

Chief Constables' Council

Title: Digital Ethics Proposal

7 October 2020

Security Classification NPCC Policy: Documents <u>cannot</u> be accepted or ratified without a security classification (Protective Marking may assist in assessing whether exemptions to FOIA <u>may</u> apply): OFFICIAL	
Freedom of information (FOI) This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with you on receipt of a request prior to any disclosure. For external Public Authorities in receipt of an FOI, please consult with sherry.traquair@npcc.pnn.police.uk	
Author:	DCC David Lewis
Force/Organisation:	Dorset Police
Date Created:	02/09/2020
Coordination Committee:	Workforce
Portfolio:	Ethics
Attachments:	App A
Information Governance & Security In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this paper is strictly on a need to know basis and in compliance with other security controls and legislative obligations. If you require any advice, please contact npcc.foi.request@cru.pnn.police.uk https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework/risk-management	

1. INTRODUCTION/PURPOSE

- 1.1. This paper briefly outlines some of the challenges for policing in using technology, particularly artificial intelligence and algorithms, and the importance of being seen to do so in an ethical way.
- 1.2. The paper proposes next steps in ensuring ethical accountability for our use of technology and seeks the support of Chief Constables' Council in exploring the options outlined.

2. BACKGROUND

- 2.1. The evolving complexity of crime today is significant and the entrepreneurial nature of criminals means that they are able to adapt swiftly to changes in society and technology.
- 2.2. There are huge potential benefits to policing in the use of technology, from the use of algorithms in our processes, through digital investigations, to facial recognition. These clearly have the potential to accelerate investigations, make our processes more efficient and allow us to invest freed-up resources in crime fighting. However, if we stand still technology and criminality will advance and we will be left behind.
- 2.3. Whilst it is clear that the use of technology by the police can reduce the likelihood of victims being harmed by crime, there is an absence of clarity from policing about what well-governed and proportionate use of technology looks like.
- 2.4. Consequently the most heard voices in the digital debate are often those of civil rights organisations. The most controversial and eye-catching initiatives – e.g. Facial Recognition – are the most debated, yet least understood, by the public and media. A number of other important issues are not widely discussed and we could do more to establish a sense of policing being a trusted force for good in the



use of technology whilst being open to public scrutiny. This goes to the heart of our legitimacy and establishing public confidence in police use of new technologies.

- 2.5. Notwithstanding these caveats there have been a number of helpful contributions from authoritative sources (or it may be that the volume and complexity of material exacerbates the problem). Broadly summarised they suggest that policing requires a clearly codified, coordinated and transparently governed approach. Appendix A contains a number of sources for those who wish to read more deeply into the issue.
- 2.6. The focus of this paper relates to digital ethics, and it may be useful to distinguish between (at least) four sub-categories: 1) Biometrics; 2) Digital Forensics; 3) Surveillance and Investigatory Powers; and 4) AI (Artificial Intelligence) and Algorithms. All of these have different ownership, governance and legal frameworks, although from a policing perspective it is often difficult to clearly separate them. That said, the main focus of our work going forward seems likely to be around AI and Algorithms, where the biggest gap exists, but there will inevitably be overlap with the other three categories.
- 2.7. In terms of stakeholders the landscape is cluttered. A variety of NPCC Coordinating Committees and portfolios are involved, notably Crime Operations, IMORCC, and Professional Standards and Ethics. Many regulators have a stake in the debate, including the Information Commissioner, the soon-to-be-established Biometrics and Surveillance Camera Commissioner, the Investigatory Powers Commissioner and the Forensic Science Regulator. Other oversight includes HMICFRS and the IOPC. OPCCs have played important roles, including MOPAC's London Policing Ethics Panel and the West Midlands OPCC's Ethics Committee, but have not yet developed a coordinated response. The Home Office are exploring digital ethics and already have a Biometrics and Forensics Ethics Group, whilst the College of Policing is developing its position. An Independent Digital Ethics Panel for Policing exists, but is struggling for support and resources, and the West Midlands OPCC are proposing options to develop their well-regarded Ethics Committee into the national sphere. The Portfolio has also engaged with industry to explore good practice already developed elsewhere and is running an engagement event with TechUK.

