2016 and is in a pilot stage. It uses an algorithm that *"identifies areas of vulnerability to specified crime types based on crimes happening previously"*.[104] The data used is historic crime or incident locations. The output of the

101 *Ibid*
102 *Ibid*
103 *Beckford, 23 December 2018, 'Minority Report' police computer is being used to 'predict' who is likely to commit crimes amid ethical concerns over £48million project, the Mail on Sunday, Available at: https://www.dailymail.co.uk/news/article-6523997/Minority-Report-police-computer-predict-likely-commit-crimes.html [Accessed January 2019]*
104 *West Yorkshire Freedom of Information response. Received 25 June 2018.*

program is a suggested "Patrol Plan", highlighting a suggested area for officers to be visible *"in order to reduce vulnerability"*.[105]

West Yorkshire Police point to some analysis conducted by Leeds University on a range of predictive techniques to inform the project, with some made available online.[106] However, the research is high level and technical, addressing the functionality of the algorithms used rather than the real-life impacts for policing.

According to West Yorkshire Police, *"the algorithm only looks at the recorded location of crimes, so bias based on any other characteristics is not possible."* [107] Again, this response neglects to consider the way predictive mapping programs have been found to initiate "feedback loops" which see the police constantly return to already over-policed communities.[108]

105 *Ibid*
106 *See: https://github.com/QuantCrimAtLeeds/PredictCode*
107 *Ibid*
108 *See page 16 for discussion of predictive policing feedback loops*

# THE FUTURE OF POLICING

# THE FUTURE OF POLICING

We have seen how predictive policing programs pose significant threats to our fundamental rights – but these threats do not exist in a vacuum. Wider trends in technology and policing only serve to compound these risks associated with predictive policing.

## Big data policing

Predictive policing programs feed off our culture of "big data" – the abundance of personal information accumulated about us in the digital age. These massive data sets can then be analysed by computers to reveal patterns and trends, and these often relate to human behaviour.

As our big data society continues to expand, the state will amass more and more information about each and every one of us – becoming increasingly reliant on algorithms and machine learning to make any use of it, just as we have seen with the use of predictive policing programs. Data has started to drive the operation – it is not the programmers anymore but the data itself that defines what to do next.[109]

The databases that the police will be able to use to feed algorithmic programs are ever-expanding. For example, the Home Office is planning a new policing super-database. By 2020, the Home Office will bring together the Police National Computer (PNC) and the Police National Database (PND) onto one platform, creating a new database called the Law Enforcement Data Service (LEDS).

109 *Oswald et al, 2018, Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality, Information & Communications Technology Law, Volume 27, 2018, Available at: https://ssrn.com/abstract=3029345 [Accessed November 2018] citing Alpaydin, 2016, Machine Learning, MIT press*





### Police National Computer (PNC)

The PNC holds a record of anyone who has been arrested, convicted, cautioned, reprimanded or warned about a recordable offence. A recordable offence is any offence punishable by imprisonment of at least one year, plus a number of other minor offences including begging or drunkenness in a public place.

Records relating to over 12 million people are currently held on the PNC, and information about people's convictions, cautions, reprimands or warnings is stored for 100 years from their date of birth.

### Police National Database (PND)

The PND, which was introduced in 2010, is a nation-wide database that includes all of the information on the PNC plus extra information and "intelligence" held by local police forces. This includes "soft" information such as allegations made against a person that did not result in any arrest being made, and concerns passed on to the police from other public bodies (for example, schools or social services).

Liberty is deeply concerned about the misuse of this system, which holds an enormous quantity of sensitive data, and how it might be used alongside predictive policing programs or other computer programs which rely on algorithms to make policing decisions.

By bringing these two databases together, the police are aiming to maximise the amount of data they have access to and link it together with other information. They have admitted that data the

police no longer have any legal basis to hold – for example, images of people taken into custody who were never charged or convicted of any crime – will nonetheless be transferred onto the new super-database.

We can expect to see even wider sharing of police data with non-policing organisations, with the Home Office inviting this simply where a *"business case"* can be made.[110] There are also issues with the security of the data held on the super-database, and with its accuracy.

Key questions remain unanswered, such as how exactly LEDS will link with other databases – including immigration databases – and how it may be used in conjunction with algorithms, artificial intelligence and machine learning to assist with profiling, predictions and police decision-making.

