

A FORCE FOR GOOD?

**Results from FOI requests on
artificial intelligence in the
police force**

WILL GRIMOND, ASHEEM SINGH
APRIL 2020

About the RSA

The RSA (Royal Society for the encouragement of Arts, Manufactures and Commerce) believes in a world where everyone is able to participate in creating a better future. Through our ideas, research and a 30,000 strong Fellowship we are a global community of proactive problem solvers, sharing powerful ideas, carrying out cutting-edge research and building networks and opportunities for people to collaborate, influence and demonstrate practical solutions to realise change.

The RSA has been at the forefront of social change for over 260 years. Today our work focuses on supporting innovation in three major areas; creative learning and development, public services and communities, and economy, enterprise and manufacturing.

About the Project

This short report is a project within the RSA's Tech and Society programme. It emerged in response to findings from the RSA's Forum for Ethical AI, which trials new approaches to public engagement with artificial intelligence, including in the criminal justice sector. For more from the RSA's Tech and Society programme please see [here](#).

Acknowledgements

The authors of this report would like to thank Ash Singleton, Jillian Linton and everyone in the RSA Tech and Society team for their support and input throughout the production of this report. All mistakes contained herein are our own.

Contents

Introduction and findings	3
Systems and their use	5
The culture of tech and policing	9
Reflections	12
Appendix 1: Methodology	15
Appendix 2: Responses in Full	16

Introduction and findings

For some time now, the use of artificial intelligence in policing has been shifting up the public consciousness. Whether it is live facial recognition at football matches in South Wales, using algorithms to forecast crime, or programs that recommend which prisoners should undergo rehabilitation, the intersection of AI and criminal justice is increasingly on the news agenda.

Despite this, comprehensive information on how police forces are using artificial intelligence is difficult to find: there is a perceived tension between the need to provide good, secure policing and public transparency on the methods deployed.

This paper begins that task: it is an exercise in understanding how police forces in the UK are communicating their use of AI and ADS.

Definitions

AI (artificial intelligence): the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence. An example of AI in policing is the algorithmic process that supports facial recognition technology.

ADS (automated decision systems): computer systems that either inform or make a decision on a course of action to pursue about an individual or business that may or may not involve AI. An example of ADS in policing would be where facial recognition technology alerts to wanted suspects in a crowd.

Our results present some cause for concern. Some of our concerns are operational, some are cultural. Through a series of freedom of information requests, we discovered that only a small minority of police forces were prepared to confirm to us whether they are using AI or ADS for policing decisions, and of these very few have offered public engagement.¹

We found:

1. Predictive policing and facial recognition remain the primary uses of these new technologies by our police forces.
2. However, these are often being used without sufficient public engagement.
3. This forms part of a wider difficulty in communicating how AI or ADS is being used by the police, and across our public services.
4. Police forces need stronger guidelines on the use of new technologies, along with greater support and oversight.

1. See Appendix II for the full breakdown of police force responses.

We recognise the demands placed on police forces and the considerable challenges they face. However, adopting new technologies without adequate cultural safeguards – especially around deliberation and transparency - risks storing up considerable problems for the future, around both community cohesion but also truly innovative technological uptake. In the spirit of moving the conversation forward, we posit some recommendations at the end of this piece.

This research took place prior to the lockdown of the UK in response to the Covid-19 pandemic. The playing field for law enforcement has shifted dramatically since then. The police have extensive new powers, deemed as necessary to limit one of the greatest public health crises in modern history. Policies may have been altered in this time, but we believe that adequate scrutiny, in particular of the use of new technologies, will be all the more necessary as we acclimatise to increasing police powers.

Systems and their use

1.1. Facial recognition technology

Facial recognition, as used in a policing context, is fast emerging as the new *bête noire* of rights campaigners. It involves capturing images of the public and comparing them against a database of suspects. This can be used in a ‘live’ setting, with individuals screened immediately and either detained or released, or with image-matching taking place after images have been captured. The latter has taken place in the UK since 2014, with recent scrutiny generally centred on the ‘live’ function of facial recognition. The Metropolitan Police and South Wales Police are the only forces overtly using live facial recognition technology (LFR).

