Committee(s): Police Authority Board Professional Standards and Integrity Committee	**Date(s):** 6th October 2020 26th November 2020
Subject: Use of Algorithms and AI within City of London Police	**Public**
Report of: Commissioner of Police Pol 69-20	**For Information**
Report author: Gary Brailsford-Hart Director of Information (CISO & DPO)	

Summary

The police service continues to attract the attention of the media in respect of how it uses technology to fulfil its policing purposes. Most notably the use of advanced technology such as analytical algorithms, artificial intelligence (AI) and facial recognition. Specifically, attention has been drawn to how Action Fraud makes use of technology in determining suitability for investigation.

This report provides a response to the instruction from the September Police Authority Board in relation to reporting on the use of algorithms and artificial intelligence across the City of London Police.

Recommendation

Members are asked to:

- Note the report.

Main Report

Background

1. At the September Police Authority Board a member query was escalated to the Chairman regarding the use of algorithms by Action Fraud in determining which cases are progressed for investigation and its compatibility with Article 22 (automated individual decision-making, including profiling) of the General Data Protection Regulation (GDPR). An instruction was therefore given to produce a report on this specific question and was expanded to include details of any systems in use across the force making use of algorithms and/or artificial intelligence in automated decision making.

2. It is important to clarify and differentiate the use of algorithms from artificial intelligence. Algorithms take an input applies mathematics and logic to produce the output. Artificial Intelligence Algorithms take inputs and outputs simultaneously to learn the data and produce outputs. Therefore an algorithm defines the process through which a decision is made, and artificial intelligence uses training data to make such a decision.

3. The City of London Police is a Competent Authority for the purpose of Part 3 of the UK Data Protection Act (DPA) and is therefore exempt from the General Data Protection Regulations where the processing of personal Data is for the purpose of Law Enforcement. Article 22 of the GDPR does not therefore apply. However, Section 49, a similar provision, exists within Part 3 of the DPA.

Current Position

4. Under article 37 of GDPR the Force is required to appoint a Data Protection Officer (DPO). This post carries a number of statutory responsibilities including the requirement to be independent and report to the highest management level. The Force has appointed an officer of sufficient seniority with direct access to the Chief Officer team and is involved in all aspects of data management and decision making across the force, including the consideration of new and emergent technology.

5. Nearly all force systems make use of algorithms, for example the crime system makes use of automated record expiration in accordance with the Management of Police Information, a set of standard instructions and conditions forming the input and the record being marked for disposal is the output. Even though these algorithms produce outputs to assist the volume and complexity of police and corporate systems they are not automated in their decision making, they merely present the output to an operator who will then make a decision or perform a task.

6. A recent review of Action Fraud business process has been conducted by the Office of the DPO in the determination of the extent to which automated decision making is taking place and whether or not further action is required.

7. The findings of this review highlighted that whilst the capability exists within the solution to automatically determine a prioritisation of fraud reports through the use of algorithms these are not currently used (due to errors within the software) to determine whether or not a case is suitable for dissemination to a partner organisation for investigation. At this time the Action Fraud process produces datasets that are then reviewed by a dedicated team of analysts for development of cases and possible dissemination. Due to the volume of reports, many will not be selected for inclusion in the dataset. Although this is a partly manual process, once the criteria have been set, reports are selected without further human intervention and this meets the definition contained in DPA section 49(1): *A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.*

8. The use of automated decision making has to be authorised by law, but this doesn't mean that there has to be a law which explicitly states that solely automated decision-making is authorised for a particular purpose. The Data Protection Act refers only to a decision which is 'required or authorised by law' (Chapter 2, Part 2, Section 14 (3)(b)).

9. As we have statutory and common law power to detect and investigate crime, and if we determine that automated decision-making/profiling is the most appropriate way to achieve this purpose, then we are able to justify this type of processing as authorised by law and rely on Article 22(2)(b). However we must be able to show that it's reasonable to do so in all the circumstances.

10. Policing activity is extensively regulated and it is reasonable to conclude that the processing is lawful.

11. The Office of the DPO has established safeguards within the organisation to ensure that any processing of information is fully considered and in accordance with the Data Protection Act and applied GDPR. A Data Protection Impact Assessment (DPIA) (Appendix 2) is conducted where any new processing is taking place and every DPIA is subject to review and approval by the DPO, any high risk processing is identified through this process and the DPO will raise any concerns directly with the Chief Officer team or the Information Commissioners Office if appropriate.

12. In addition to the DPIA, the Office of the DPO is introducing a Data Ethics Framework (Appendix 3) to ensure that processing is considered on ethical grounds as well as legislative compliance. The process is currently in the early stages of implementation but is considered a necessary approach to support future technical, procedural and analytical ambitions.

13. The force does not currently make use of artificial intelligence (AI) in any of its operational systems. However, it is anticipated that AI will become more mainstream in the technical systems being deployed to assist policing and we would be naïve to not ensure we are able to lawfully and ethically exploit this technology to ensure we are effective in protecting the public. By contrast we are already seeing criminals using AI to commit crime unhindered by geographic boundaries or regulation.

14. National Policing and Government are developing frameworks to support the Police in the use and exploitation of technology in contentious areas, such as data analytics and facial recognition. However, although the production of such frameworks will guide the implementation of those technologies they will still be subject to the established data protection regime across the City of London Police.

Conclusion

15. The use of algorithms in the automated decision making by Action Fraud is proportionate, necessary and lawful. There are sufficient safeguards in place to ensure that information is being processed in accordance with the Data Protection Act 2018.

16. The use of algorithms across the Force is common place but are relatively simple operators and are not used for any significant decision making. Therefore it is not considered relevant for data protection act purposes.

17. Although artificial intelligence is not currently in use, the Force will be seeking opportunities to enhance our policing capabilities in accordance with the pace and demands of modern policing ensuring this is undertaken in a lawful, ethical and timely manner.

Appendices

- Appendix 1 – UK Data Protection Act 2018 considerations
- Appendix 2 – CoLP Data Protection Impact Assessment Template
- Appendix 3 – CoLP Data Ethics Framework Template

Gary Brailsford-Hart
Director of Information (CISO & DPO)

T: 0207 601 2352
E: gary.brailsford@cityoflondon.pnn.police.uk