Replacing the need for suspicious behaviours that officers can actively observe with "suspicious" data will exacerbate the current use of arbitrary and speculative stops which are disproportionately targeted against people from BAME and low-income communities. Researchers have cautioned that *"without the requirement of some observable activity, the odds increase that predictive stops will target innocent people, criminalize by association, and negatively impact individuals based on little more than a hunch supported by non-criminal facts."* [111]

110 *Home Office, 2018, LEDS – Privacy Impact Assessment Report, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf [Accessed November 2018]*

111 *Ferguson. 2015. Big Data and Predictive Reasonable Suspicion. University of Pennsylvania Law Review163, p 387, Available at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9464&context=penn_law_review [Accessed November 2018]*





## A web of surveillance

The use of predictive policing programs is one of a whole host of technological developments being rolled out by police across the country.

Recent developments include widespread use of body worn video cameras, facial recognition (a camera which scans the faces of every single passer-by to match them against a "watch list" – Liberty is currently challenging South Wales Police's use of this technology in the courts),[112] mobile fingerprint scanners (which identify people on the street using their biometric data)[113] and mobile phone extraction (which allows police officers to download all the content of your mobile phone – without your consent or even your knowledge – whether you are a victim or someone who is being detained).[114]

Police forces have also purchased IMSI catchers,[115] a technology which tricks all mobile phones in a certain area into connecting to it so it can identify the owner of the mobile phone and intercept their communications. The police refuse to give the public any information about the use of these extraordinarily invasive devices and will "neither confirm nor deny" that they are in use – despite clear evidence that police forces have purchased them, or put aside money to purchase them.[116] Liberty is currently representing

112 *For more information, see: https://www.libertyhumanrights.org.uk/resist-facial-recognition, https://www.libertyhumanrights.org.uk/human-rights/privacy/police-surveillance-technology and https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/cardiff-resident-launches-first-uk-legal-challenge-police-use*

113 *For more information, see: https://www.libertyhumanrights.org.uk/news/blog/papers-please-how-biometric-id-checks-put-our-rights-risk and https://www.libertyhumanrights.org.uk/human-rights/privacy/police-surveillance-technology*

114 *For more information, see: https://www.libertyhumanrights.org.uk/human-rights/privacy/police-surveillance-technology*

115 *Aviram, 2016, Revealed: Bristol's police and mass mobile phone surveillance, Bristol Cable, Available at: https://thebristolcable.org/2016/10/imsi/ [Accessed November 2018]*

116 *Ibid*

Privacy International to challenge the police forces' reliance on the "neither confirm nor deny" position.[117]

## The role of the private sector

Private companies are not only developing predictive policing programs – they are using them. For example, PredPol revealed in April 2018 that it will bring its "police-tested technologies" to the private sector, stating that *"private security companies have responsibilities much like law enforcement"*.[118] This emphasises a troubling pattern whereby technologies are developed for use in the context of law enforcement and then rolled out to private settings – increasing the surveillance we are all under. According to PredPol, one out of every 33 people in the United States will be in an area where PredPol is in use.[119] Add in use by private companies and the number of communities who may be exposed to rights infringements becomes even more significant.

Each of these individual developments represents a threat to our human rights – and taken together, they become something even more sinister. Increasing numbers of private companies are also deploying technologies such as facial recognition, expanding the ubiquitous web of surveillance.[120] Add to this the enormous quantities of personal data that the state holds on us, and their

117 *Liberty press release, 7 August 2018, Privacy International and Liberty fight to unearth police use of intrusive mobile phone monitoring technology, Available at: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/privacy-international-and-liberty-fight-unearth-police-use [Accessed November 2018]*

118 *See http://blog.predpol.com/predpols-advanced-predictive-policing-technology-now-available-to-corporate-customers*

119 *See https://www.predpol.com/about/*

120 *See: Archer, 2018, Facial recognition to be used in British supermarkets for the first time, The Telegraph, Available at: https://www.telegraph.co.uk/technology/2018/10/17/facial-recognition-used-british-supermarkets-first-time/ [Accessed November 2018]. See also: Robson. 2018, Greater Manchester Police monitored every visitor to Trafford Centre for SIX MONTHS using controversial technology until they were told to stop, Manchester Evening News, Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943 [Accessed November 2018]*





ability to run it through algorithms to make predictions and decisions, and we have a disturbing vision of the future. We need to challenge all elements of the ubiquitous surveillance state and its normalisation in our society, and this includes standing up to predictive policing programs and other machines which make decisions impacting on our human rights.

