Written evidence submitted by the Human Rights, Big Data and Technology Project

Executive summary

- This submission highlights opportunities and risks associated with the adoption of new technologies by police in England and Wales.
- Opportunities include the implementation of data driven technologies which improve police efficiency by facilitating the prediction and pre-emption of crime that has yet to take place.
- Risks include the ineffective and/or discriminatory use of data driven technologies due to low quality or biased data, as well as privacy issues related to bulk and indiscriminate data collection.
- Recommendations include the creation of oversight and regulatory mechanisms to assess the implementation of data driven technologies and to address associated risks.

Introduction

1. This submission is made by the Human Rights, Big Data and Technology Project (‘the Project’), funded by the Economic and Social Research Council and based at the University of Essex’s Human Rights Centre.¹

2. The Project analyses the opportunities and risks presented by the use of big data and associated technologies from a human rights perspective. Drawing on the expertise of its interdisciplinary researchers and partner organisations, the Project considers how human rights approaches are adapted to meet the rapidly evolving technological landscape. The Project also brings together State, industry and United Nations officials, and academics in the fields of human rights, big data and associated technologies to assess existing regulatory responses and whether reforms are needed to protect human rights.

3. The Project is grateful to the Home Affairs Committee for the opportunity to provide this submission on ‘Policing for the future: changing demands and new challenges’.

Policing for the Future: Opportunities and Risks Associated with the Adoption of Data Driven Technologies

4. Among the changing demands and challenges facing police in England and Wales are the opportunities and risks associated with the adoption of new technologies. Based on our ongoing research and review of the academic literature, this submission offers insights into some of the specific opportunities and risks concerning the police’s adoption of ‘data driven technologies,’ which aid the bulk collection, storage, and analysis of data about persons, places, and activities.

5. Data driven technologies can improve the efficiency of police work by offering law enforcement agencies methods of analysing crime data and generating predictions about crime that is yet to take place. For example, police can use data driven technology to make decisions regarding the most-effective allocation of scarce police resources. However, existing research² indicates a series of risks that must be considered when adopting data driven technologies. This submission highlights three risks associated with data driven technologies, focusing on: the quality of the input data, the potential for discriminatory decision-making, and privacy harms.

Opportunities Associated with Police Use of Data Driven Technologies

6. In the era of big data and advanced information communication technologies, data driven technologies are central to daily interactions with economic, political, and social institutions. For example, online retailers rely on data driven technologies to: collect data on consumer habits, analyse this data to discover consumer trends, and use

¹ HRBDT website. Available at: www.hrbdt.ac.uk
knowledge of these trends to make predictions about future consumer behaviour. Predictions are then capitalised on by retailers in the form of purchase recommendations and personalised advertisements.

7. When adopted by police, data driven technologies serve a similar function by collecting data related to criminal behaviour, analysing this data to determine trends, and using knowledge of these trends to make predictions about future crimes. Predictions are subsequently used to make decisions about the allocation of police resources, hence the term ‘predictive policing.’ Contemporary predictive policing uses software that amalgamates the police’s crime data (information from police databases) and data from other sources. Relevant data in this regard may include publicly available open source information, or more personal information obtained by law enforcement or intelligence agencies based on the powers established in the Investigatory Powers Act.

8. There are many types of predictive policing. For example, certain predictive technologies attempt to identify specific individuals. This may involve: predicting victims (those most likely to be victims of crime); predicting perpetrators (those most likely to be guilty of having committed a crime); or predicting future offenders (those most likely to commit crime in the future). Predicting future offenders can involve calculating and applying “threat scores” that assign labels (usually numerical digits or colour-codes) to individuals representing the likelihood that they will commit crimes. Threat scores are based on datasets populated with information such as: demographic information, personal data, an individual’s contact network, or an individual’s criminal history. A contemporary example of threat scoring is the Fresno California Police Departments’ use of Beware Software, which analyses publicly-available data to assign a colour-coded threat level to an individual previously identified as being of interest to the police.