Public attitudes towards the use of facial recognition are mixed. A 2019 report by the Ada Lovelace Institute found that 70 percent of the public were supportive of police use of the technology for criminal investigations, although 55 percent want it to be limited to specific circumstances.²

South Wales Police’s (SWP) facial recognition programme operates under constraints: images are not stored for more than 24 hours after being captured. SWP have a dedicated website for the programme, with FAQs, guidelines, and a record of each deployment. In spite of this, the force has faced criticism. Last year they won a court case regarding the use of LFR, brought against them on human rights grounds.³ In the summer of 2019, South Wales Police trialled a facial recognition system using officers’ smartphones, carried out with systems that can identify suspects with a single photograph.⁴

The Met trialled LFR in several London locations last year. The force has deemed these a success, even if they were reported negatively in some areas of the press, including a case where a man was fined after arguing with a police officer who insisted he show his face.⁵ Nevertheless, in January of 2020 they announced that the programme is to be rolled out in full, its use being “intelligence-led and deployed to specific locations in London”.⁶

2. Ada Lovelace Institute (2019) Beyond Face Value: Public Attitudes towards facial recognition technology [pdf] Ada Lovelace Institute. Available at: www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/

3. Rees, M. (2019) ‘South Wales Police use of facial recognition ruled lawful’ [online], BBC, 4 Sept. 2019., Available at: www.bbc.co.uk/news/uk-wales-49565287

4. The BBC (2019) ‘South Wales Police to use facial recognition app on phones’ [online] 7 Aug. 2019. Available at: www.bbc.co.uk/news/uk-wales-49261763

5. Metropolitan Police, 2020. *Met begins operational use of Live Facial Recognition (LFR) technology*. [press release] 24 Jan. 2020 Available at: news.met.police.uk/news/met-begins-operational-use-of-live-facial-recognition-lfr-technology-392451 and Burgess, M. (2019) ‘Inside the urgent battle to stop UK police using facial recognition’ BBC, 17 Jun. Available at: www.wired.co.uk/article/uk-police-facial-recognition

6. Ibid.

This move provoked further consternation from civil liberties and human rights groups.⁷ The programme began deployment the following month, being used in Westfield shopping centre in Stratford in February 2020.⁸

All territorial police forces have access to retrospective facial recognition through the Police National Database (PND), which contains millions of images of police suspects. Police forces can upload images to the database to find potential matches. Hampshire Constabulary and Thames Valley Police reported to us that they are currently using facial recognition, although they did not specify whether this was live or retrospective. As they referred to guidelines about using the PND, we suspect it is the latter. Durham Constabulary also mentioned use of the facial recognition element of the PND.

We were concerned by the relative unwillingness of forces to detail their use of retrospective facial recognition through the freedom of information process. This is a matter of public record; the Home Office has noted that all police forces use retrospective facial recognition as recently as September 2019.⁹ These two items taken together points, if not to a culture of quiet, then to a lack of understanding by police information offices about what facial recognition constitutes – they may for example have assumed that using ‘facial recognition’ only pertains to LFR.

1.2 Predictive policing

Predictive policing is the application of analytical techniques to identify locations or individuals at higher risk of criminal activity. Statistical methods of predicting crime precede the computer age, but it is only recently that the police have been able to harness and analyse large datasets in order to forecast crime, not least due to the proliferation of new technologies.¹⁰

Predictive policing relies on historical data on the nature, location and time of past crimes, with insights feeding into crime prevention strategies, such as where and when officers should patrol. It rests on the assumption that decisions made through such systems will result in crimes being tackled or resources used more effectively than with traditional approaches to law enforcement.

There is an obviously alluring science fiction quality to such systems; often however the reality can be more prosaic. West Midlands Police use a system, MapInfo Professional, which falls within certain definitions of predictive policing. This allows for the mapping the locations and dates of incidents, for the purpose of locating crime hotspots. Surrey Police use predictive policing in the form of crime pattern analysis, and trains data analysts in this area.