Increasingly, police forces are rushing to adopt new technologies without proper piloting and evaluation. These processes are essential – for ensuring that advancements in technology actually achieve police aims, are rights-respecting and attract public confidence.

We have often seen operational use of new technologies simply labelled a "trial", but with little or no oversight – and no consent from those who end up as unwitting participants.[121] Little information is made public as to how these trials are evaluated and what the results show.

As technology continues to advance and companies continue to design technologies to flog for deployment by police forces and other private companies – contributing to our ubiquitous surveillance state – we need a well-informed public debate about whether this technology is beneficial for our society and the inherent threat to our human rights. This should be an open, transparent and informed debate for both our parliament and for the public.

121 *See, for example: Couchman, 2018, "Not a fool-proof system": Facial recognition in action, Liberty blog, Available at: https://www.libertyhumanrights.org.uk/news/blog/%E2%80%9Cnot-fool-proof-system%E2%80%9D-facial-recognition-action [Accessed November 2018]*

The rush to roll out new, untested technologies is partly the result of increasing pressures on police forces. But as forces are pushed to do more with less, we should call for a focus on public accountability, rather than accepting innovation which allegedly reduces costs at the expense of our rights.

## People as "pre-criminals"

Predictive policing is predicated on the idea that we should use clues in data to make assumptions about how people will behave.

The idea of "pre-criminality", based on prejudicial generalisations, is already prevalent in the way we are policed. In order to resist predictive policing, we need to resist the dangerous practice of categorising people and subjecting them to additional surveillance and monitoring because we think we know how they are going to act.

Pre-criminality is one of the hallmarks of policies deployed by the police, including the Gangs Matrix and Prevent. Both of these deeply problematic schemes show significant racial bias.

Prevent is a government policy with the stated aim *"to stop people becoming terrorists or supporting terrorism"*.[122] The most recent statistics on Prevent referrals which note the religion of the referred individuals relate to the year 2012-2013. The figures indicate that in that year, 57.4 per cent of all referrals were Muslim (as against other groups of 26.7 per cent of unknown religion, 9.2 per cent Christian, and no other religion having representation over

122 *One of the stated objectives is to "prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support", with the responsibility to deliver of this objective resting with specified public authorities under the Counter-Terrorism and Security Act 2015. By 1 July 2015, all schools and registered childcare providers in England, Wales, and Scotland (including registered child minders) were subject to a duty, under section 26 of the 2015 Act, to "have due regard to the need to prevent people from being drawn into terrorism".*





0.5 per cent). Prevent is a discredited and discriminatory strategy, based on a flawed model of extremism prevention.

RightsWatch UK found, as part of their report "Preventing Education", that *"the Prevent strategy...is predicated on a series of flawed assumptions. The most concerning of these is that holding non-violent extremist views is a reliable precursor of future participation in terrorism".* Lord Ken Macdonald, former Director of Public Prosecutions, has also observed: *"many, perhaps most, of the behaviours targeted by Prevent, are behaviours that are not in themselves criminal in any way ... [this] intensifies the strength of surveillance and government reach into people's every-day lawful lives – and indeed into whole areas of their everyday lawful discourse"*.[123]

Another example of the use of "pre-criminality" in policing is the Gangs Matrix – a database of people that the police claim are vulnerable to being drawn into "gangs" or at risk of violence from "gang" members.

In July 2016, 87 per cent of the people included on the Gangs Matrix were from black and minority ethnic communities, with 78 per cent being black. Seventy-five per cent were victims of violence themselves, and 35 per cent had never committed a serious offence.

Research undertaken by Amnesty International UK[124] shows that the Gangs Matrix is based on a vague and ill-defined concept of "the gang" that has little objective meaning and is applied inconsistently in different London boroughs. The Matrix itself and the process for adding individuals to it, assigning "risk scores" and

123 *Lord Ken Macdonald, 2018, video of speech regarding Prevent in the Academy, Available at: https://www.wadham.ox.ac.uk/news/2016/february/prevent-in-the-academy [Accessed November 2018]*

124 *Amnesty International UK, 2018, Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database, Available at: https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf [Accessed November 2018]*

sharing data with partner agencies, appears to be similarly ill-defined with few, if any, safeguards and little oversight.

Inclusion on the Gangs Matrix is deeply stigmatising and can follow people in their interaction with service providers such as housing and education, and conflates elements of urban youth culture with violent offending, and in a way which is heavily influenced by race.