3. PROPOSAL

3.1. PROPOSED AREAS FOR ACTION

- 3.1.1 Given all the above it is evident that the landscape needs some clarity and coordination. At present the portfolio has identified four areas, plus 1, that would benefit from focused and coordinated activity. They are to:
- 3.1.2 **Catalogue and maintain an up to date record of police use of technology.** It is suggested that this is limited to a manageable scope and that high profile measures, such as the use of facial recognition technology and the use of algorithms to inform decision-making, could form the initial basis of this activity.
- 3.1.3 **Develop new national guidelines for police use of data analytics.** The College of Policing are key partners in this respect and are keen to work alongside the Portfolio. This would be a positive outcome and we are already working with the College to explore opportunities. Likewise, possibilities exist in other spheres, such as industry and other public sector bodies, to adapt good practice.
- 3.1.4 **Re-establish an independent digital ethics committee.** This will provide independent ethical monitoring, scrutiny and oversight as well as a place to debate dilemmas. There are options, as mentioned above, but whatever happens this body will need to be given an authoritative independent status, will need to recruit high quality participants with the requisite expertise and will also require resourcing. Consideration should be given to the volume of work that might be placed on such a body and whether local arrangements, with an escalation process, should be put in place.
- 3.1.5 **Coordinate a communications response to the challenges of the use of technology, data and AI.** It is important to have prominent positive voices making the case for a trusted police service which is using technology transparently to deliver safer communities and fight crime. It is proposed that a series of

interventions are coordinated and a clear response is put in place in the public debate about police use of technology. Led by the NPCC this would involve the College of Policing, Home Office and APCC, as well as other stakeholders.

- 3.1.6 **Plus 1. Educate and equip police leaders in their understanding of the use of digital technology.** External observers tend to agree that we do not as a collective have a thorough or deep appreciation of the opportunities that the use of tech provides. Whilst not the preserve of the Ethics Portfolio per se, it is obvious that a lot of the success of these proposals hinges on the professional knowledge and capabilities of leaders in this area. The Portfolio is happy to work alongside NPCC leads and the College in developing this as an opportunity.

3.2. COORDINATION COMMITTEE APPROVAL

- 3.2.1. We have been consulting widely for some time, speaking to the various organisations referenced earlier in the report, and have built a body of support for the proposed approach. The Ethics Portfolio sits within the Professional Standards and Ethics Portfolio, working to the Workforce Coordination Committee. Having been supported there, we have also engaged the Crime Operations and IMORCC Committees, who have also both backed progression of the work outlined in this paper.

3.3. STATEMENT/DETAILS OF COST OR RESOURCE IMPLICATIONS

- 3.3.1. There is clearly a potential cost implication in developing this work. However, as yet it is not yet clear what financial support may be sought from forces, if any. Negotiations are continuing with the Home Office, College of Policing, APCC and potential academic partners. Options outside of the use of forces' budgets are being sought. No shared NPCC resources will be committed to the work without the approval of Chiefs' Council.
- 3.3.2. It is clear however that partners are keen to know that there is a mandate from the NPCC about the direction of travel, and it would be an important step to secure the support of Chiefs' Council in order to move forward.

4. CONCLUSION

- 4.1. The police service has embarked on a journey to gain public trust and confidence in its use of new technologies, but has not yet arrived. Transparent, well-structured governance and a strong, positive policing voice is required. This paper outlines a proposal for the next steps to take us there.

5. DECISIONS REQUIRED

- 5.1. Chief Constables' Council is asked to support the work described at 3.1, so that the Portfolio can bring back stakeholder-supported progress and a concrete proposal to a future meeting.

David Lewis
Deputy Chief Constable
NPCC Lead for Ethics