Algorithmic policing and freedom of information – how far should transparency extend?

Marion Oswald

Algorithmic transparency is the new watchword – from the UK Parliament's Science and Technology Committee (House of Commons Science and Technology Committee, 2016), to the European Data Protection Supervisor (EDPS, 2016) and even Angela Merkel (Connolly, 2016). With the current controversies over fake news online, the spotlight has fallen mainly on the private sector - internet platforms, search engines, social media - but for how long?

The operational deployment of algorithmic tools (computational methods that analyse data sets in order to draw conclusions, increase knowledge and make links) within the U.S. criminal justice system has provoked considerable debate. Third party proprietary systems used for parole and sentencing decisions have been accused of hardwiring discrimination into the system (ProPublica, 2016) and raise issues of natural justice and procedural fairness (Oswald & Grace, 2016).

Predictive database-driven tools for offender management in the probation and prison contexts have been used in the UK for several years (NAMS, 2015). However, the extent to which algorithmic tools have been adopted within UK policing for investigative operations and intelligence analysis appears to vary significantly between forces and be less than transparent. For instance, a search on Kent Police's website for predictive policing tool 'PredPol' brings up no results, despite coverage of the force's deployment of the algorithmic technology in the UK press (see for instance O'Donoghue, 2016).

My freedom of information-based study (with Jamie Grace, Sheffield Hallam) into algorithmic analysis of police *intelligence* in the UK (Oswald & Grace, 2016) suggested that a relatively small number of forces were using computational or algorithmic *intelligence* analysis. Although, due to the limitation of such studies, this is unlikely to represent a complete perspective, the results may still give support to James's conclusion in October's blog (James, 2016) that the institution is 'failing to make the best use of its intelligence' and so is 'not working smart enough.'

Responses from UK police forces to our freedom of information request indicated that algorithmic tools were used both at the 'macro' level – for instance, assessing crime patterns – and at the 'micro' level such as for decision-making or risk assessment relating to individuals. Detail was lacking however, with no details as to the specific crimes, activities, schemes or laws that were the focus of the tools. For instance, it would not be possible to determine from the responses whether the tools were used to assist decisions pursuant to the preventative disclosure schemes 'Clare's Law' and 'Sarah's Law'. The reasons for using such technology were expressed in general terms, and the exemptions under the UK's Freedom of Information Act engaged by many forces may disguise other uses of such tools, or, importantly, gaps in operational capability.

In response to our freedom of information request, thirty-two responses used some form of exemption. Twenty-seven responses cited the Section 23 absolute exemption: 'Information supplied by, or relating to, bodies dealing with security matters' - MI5, MI6, GCHQ and so on - outnumbering the use of the Section 31 exemption (Law enforcement) cited by only five responses. The Section 31 exemption was combined with the Section 23 exemption four out of the five times that Section 31 was used. Section 23 was most often cited on its own rather than being combined with other exemptions.

Most (although not all) responses that cited Section 23 combined it with ‘neither confirm nor deny’ wording, which should be used when either confirming or denying would reveal exempt information in itself. Section 31 is a qualified exemption, requiring the public body to engage in a public interest balancing exercise to decide whether or not to release the requested information. There were considerable inconsistencies in the way that forces handled this balancing exercise, with some forces providing rather generic arguments either way, and one providing only a bland statement that a test had been completed.

So what can we take from this? The inconsistent use of FOI exemptions may allow sensitive information to be inadvertently exposed or gaps in capability inferred, which could be damaging to law enforcement and national security interests. However, if one thing can be learned from the debate surrounding the Investigatory Powers Bill, it is that the adoption of new technology by the State without appropriate transparency around methods can result in damage to public trust as well as legal challenge.

Operational details and methods must be protected. Yet balanced transparency is also vital. Examples of such balanced transparency exist, for example in Canada, where, while a detailed understanding of the Violent Crime Linkage System (ViCLAS) 'is quite rightly not in the public domain due to investigative sensitivities - but official, clear, easy to find information on what the system is, who can use it, how to go about access and related research *is available*' (Dawson and Stanko, 2016).

The Investigatory Powers Bill is in itself an example (in some eyes a flawed one) of an attempt to achieve balanced transparency and oversight. As the use of algorithmic tools within UK policing appears to be at a fairly early stage, now would seem to be the right time to assess the legal underpinning and the governance framework, and to ensure that appropriate transparency is built into contracts with third party software suppliers. Such an exercise may help to demonstrate the effectiveness of these tools, as well as increasing public trust and so could contribute towards James’s call for the institution to make the best use of its intelligence.

Marion Oswald is a Senior Fellow in Law, and Head of the Centre of Information Rights at the University of Winchester, and a solicitor (non-practising). Email: marion.oswald@winchester.ac.uk.
@_UoWCIR @IRPandPJournal