West Yorkshire Police is currently developing and trialling a predictive policing programme. The force is working with University College London to develop an algorithm to pre-empt areas of high crime (‘Patrol-Wise’). The

7. Amnesty International, 2020. *Met Police’s use of facial recognition technology ‘a huge threat to human rights.’* [press release] Available at: www.amnesty.org.uk/press-releases/uk-met-polices-use-facial-recognition-technology-huge-threat-human-rights

8. Murgia, M., ‘Met Police try to calm tensions as live facial recognition hits London’, *Financial Times*, [online] 12 Feb 2020. Available at: www.ft.com/content/db8bfc3c-4cf4-11ea-95a0-43d18ec715f5

9. Home Office (2019) *Fact Sheet on live facial recognition used by police.* [online] Available at: homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/

10. Perry, W., McInnis, B., Price, C., Smith, S., & Hollywood, J. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (p. 2). RAND Corporation.

rationale given was that they hoped to prioritise vulnerable parts of their jurisdiction and use resources efficiently. North Wales Police told us they are developing and testing predictive models, although they are yet to be deployed. These could cover “any area of force business”, including our prompts of crime pattern analysis and crime pattern analysis.

The space remains contested. A 2019 report from the Royal United Services Institute warned of the potential of such systems to skew the decision-making process and create systematic unfairness.¹¹ In the same year, a report on predictive policing by the campaign group Liberty flagged that it could lead to discriminatory patterns of policing.¹² Existing biases may be codified when historical data is used to predict future crime.

The potential for bias – especially against historically marginalised groups in high-crime areas – is logical and clear. New injustices may emerge too. Geospatial predictive algorithms could change the behaviour of police officers when patrolling areas identified as high-risk and lead to differential, possibly harmful policing practices across areas.¹³

Other forms of predictive policing focus on individuals rather than geography. Durham Constabulary operates a predictive system to assess individuals within the criminal justice system. The Harm Assessment Risk Tool (HART) maps individual risk factors and predicts the likelihood of individuals to reoffend. This data is then used to recommend whether the person concerned should be recommended for a rehabilitation scheme, known as Checkpoint, and does not influence further penal decisions.

Recent research on similar models in the US has suggested that algorithmic predictions of reoffending are slightly more accurate than those made by untrained individuals.¹⁴ This is in spite of evidence found of bias within these systems.¹⁵ Further research is necessary to gauge whether these systems are effective in a UK context.

At the beginning of 2019, Liberty reported that 14 police forces were using, planning to trial or had used predictive policing programs.¹⁶ Our data shows only 4 forces using predictive policing or similar systems, albeit with some yet to report.

The Liberty report looked at the broader and historical use of predictive

11. Babuta, A. and Oswald, M. (2019) Data Analytics and Algorithmic Bias in Policing [pdf] Royal United Services Institute, Available at: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

12. Couchman, H. (2019) *Policing by Machine* [pdf] Liberty. Available at: www.libertyhumanrights.org.uk/policy/report-policing-machine

13. Meijer, A. & Wessels, M. (2019) Predictive Policing: Review of Benefits and Drawbacks, *International Journal of Public Administration*, 42:12, 1031-1039, DOI: 10.1080/01900692.2019.1575664

14. Lin Z., Jung J., Goel S,* and Skeem J (2020) ‘The limits of human predictions of recidivism’, *Science Advances*, [online] Vol. 6 no. 7 Available through: advances.sciencemag.org/content/6/7/eaazo652

15. Angwin, J., Larson, J., Mattu, S., and Kirchner, L. (2016) ‘Machine Bias’, *ProPublica* [Online] May 23, 2016. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

16. Couchman, H. (2019) *Policing by Machine*

analytics in general rather than specifically through ADS or AI, and forces which use less sophisticated methods of prediction may not have been picked up in our survey.

However, we suspect, bar a recent change in strategy, some of those who do use these technologies may have not responded with information about their programs. Whether this difference in results suggests that predictive policing is on the wane, or whether it is because forces are changing how they report on this potentially problematic technology is difficult to ascertain.

