Summary

1. With regard to the terms of reference for this inquiry, I would offer some recommendations as follows, with a particular focus in relation to the algorithmic analysis of police intelligence:
   - There should be the introduction of a single statutory oversight body and regulator for the use of police databases and algorithmic analysis in criminal justice – independent from the Home Office, police forces, and other policing policy bodies such as the National Police Chiefs’ Council, with statutory powers of audit, investigation and regulation of emerging police intelligence and algorithmic analysis technologies.
   - A new statutory framework entailing a police intelligence regulator is needed to address the problems inherent in determining models of proportionate intelligence retention and (where appropriate) deletion; allowing for both individual challenge and the systematic removal of data from police intelligence databases.
   - A national regulator could act as a national approval body, with the proportionate deployment of police algorithmic intelligence analysis technologies/software or techniques entailing pre-approval by such a body.
   - Strong safeguards are needed around the use of algorithmic analysis of police intelligence that drew on ‘personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation’.
   - Law or policy must ensure a statutory national regulatory body maintaining suitably transparent and detailed records of police usage of algorithmic intelligence analysis, which would be lodged with the body.
   - Law or policy must facilitate the issue of individual complaints to this statutory national regulatory body.

Introduction

3. I am a Senior Lecturer in Law at Sheffield Hallam University, and an active researcher in the Helena Kennedy Centre for International Justice. My published research to date focuses on aspects of privacy law, personal information and human rights, specifically in the policing and criminal justice context.

4. My focus in responding to this call for written evidence for the inquiry into algorithms in decision-making is on the use of algorithmic analysis of police intelligence and other ‘criminality information’. My research into this field has been conducted with my fellow research Marion Oswald, of the University of Winchester.

5. Our published research on police use of intelligence analysis (including algorithmic techniques), and in particular the privacy law issues relating to these growing police practices, can be cited as follows, and is freely available for the Committee to examine, using the hyperlinks provided here, below:
Written evidence submitted by Jamie Grace, Senior Lecturer in Law,
Sheffield Hallam University (ALG0003)


- J. Grace and Oswald, M. "'Being on our radar does not necessarily mean being under our microscope": The Regulation and Retention of Police Intelligence", (2016) 22(1) *European Journal of Current Legal Issues* (online at: http://webjcli.org/article/view/441/621)

Written evidence

6. The use of algorithmic analysis of police intelligence is growing, and there could be considerable investment in these technologies in the near future by police forces in the UK, due to the potential power of ‘predictive policing’ techniques, drawing on decision-making using algorithmic intelligence analysis.

7. There are concerns that police use of algorithmic intelligence analysis may amplify biases or discrimination, and as such police use of algorithms must be subject to structures providing for independent oversight and challenge, both in terms of possible restrictions on the deployment of particular software in contexts across geographical areas or policing operations as a whole, and also, on a micro-level, in relation to individual cases where a person objects to the impact and interference with their personal privacy.

8. There are means by which algorithmic decision-making can be conducted in a transparent and accountable way, as follows:

   i) There should be the introduction of a single statutory oversight body and regulator for the use of police databases and algorithmic analysis in criminal justice – independent from the Home Office, police forces, and other policing policy bodies such as the National Police Chiefs’ Council, with statutory powers of audit, investigation and regulation of emerging police intelligence and algorithmic analysis technologies.

   ii) A new statutory framework entailing a police intelligence regulator would need to address the problems inherent in determining models of proportionate intelligence retention and (where appropriate) deletion; allowing for both potential individual challenge and the systematic, necessary removal of data from police intelligence databases.

   iii) A national regulator could act as a national approval body, with the proportionate deployment of police algorithmic intelligence analysis technologies/software or techniques entailing pre-approval by such a body.

9. The EU General Data Protection Regulation 2016 does not apply to algorithmic analysis in the policing and criminal justice context, and the UK government is unlikely to opt-in to the relevant substantive provisions of the Police and Criminal Justice Data Protection Directive 2016 (and in particular the safeguards in Articles 10, 11, 24 and 52 of the Directive (see Appendix A, below)), instead likely preferring the approach of allowing continuing regulation through the Data Protection Act 1998 – but this is not to say that UK domestic law and/or policy could not afford individuals a commensurate level
Written evidence submitted by Jamie Grace, Senior Lecturer in Law, Sheffield Hallam University (ALG0003)

of protection from abuse or misuse of algorithmic analysis in the policing and criminal justice context. On a practical level, this would entail, in relation to police algorithmic intelligence analysis usage:

i) strong safeguards around the use of algorithmic analysis of police intelligence that drew on personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation;

ii) maintaining suitably transparent and detailed records of police usage of algorithmic intelligence analysis, which would be lodged with a statutory national regulatory body

iii) facilitating the issue of individual complaints to this statutory national regulatory body

February 2017

Appendix A – Key Articles of the Police and Criminal Justice Data Protection Directive 2016

Article 10

Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;
(b) to protect the vital interests of the data subject or of another natural person; or
(c) where such processing relates to data which are manifestly made public by the data subject.

Article 11

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.
Written evidence submitted by Jamie Grace, Senior Lecturer in Law, Sheffield Hallam University (ALG0003)

Article 24

Records of processing activities

1. Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(d) a description of the categories of data subject and of the categories of personal data;

(e) where applicable, the use of profiling...

Article 52

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.

3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.