The Information Commissioner's Officer (ICO) carried out an investigation into the Gangs Matrix in 2018, finding that there were *"multiple and serious breaches of data protection laws"*.[125] The ICO found that the Gangs Matrix does not clearly distinguish between "perpetrators" and "victims" and that the model was operated in an unclear and inconsistent way across the boroughs. Some boroughs even operated informal lists of people who had been removed from the Gangs Matrix, so that the Met could continue to monitor people even when intelligence had shown that they were no longer active gang members. There was also excessive processing of data which resulted from *"blanket sharing"* with third parties.[126]

What's more, the policing super-database will provide the capability to combine and link this data in more detail than ever before. How long will it be until the Gangs Matrix and Prevent are combined with other data and run through predictive policing algorithms to decide who should be arrested on the suspicion of a recently committed offence?

125 *See: Information Commissioners Office, 2018, ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws, Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/ [Accessed November 2018]*

126 *Ibid*





The subjectivity of the criteria for inclusion on such as the Gangs Matrix and Prevent inevitably lead to referral under arbitrariness. There is the potential for predictive policing, the concept of "pre-criminality", big data and surveillance to link together and create a ubiquitous surveillance system that normalises the invasion of our privacy and chills our freedom of expression in an unprecedented way – impacts which will be felt most keenly by marginalised communities.

We need to say no to this dystopian future for policing, and instead demand that the police work to minimise their use of data and focus on improving community relations and reducing bias within the criminal justice system.

**Recommendation Five:** Police forces should examine more widely their use of data, to include a full review of the Gangs Matrix and similar databases. Police forces must, at the very least, introduce guidance requiring that police databases such as the Gangs Matrix set out targeted criteria for inclusion and removal, outline a process for challenging a person's inclusion, explain the sources used to populate the database, and establish safeguards to prevent discriminatory use of data. Similarly, and in line with commitments to an independent review into the "Prevent" strategy,[17] the police should review the way in which they hold and use data obtained under the "Prevent" scheme.

# CONCLUSION

# CONCLUSION

Affording discriminatory policing practices a technological veneer of legitimacy is dangerous. There is no clear evidence to suggest that this use of new technology leads to safer communities,[127] fairer treatment, greater transparency or increased trust in the police. Instead, we are likely to see the perpetuation of racial profiling, incursions on our privacy, ever more invasive surveillance and the increasing infringement of our rights.

Achieving greater transparency, proper oversight, robust regulation and rights compliance would mitigate the risks posed by predictive policing to some extent – but these aims are not currently achievable due to the lack of transparency surrounding the use of these programs and how they work.

In any case, the introduction of a regulatory system or new oversight bodies will not adequately meet these concerns as they currently stand. A regulatory system cannot resolve the serious issues of bias which are so intrinsic in data sets and the use of machine learning. An oversight body cannot decipher complex

127 *See, for example: Hunt et al, 2014, Evaluation of the Shreveport Predictive Policing Experiment, Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR531/RAND_RR531.pdf [Accessed November 2018], Lum et al, 2016, To predict and serve?, Significance Magazine, Available at: https://rss.onlinelibrary.wiley.com/doi/abs/10.1111/j.1740-9713.2016.00960.x [Accessed November 2018], Robinson et al, 2016, Stuck in a Pattern: Early evidence on "predictive policing" and civil rights, Available at http://centerformediajustice.org/wp-content/uploads/2016/08/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf [Accessed November 2018]*





algorithms to allow for proper transparency and accountability – even those who have significant technical expertise are unable to explain exactly how an algorithm makes a decision.

While it may seem a laudable aim to prevent crime before it ever occurs, this is best achieved by addressing underlying social issues through education, housing, employment and social care. The solution does not lie in policing by machine.

# APPENDIX 1:
# PREDICTIVE POLICING NOT IN USE

The following police forces have not used and are not currently using predictive mapping programs, or held no information on them. Holding no information can generally be taken to mean that they are not in use.

- Bedfordshire
- Cambridge
- City of London
- Cleveland
- Cumbria
- Derbyshire
- Devon and Cornwall
- Dorset
- Durham
- Gloucestershire
- Hampshire
- Hertfordshire
- Leicestershire
- Lincolnshire
- Norfolk
- North Yorkshire
- North Wales
- Northumbria
- Nottinghamshire
- Police Service of Northern Ireland
- Scotland
- South Yorkshire
- Staffordshire
- Suffolk





The following police forces have not used and are not currently using individual risk assessment programs, or held no information on them. Holding no information can generally be taken to mean that they are not in use.