9. Another type of predictive policing involves producing “crime maps” and predicting areas where crime is likely to occur in the future, also known as “hot spots.” A contemporary example of this type of predictive policing is the Los Angeles Police Department’s (‘LAPD’) use of PredPol software, which uses three data points (time, place, and type of crime) to identify likely hotspots. PredPol employs advanced algorithms capable of examining crime data and identifying hotspots at a speed that human crime analysts cannot. It is argued that its speed and accuracy mean that PredPol holds the potential to increase the efficiency of police work by allowing officers to quickly locate and pre-empt crime, resulting in a reduction in overall crime rates. By focusing on the geography of crime rather than details such as the demographics of victims or perpetrators, the designers of PredPol and other location-based predictive software claim that predictive policing avoids discriminating against members of certain groups.

10. PredPol is now used in several LAPD divisions (and over 60 other departments in the US), and predictive technologies are currently migrating to England and Wales. For example, Kent Police have adopted PredPol, and early studies suggest the software may have contributed to a 6% reduction in crime rates in North Kent. The

---

6 EMPOWER FIRST RESPONDERS WITH ENHANCED SITUATIONAL AWARENESS.’ West.com. Available at: https://www.west.com/safety-services/public-safety/powerdata/beware/
8 PredPol.com. Available at: www.predpol.com
9 PredPol.com Blog. 11 November 2015. Available at: www.predpol.com/ucla-predictive-policing-study/
10 PredPol.com. About Page. Available at: www.predpol.com/about/
Metropolitan Police Service in London have also trialled a predictive software developed by Accenture to predict gang associations and gang violence. Similar predictive technologies will be trialled in South Wales and Gwent Forces as part of a test of a virtual reality program known as “Gotham,” designed to help police analyse crime patterns.

11. Despite the potential benefits of predictive software, including their potential to reduce overall crime rates, existing research has identified significant risks that must be addressed. Three key risks are presented here for illustrative purposes.

Three Risks of Data Driven Policing and Predictive Software

12. Data Quality: The effectiveness of predictive software relies on the quality of input data. If the data that is analysed by predictive software is inaccurate, incomplete, or skewed, this will significantly affect the quality of predictions. For example, predictive algorithms based on deficient data may result in false positives (no crime in alleged “hot spots”) or false negatives (crimes in areas identified as low-risk). There are many reasons that data may be deficient, including a heightened emphasis on more visible forms of crime and disorder, whilst concealing others that are less visible. For example, some crimes are consistently under reported – in relation to both the type of crime, and the areas in which crimes are typically reported as occurring – meaning crime data is often incomplete and cannot provide algorithms with a quality representation of the actual recurrence of crimes in a space. Furthermore, police discretion introduces a level of subjectivity into the production of crime data, which may affect the quality of that data in terms of its depiction of crimes rates. Resulting crime data will present a skewed portrayal of the persistence crimes in a space and predictive software will be unable to accurately locate hot spots.

13. Discriminatory Capacities: Data driven policing and the use of predictive software can result in discriminatory outcomes. Despite police efforts to adopt an objective methodology, concerns about biased policing persist, particularly in terms of decision making about the locations in which police officers patrol. Evidence suggests that some police officers continue to target members of marginalised groups and impoverished neighbourhoods, if this approach is taken, crime data will falsely suggest that crime rates are particularly high in impoverished neighbourhoods, not because they are the locations where crime is most common, but because they are the locations in which police focus most of their patrols, overlooking similar crimes occurring in areas where there is limited police presence. Once this skewed data is introduced to predictive software, the software will most likely notice that crime data suggests that most crime takes place in impoverished neighbourhoods, and predict that

---

16 UKCrimeStats. Available at: www.ukcrimestats.com/AboutData/
18 Alan Travis. ‘Police crime figures losing official status over claims of fiddling.’ The Guardian. 15 January 2014. Available at: www.theguardian.com/uk-news/2014/jan/15/police-crime-figures-status-claims-fiddling
future crimes are likely to follow this pattern. Such predictions will funnel more police into already over-policed spaces, resulting in a self-fulfilling cycle in which the criminality of impoverished spaces is given priority by police, and crime data continues to suggest a correlation between impoverished spaces and crime. This self-fulfilling cycle is sometimes referred to as the ‘ratchet effect’ as it persistently narrows the criminal justice system’s focus on impoverished spaces.

