

National Law Enforcement Data Programme:

Developing and implementing the ethical use of LEDS

Discussion Document

Draft Final

08 September 2018

This Document has been written with the aim of stimulating discussion on the impact of Data Quality on ethical use of data. It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to Law Enforcement Governance bodies and Civil Society Organisations for reflection.

NLEDP - Non Paper

1. According to the Department of Digital, Culture, Media and Sport, data ethics is an emerging branch of applied ethics which describes the value judgements and approaches we make when generating, analysing and disseminating data.

This includes a sound knowledge of data protection law and other relevant legislation, and the appropriate use of new technologies. It requires a holistic approach incorporating good practice in computing techniques, ethics and information assurance.

2. A Eurobarometer survey of data protection (June 2015) showed that over 80% of respondents had concerns that authorities and private companies holding information about them, may sometimes use it for a different purpose than the one it was collected for. This coupled with the recent data breaches within central government and criminal justice sectors has created a perfect storm in which the collection and use of policing data is under greater scrutiny than ever.
3. This brief paper has been written to consider the ethical issues that face policing in relation to the creation and acquisition and use of data in an operational context. This paper also acknowledges the complex information management landscape in which policing operates and the challenges that this creates; these are exceptional times:

- **Legislation**

Multiple legislation, regulation and policy govern how policing manages and uses data (Police & Criminal Evidence Act (PACE), Criminal Procedure & Investigations Act (CPIA), Management of Police Information (MoPI), Data Protection, Protection of Freedoms Act etc). It is the aggregation of this legislation which creates the complexity – made more so by the Inquiries Act and the two ongoing public inquiries (Undercover Policing Inquiry (UCPI) and the Independent Inquiry into Child Sexual Abuse (IICSA). Does policing truly understand the purpose for which data is collected and how that data can be used, shared and managed?

- **Exponential growth in data both in volume and platforms**

Policing now collects data via: body worn cameras, drones, mobile telephones are computers and hold vast amounts of data; the internet of things and the internet of thinking mean we are dealing with increasingly intelligent environments on which data sits, yet policing has not developed similarly intelligent environments on which to manage data.

- **ICT transformation**

Presents an opportunity – policing should start to build data quality considerations at the concept stage and use technology to support high quality data at the point of creation.

- **Increased scrutiny**

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

Parliamentary regulators (information, biometrics, surveillance camera and forensics) have expressed concerns in the way in which the service is using and managing data.

- **Public trust and confidence**
The service polices by consent and this must include the way in which data is collected, managed and used.
4. Data has long been recognised as an asset, but only if it is treated as such. Data “treated badly” creates risk, both for the organisation that holds the data and the individual to which the data relates.
 5. By its very nature policing data contains some of the most sensitive data about people. These people may be offenders, suspects, victims or witnesses and in many cases, may be known to policing in more than one capacity. Policing will hold crime, intelligence, safeguarding, public protection, incident information from the point at which a call for service is received through to any criminal justice outcome and beyond.
 6. For policing to maximise the benefits of data it must accurately reflect the POLE (Person, Object, Location, Event) entity to which it relates. It is at the point of creation that ethics and data quality are most closely aligned, and it is at this point that the risks of poor data become clear. Data that is not accurate will not be connected, will not be accessible and will result in negative outcomes for both the citizen and policing.
 7. GDPR requires organisations to put in place appropriate technical and organisational measures to implement data protection principles and safeguard individuals’ rights. This concept is not new, but as a legal requirement it now rightfully raises the bar. However, privacy cannot be guaranteed by technology alone, alongside a compliance mentality there needs to be a more ethical approach - policing using data in accordance with core values.
 8. These values could come from the College of Policing “Code of Ethics”. This code sets and defines the exemplary standards of behaviour for everyone who works in policing – accountability, honesty, integrity, leadership, objectivity, openness, respect and selflessness.
 9. Technology makes the exploitation of data possible, our legal and regulatory framework allows us to collect data and specifies the purpose (some might argue more than policing actually needs), but ethics will determine whether “it is the right thing to do”. How this is woven into the fabric of policing needs to be considered in order for the service to maximise the operational benefits of data lawfully and ethically. In summary, values, coupled with technical data standards and a clear understanding of the law.

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

10. What does policing therefore need to do to be considered a data driven, ethical service?
- a. Understand the policing purpose for creating/acquiring data and the rationale for continued retention
 - b. Understand and embed the rights of the individual into technology and processes
 - c. Develop a Data Ethics Strategy underpinned by the Code of Ethics
 - d. Address organisational attitudes and behaviours that foster poor data – tackling the root causes
 - e. Agreed national data standards – ensuring that data has the same prominence in innovation as technology
 - f. Consistently share data nationally in accordance with standards and values

Key Questions:

- 1. How can NLEDP ensure that the aggregation of the PNC and the PND does not increase the risk of individuals' rights being compromised?**
- 2. How can policing weave data ethics into the College of Policing "Code of Ethics"?**
- 3. As policing collects more data, how do we manage and monitor the technologies available to exploit this data, what governance is required to maintain an ethical approach?**
- 4. How do we engage with the public to ensure that they understand what data is held, how it is used and how it is managed – without jeopardising core policing tactics?**