1.3 Case assessment tools

New technologies are also being used to assess individual cases of crime. Kent Police use an ‘Evidence Based Investigation Tool’ (EBIT), in which an algorithm assesses cases on their apparent solvability. They told us that this is not a form of ADS, but their description of the program as “a separate IT application which uses evidence based solvability and public interest/vulnerability factors to determine whether a crime should be allocated, filed, or reviewed further” would suggest otherwise. This tool is currently limited to four types of crime, including assault and criminal damage. In early 2019 it was reported that this has resulted in a decline in cases being pursued, from 75 percent to 40 percent of all cases.¹⁷

The justification for the use of EBIT is that it allows resources to be allocated more efficiently, by reducing the volume of crime allocated for investigation and reducing the workload of supervisors.¹⁸ Kent Police are keen to stress that the system only provides advice to supervisors, who ultimately decide what crime is pursued.¹⁹

¹⁷. Howgego, J., ‘A UK police force is dropping tricky cases on advice of an algorithm’, *New Scientist*, 8 Jan. 2019, Available at: [newscientist.com/article/2189986-a-uk-police-force-is-dropping-tricky-cases-on-advice-of-an-algorithm/](https://www.newscientist.com/article/2189986-a-uk-police-force-is-dropping-tricky-cases-on-advice-of-an-algorithm/)

¹⁸. Kent Police Force (2018) Force Management Statement, [pdf] Kent: Kent Police Force. Available at: <https://www.kent.police.uk/SysSiteAssets/foi-media/kent/how-we-make-decisions/force-management-statement/force-management-statement-fms.pdf>

¹⁹. Ibid.

The culture of tech and policing

2.1 Public engagement

As we move from technological development being essentially about constraints on manufacturing, to being about technology's relationship to power, institutions and society, there is a conspicuous and concerning lack of public engagement around AI and ADS.

Of the police forces which confirmed that they are using AI or ADS for policing decisions, only South Wales Police replied with confirmation that they had consulted with the public on how they are using AI. Durham Constabulary did not respond with an answer regarding whether they had undertaken public engagement around the use of their HART system, although they have previously participated in an RSA-led deliberative body on the use of AI and ADS in policing, which largely focussed on Durham Constabulary as a case study.²⁰

The Met Police have stated that they are planning a programme of public engagement around deployments, although the detail of this has not yet been outlined in full. Their guidelines for the use of live facial recognition states that before and after deployment, "It may be appropriate to pursue engagement opportunities with a number of stakeholders, including MOPAC [The Mayor's Office for Policing and Crime], local authorities, and public consultative or ethical review bodies."²¹ This guidance makes public consultation an optional extra rather than an integral part of the deployment process. A follow-up request returned in early March 2020 (and therefore after deployment had begun) found that the Met had no written record of any such engagement taking place. Kent Police gave a similar answer, replying that public engagement regarding their EBIT system had not taken place, but "could do so" in the future.

This is aside from historical failures to publicise the use of AI or engage with the public on the use of LFR by UK police forces. While South Yorkshire Police are not currently using the technology, in early 2018 they collaborated with Meadowhall shopping centre in Sheffield to deploy LFR without informing the public or putting up signs. This was criticised by the Surveillance Camera Commissioner.²²

20. The RSA, *Democratising decisions about technology: A toolkit* (2019) p. 39, Available at: www.thersa.org/discover/publications-and-articles/reports/democratising-decisions-technology-toolkit

21. Metropolitan Police Service (2020) 'MPS LFR Guidance Document', Metropolitan Police Service. Available at: www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mpf-lfr-guidance-document-v1-0.pdf

22. White, G. and Clifton, H. (2020) 'Meadowhall facial recognition scheme troubles watchdog' BBC, 28 Jan. Available at: www.bbc.co.uk/news/technology-51268093

Public engagement is crucial when deciding whether to deploy ADS in public services. Aside from allowing the end users of these services to voice their concerns, public engagement is an educational process for both sides and a necessary recognition that the issues are more than just operational in nature. These technologies and their myriad uses are alien to much of the public – in 2018 RSA research found that just nine percent of the public are aware that AI is being used in criminal justice.²³ Consultation needs to have real consequences: feedback must be considered seriously and acted upon.