14. Therefore, despite claims about the objectivity of algorithms, there is a risk that predictive software reinforces the targeting of impoverished spaces and the residents within these spaces, often racial and ethnic minorities. This conclusion is supported by studies in the United States including the Human Rights Data Analysis Group’s research finding that algorithms that are trained on biased input data tend to make predictions encouraging the police to focus on impoverished spaces. For instance, the study found that, when applied to Oakland Police Department’s data on drug crimes, the algorithm suggested police almost exclusively target lower income, minority neighbourhoods. Similarly a study by the RAND Corporation suggested racial and ethnic biases among the targets of police interventions persisted despite the implementation of predictive software that claimed to remove biases from the police’s decision making. A related consideration here is the degree to which any inaccuracies, or inbuilt biases, are reviewed and evaluated.

15. Privacy Harms: The use of data driven technologies requires the collection of large quantities of data. Mass data collection raises questions about the police’s contributions to bulk and indiscriminate surveillance. Despite the argument that surveillance in service of crime control should not concern those with ‘nothing to hide’, surveillance poses significant risks. Risks include violations of privacy rights through the mass surveillance of large numbers of citizens. Without privacy, citizens are left without a retreat from which to carry out unmonitored communication, thought, and self-expression. This may affect the functioning of democracy, or may result in a "chilling effect" based on the premise that citizens inhibit their behaviour (related to political opinion, sexuality, or religious belief for example) and conceal information (related to one’s health or political views for example) that, if publicised, could result in social exclusion and/or the denial of opportunities.

---

22 Matt Stroud. ‘The minority report: Chicago’s new police computer predicts crimes, but is it racist?’ The Verge. 19 February 2014. Available at: www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist


30 See, for example, Maximillian Schrems v. Data Protection Commissioner, Judgment, European Court of Justice, Case C-362/14, 6 October 2015, para. 33; Szabo and Vissy v. Hungary, Judgment, European Court of Human Rights, Application No. 37138/14, 12 January 2016, paras. 53–54;

31 See, for example, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others, Judgment, Grand Chamber, European Court of Justice, Cases C-203/15, C-698/15, 21 December 2016, paras. 93, 101; Perry v. the United Kingdom, Judgment, Grand Chamber, European Court of Human Rights, Application No. 63737/00, 17 July 2003, para. 36; Digital Rights Ireland, Judgment, European Court of Justice, Cases C-293/12 & C-594/12, 8 April 2014, para. 28.

32 See, for example, Zakharov v. Russia, Judgment, European Court of Human Rights, Application No. 47173/06, 4 December 2015, para. 232.


34 See, for example, Opinion of Advocate General Saugmandsgaard Oe, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others, European Court of Justice, Case Nos. C-213/15 & C-698/15, 19 July 2016, paras.
European Court of Human Rights has repeatedly highlighted the risk that ‘a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.’

**Recommendations: Regulation and Oversight**

16. The future demands and challenges of policing will depend on the police’s ability to address the opportunities and risks of data driven technologies, particularly those involved in predicting crime. Among the challenges faced by police is the need to simultaneously make effective use of data driven technologies to improve their ability to serve the safety and security expectations of the public, while addressing challenges related to the social implications of data driven technologies. Of particular concern is the fact that the risks identified with such policies bring into play legal requirements relating to, for example, the prohibition of discrimination, the right to privacy, and the right to freedom of expression.

17. Addressing these social and legal concerns will require the adoption of oversight and regulations facilitating independent assessment of crime data. It will also require the police to create systems and policies that ensure use of data driven technologies comply with human rights law and address concerns about the far-reaching and intrusive nature of mass surveillance. Accordingly, the Project recommends the creation of detailed oversight and regulation mechanisms with particular attention paid to if and how police address the limitations of crime data, and the discriminatory capacities and privacy harms related to the use of data driven technologies.

18. The Project has dedicated resources to an empirical case study exploring police organisations use of predictive and crime mapping technologies to determine how police organisations have addressed the risks discussed in this submission, and further oversight and regulatory mechanisms that may be required.

**Human Rights, Big Data and Technology Project**

University of Essex’s Human Rights Centre

---

257-259.


37 HRBDT website. Available at: www.hrbdt.ac.uk