- Bedfordshire
- Cambridge
- City of London
- Cleveland
- Cumbria
- Derbyshire
- Devon and Cornwall
- Dorset
- Gloucestershire
- Hampshire
- Leicestershire
- Lincolnshire[128]
- Merseyside[129]
- Northumbria
- North Wales
- Scotland
- South Yorkshire
- Staffordshire
- Suffolk
- Warwickshire
- West Mercia
- West Yorkshire

128 *Lincolnshire Police originally refused to respond to Liberty's FOIA request on the basis that doing so would undermine the use of algorithms and/or artificial intelligence software as a tool. We requested an internal review of this position and it was overturned.*

129 *Merseyside originally refused respond to Liberty's FOIA request on the basis that doing so would be too expensive in terms of time and resources. We refined our request and received a response.*

# APPENDIX 2: NO RESPONSE

The following police forces did not respond to our requests for information on predictive mapping programs in sufficient time to be included in this report. All were considerably over the 20 working day time limit given to public authorities to respond to FOIA requests.[130]

- Essex
- Humberside
- South Wales
- Surrey
- Sussex
- Wiltshire

The following police forces did not respond to our requests for information on individual risk assessment programs in sufficient time to be included in this report. All were considerably over the 20 working day time limit given to public authorities to respond to FOIA requests.[131]

- Greater Manchester
- Hertfordshire[132]
- Humberside
- Kent
- Lancashire
- Northamptonshire
- Nottinghamshire
- North Yorkshire
- Police Service of Northern Ireland
- Surrey
- Sussex

130 *Responses which arrived outside the 20 working day time limit were included where possible.*
131 *As above, responses which arrived outside the 20 working day time limit were included where possible.*
132 *Hertfordshire responded by outlining information in relation to facial recognition, rather than algorithmic risk assessment tools as specified in our request. We responded to invite discussion on the correct subject matter, but no reply has been received.*



# APPENDIX 3: HISTORICAL TRIALS

The following police forces have trialled predictive mapping programs, but say that they have decided against formally procuring a program:

## Gwent

From January 2015 until April 2017, Gwent Police were involved in a Small Business Research Initiative funded project. This project was called “Next Generation Predictive Policing” and was run jointly with Welsh Government, Gwent Police and Innovate UK. The programme brought together small technology companies and public sector organisations who have *“a problem that needs a solution”*. A competition was run and successful companies were awarded funding and access to the organisation in order to help them develop a working prototype, which the public sector organisation could choose to purchase at the end of the project if they feel it met their specific need.

Two companies were chosen to work with the force to develop a prototype, but the force chose not to enter into a formal procurement situation for either product. The two companies involved in the project were Innaxys Ltd, whose solution was called “Gotham”, and GPC Ltd whose solution was called “Trinity”. Gwent Police stated that details of how the solutions worked were the intellectual property of the two companies involved.

## Thames Valley

Thames Valley Police told us that they are not currently trialling any predictive policing software, but it has done in the past. The program in question was a “Near Repeat Calculator”.

They said that the trial was *“extremely limited and took place in either 2012 or 2013 according to staff memory”*.[133]

Due to the age and outcome of the trial (which we can only assume did not result in any procurement of the program for long-term use), we were informed that no material has been retained.

While Thames Valley did not supply any more information about this program, “Near Repeat” programs generally rely on the fact that criminals will return to the same area to commit crimes once they've been successful somewhere, and will continue in that area until returns drop or risk rises. While this is slightly different to identifying longer-term “hotspots”, many of the implications concerning over-policed communities are the same.

133 *Thames Valley Freedom of Information response. Received 29 June 2018.*

# ACKNOWLEDGEMENTS

With thanks to Professor Peter Fussey and Dr Daragh Murray of the Human Rights, Big Data and Technology project based at the University of Essex Human Rights Centre.



# ABOUT LIBERTY

Liberty is one of the UK's leading civil liberties and human rights organisations. We campaign for everyone in the UK to be treated fairly, with dignity and respect. Together with our members, Liberty has been standing up for people and holding the powerful to account since 1934. We work to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty is currently working on the implications of tech developments for human rights and civil liberties, both in policing and more broadly.

Liberty's policy papers are available here:

https://www.liberty-human-rights.org.uk/policy

# LIBERTY

**Liberty House**
**26–30 Strutton Ground**
**London SW1P 2HR**

**020 7403 3888**
**libertyhumanrights.org.uk**
**@libertyhq**