The RSA's recent report from the Forum for Ethical AI highlighted three core benefits of engaging the public on technology: insights, trust and governance. Deliberative engagement can produce new perspectives on how technology is perceived and used. Educating the public can improve buy-in and therefore trust. Public engagement can also inform governance structures and give legitimacy to regulatory or policy decisions.²⁴

Notably, none of the forces deploying or planning to deploy predictive policing systems confirmed to us that they had consulted with the public. One information office we contacted linked this to the fact that as their predictive policing programme only mapped crime data, rather than suspects or intelligence, public consultation was not necessary, the implication being that as the system tracked trends rather than individuals it was not necessary to input public voice.²⁵

This lack of public engagement demonstrates a concerning lack of awareness regarding attitudes towards how personal data is being deployed by public agencies. The absence of public consultation, we fear, will serve to further distance the public from decisions made using these broadly unfamiliar technologies. A new cultural framework is required to shift these entrenched attitudes.

2.2 Cultures of innovation are generally at risk

This is not limited to the police per se: rather it is an example of how government generally is failing to adapt to the uptake of new and radical technologies. A consistent theme across this investigation was the inconsistency and paucity of information provided by police forces regarding how they are using AI. This is not just in regards to our specific requests – the information provided to the public online and to the media is often also insufficient.

There is a lack of openness and communication around the use of new technologies across the public sector. The Committee on Standards in Public Life has recently called for improved transparency in the use of AI by public sector bodies, recommending that guidelines be established around declaring and disclosing how these technologies are being deployed. The report found that 51 percent of people were more comfortable with decisions being made through AI if it came with an

23. The RSA, *Artificial Intelligence: Real Public Engagement* (2018) p. 25, Available at: www.thersa.org/discover/publications-and-articles/reports/democratising-decisions-technology-toolkit

24. The RSA, *Democratising decisions about technology: A toolkit* (2019)

25. Correspondence on 30 January 2020 with West Yorkshire Police

easy-to-understand explanation for why it had taken place.²⁶

There were significant difficulties in receiving responses from some police forces. Under the rules laid out by the Information Commissioner's Office, organisations have 20 working days to reply to an FOI, and can only spend a set amount of staff hours on each request. In one instance we were given only a partial response by a force which uses ADS "because there is no central point of contact [on AI or ADS]" and "the only way to determine this information would be to approach every single department and unit within the force" and therefore exceed the maximum cost for an FOI.²⁷ 5 police forces are still working on their reply, 5 months and several follow-ups after the original request.

2.3 More than guidelines needed

A majority of AI-using police forces told us that they offer guidelines to their staff, but there is little consistency in the guidelines which are being provided, and information on how police officers are being trained on the use of AI is even more scarce. Some police forces referred us to the guidelines for using the Police National Database. These are more focussed on GDPR-compliance and information-sharing than educating staff on specific issues around AI. Guidelines are also drawn from other sources, such as academia.²⁸

This issue has been previously highlighted by the Information Commissioner's Office (ICO), regarding the use of live facial recognition. In a response to the South Wales Police court case, the ICO commissioner released a statement calling for "a statutory and binding code of practice, issued by government, [which] should seek to address the specific issues arising from police use of LFR and, where possible, other new biometrics technologies."²⁹ Without this, the police risk further undermining public confidence in the use of LFR. The ICO also warned that as more police forces trial these technologies without adequate guidelines, the likelihood of compliance failures will increase.³⁰

26. Committee on Standards in Public Life, (2020) 'Artificial Intelligence and Public Standards', Committee on Standards in Public Life. Available at: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/863657/AI_and_Public_Standards_Web_Version.PDF

27. West Midlands Police freedom of information response, received 22nd of November 2019.

28. North Wales Police, for instance, is using an ethical framework based on the 'Algo-care model', outlined in Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455

29. Information Commissioner's Office (2019) 'Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places', Information Commissioner's Office. Available at: ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

30. Ibid.

Reflections

This paper is intended as a building block for further research into the use of AI or ADS by police forces.

One of our overriding concerns comes from the use of artificial intelligence as a means of increasing the efficiency of policing rather than the quality of it: new technologies must be used responsibly, and for the purposes of improving police work rather than simply as a cost-cutting measure. This was directly cited as a reason for developing these systems by at least one respondent.³¹ The worry here is that artificial intelligence systems allow for cost-saving which decreases the availability of less-measurable benefits of policing, such as relationship and community building. There is also a danger that efficiency gains may be misleading or can produce unintended consequences.³² Racial and gender biases can be exacerbated by technologies as they are based on historic data, and we fear that a lack of transparency could undermine the principle of policing-by-consent. This chimes with concerns raised in other areas of our research, such as the use of new technologies in healthcare.³³

A 2019 report by Deloitte found that police chiefs are in fact very confident that they are doing enough to engage the public on policing issues in general, but that confidence in their forces' ability to adopt new technologies is lacking. The same report also found that very few forces are using deliberative methods.³⁴ In 2017 a trial of deliberative methods took place across 7 policing districts, with over 250 participants. Those who participated came out with a greater understanding of complexity within police work, and the experiment showed that the deliberative process can produce different results to traditional methods of engagement, such as surveys.³⁵

The RSA has a toolkit for building-in public engagement to the procurement process for ADS in public services. *Democratising Decisions About Technology*, released in October 2019, outlines a model of citizen engagement centred around a deliberative process. Participants are educated on the issues around the use of a certain technology before

31. Correspondence with West Yorkshire Police 30/01 2020

32. See Babuta, A. and Oswald, M. (2018) *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* [pdf] Royal United Services Institute, Available at: rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf

33. A. Singh (2019) *Patient AI: Towards a human-centred culture of technological innovation in the NHS* [pdf] The RSA. Available at: www.thersa.org/globalassets/reports/2019/patient-ai-report.pdf

34. Deloitte (2018) *Policing 4.0: How 20,000 officers can transform UK* [pdf] p. 23 Deloitte Touche Tohmatsu Ltd. Available at: www2.deloitte.com/uk/en/pages/public-sector/articles/the-future-of-policing.html

35. The Police Foundation (2017) *Understanding the public's priorities for policing* [pdf] The Police Foundation. Available at: www.police-foundation.org.uk/2017/wp-content/uploads/2017/10/understanding-public-priorities-final.pdf

being encouraged to discuss and debate the issues. The criminal justice leg of this ‘citizens’ jury’ surfaced interesting insights into the use of individual risk assessment programmes and facial recognition.

New technologies will only be used effectively and responsibly by keeping a ‘human in the loop’ – AI must have real human oversight from beginning to end, providing continuous feedback and modification. Deliberative methods could provide a bridge from the machinations of predictive policing and facial recognition to the end users who are impacted by their decisions. The importance of a ‘human in the loop’ approach was highlighted by participants when our citizens’ jury discussed AI and policing.³⁶

We are interested in exploring how deliberative methods can be further applied to deal with the deficit in engagement identified in this report. We note that engagement is a broad term that is best satisfied when diverse, multidisciplinary groups come together and challenge the complex social, philosophical and practical issues around these technologies.

3.1 Further work

This report is just a starting point. A difficulty encountered during this investigation was mapping how covert surveillance is being used. Almost every police force replied with exemptions under Section 24(2) and Section 31(3) of the Freedom of Information Act, which cover national security and law enforcement respectively, stating that they cannot state whether covert surveillance is occurring within their jurisdictions. A typical response was:

“Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of facial recognition would lead to an increase of harm to covert investigations and compromise law enforcement.

...It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.”³⁷

As such there is no way of mapping a full picture of how facial recognition is being used by police in the UK. The use of covert surveillance is regulated but only publicised selectively. It is also unclear how much communication there is between national security bodies, such as MI5 and Government Communications Headquarters, and local police forces regarding the use of AI in their jurisdictions. Secrecy over the extent of these services’ use of surveillance has been challenged by privacy campaigners and they faced criticism from then-home secretary Sajid Javid over compliance issues related to surveillance in 2019.³⁸

A further under-reported issue is the use of facial recognition and other technologies in the private sector.

36. The RSA, *Democratising Decisions About Technology*, p. 42

37. Correspondence with West Mercia Police, 28th January 2020

38. Bond, D. (2019) ‘MI5 probed over potential data compliance breaches’, *The Financial Times* [online] www.ft.com/content/865914a0-7646-11e9-be7d-6d846537acab

Numerous police websites suggest that private businesses should install CCTV with facial recognition software for security purposes.³⁹ Research into this issue might look more closely at how private organisations in the UK are handling data drawn from these systems, how this is contributing to police and security work, and levels of public knowledge and engagement about these practices. As facial recognition technology and other forms of AI and ADS become cheaper and higher-quality, we can expect their use to further proliferate across various areas of public life.

39. For instance, see Hampshire Constabulary (www.hampshire.police.uk/cp/crime-prevention/business-robbery/protect-your-business/) and West Mercia (www.westmercia.police.uk/cp/crime-prevention/business-robbery/protect-your-business/)

Appendix I: Methodology

In November 2019, we asked every territorial police force in the UK a series of questions via Freedom of Information Requests (FOI):

- Whether they were using AI or ADS to make policing decisions, and for what;
- If so, whether they were offering training and/or guidelines to their staff on how to use these technologies;
- Whether they had engaged with the public on their use of AI or ADS.

At the time of publication, 40 out of 45 territorial police forces have responded. All information in this report was correct at the time of receipt, between the end of November 2019 and March 2020.

We asked police forces whether they are using AI or ADS currently, but some police forces voluntarily offered information about plans for deployment in the future, or uses of AI in the past. As such, we only have information about those presently using AI or ADS in police work. Where necessary we have updated the record using other sources.

Appendix II: Responses in full

7 police forces responded to our initial request that they are currently using or trialling AI and/or ADS for policing decisions: **Durham Constabulary, Hampshire Constabulary, Kent Police, South Wales Police, Surrey Police, Thames Valley Police, and West Yorkshire Police.** The Met responded in mid-January that they were not at that time using AI or ADS for policing decisions, a week prior to their announcement regarding the full deployment of LFR, bringing the tally to 8.

Durham Constabulary, Surrey Police and West Yorkshire Police are using systems for predictive policing. West Midlands Police use a geospatial crime mapping software, MapInfo, which bears strong similarities to predictive policing systems and influences police deployments. North Wales Police responded that they are currently developing a predictive policing system, and Kent Police is using an ADS for case assessment. Northern Ireland responded that they are using robotic process automation to automate some stages of granting firearms licenses, and Kent Police stated that they are using a similar technology for administrative purposes regarding road traffic collisions. All other forces answered 'no' or 'no information held'.

We do not have a full picture of who is developing or planning to develop AI use in future. For some this may be a relatively distant aspiration - Police Scotland have for instance highlighted the use of AI in Policing 2026, which in 2016 set out policing priorities for the decade ahead.⁴⁰

Hampshire Constabulary, Kent Police, North Wales Police, South Wales Police, Surrey Police, Thames Valley Police, West Midlands Police and West Yorkshire Police confirmed to us that they were providing training, and all of these, other than Surrey Police, confirmed that they offer guidelines for staff.

Only South Wales Police confirmed in their response that they have offered public engagement, with the Met suggesting plans to do so in a separate statement after our request, although they could not provide evidence of this in a follow-up freedom of information request. Durham did not answer this question, disputing what 'policing decisions' might involve and not responding to further questions. Previous RSA work with Durham suggests that some level of public engagement has been carried out. West Midlands Police could not answer in full due to cost constraints.

The extent of the use of AI or ADS is further made opaque by what we see as a perceived misunderstanding by police's information offices on the

40. Police Scotland (2017) *Policing 2026* [online] Available at: www.scotland.police.uk/assets/pdf/138327/386688/policing-2026-strategy.pdf

use of facial recognition through the Police National Database. All police forces have access to this, but it appears that almost all responses we received (other than Hampshire Constabulary, Thames Valley Police and Durham Constabulary) gave no indication that this was in use.

At the time of publication, we have not had responses from Northamptonshire Police, North Yorkshire Police, Nottinghamshire Police, Sussex Police or Warwickshire Police. Each of these have had far longer than the 20 working day limit in which to respond, with requests sent out at the beginning of November. Each of these forces gave receipt of our request.

The RSA (Royal Society for the encouragement of Arts, Manufactures and Commerce) believes in a world where everyone is able to participate in creating a better future. Through our ideas, research and a 30,000 strong Fellowship we are a global community of proactive problem solvers. Uniting people and ideas to resolve the challenges of our time.



8 John Adam Street
London WC2N 6EZ
+44 (0)20 7930 5115

Registered as a charity
in England and Wales
no. 212424

Copyright © RSA 2020

www.thersa.org
