Tuesday 3rd July Open Space Workshop Write Up

1. Contents 1
2. Actions from the Workshop 2
3. Summary & Introduction 4
4. The Space 5
   - 4.1. Principles of Working Together
   - 4.2. The Scope of the Process
5. Identifying & Prioritising Issue Areas 7
   - 5.1. Automated Processing
   - 5.2. Retention of Custody Images
   - 5.3. Data Sharing
   - 5.4. Security, Audit & Access Controls
   - 5.5. Oversight, Inspection & Governance
   - 5.6. Code of Practice
   - 5.7. Other Issues
   - 5.8. Sources of Further Information
6. Next Steps & Actions 13
   - 6.1. Who else is needed in the room?
7. Conclusion 13
8. Appendix 14

2. ACTIONS FROM THE WORKSHOP

Actions	Responsibility
Action 1: Home Office (HO) to arrange demonstration of the high level architecture and prototype for new system for civil society organisations (CSOs).	HO & CSOs
Action 2: Involve & HO to link up with Aerospace Defence Security Space (ADS) process.	HO & Involve
Action 3: HO to clarify level of accuracy of Data through the new Data Quality Dashboard and to share the Data Quality definitions. These will feed into the Data Protection Impact Assessment (DPIA).	HO
Action 4: HO to look into how new system will impact officer decision-making and therefore training.	HO
Action 5: To avoid the possibility of discussions in the Open Space being derailed at a late stage the HO to engage with relevant non-CSO actors early to avoid those last minute amendments.	HO
Action 6: HO to add headline issues to the timelines that are being discussed with law enforcement organisations and any other organisations and circulate to CSOs.	HO
Action 7: HO committed to giving early warning to this space if Automatic Facial Recognition (AFR) and other areas are due to become part of Law Enforcement Data System (LEDS).	HO
Action 8: Involve to follow up with Defence Lawyers & Law Enforcement organisations.	Involve
Action 9: Ensure governance of LEDS is a key topic in workshop 4 covering future service/capability & future engagement on this area too and will be threaded throughout the other workshops	HO & Involve
Action 10: HO to share law enforcement mission statements with CSOs.	HO
Action 11: HO to share with CSOs list of competent authorities they are discussing LEDS with before next workshop and explain levels of access for those on the list.	HO
Action 12: HO to share with CSOs a list of business services accessible through LEDS before next workshop.	HO

Action 13: HO committed to providing provocation paper on data sharing in LEDS, including but not limited to the types of data shared and sharing of data with 3rd parties.	HO
Action 14: HO confirmed they will provide visual representation of system to CSOs.	HO
Action 15: HO confirmed that they will provide progress document to detail timeframes on the whole programme.	HO
Action 16: HO to share prioritised list of operational impact assessments for new LEDS data sets and capabilities.	HO
Action 17: HO need to check how they can share data types but will review and follow up.	HO
Action 18: HO to share outputs with CSOs from other impact assessment discussions.	HO
Action 19: Share "who else needs to be in the room?" criteria for CSOs to review & feedback on.	Involve & CSOs
Action 20: Share slides with attendees.	Involve

3. Summary & Introduction

The following paper is a write up from the first workshop for the Home Office Open Space process facilitated by Involve.

This process aims to bring together CSOs and HO representatives for constructive conversations around future plans for the National Law Enforcement Data Programme (NLEDP).

This meeting note captures the areas of the process road map which were sketched out and agreed to at the meeting that need to be covered throughout this work. The note is not intended as a complete record of all discussions held at the workshop, however, where specific decisions and actions about the process were committed to, these have been included.

We are aware of the length of this document but felt it important to capture the actions and context in detail. To this end, we will also be sharing the full slide pack from the workshop and photos of each flip chart page of notes if needed for reference. There are summaries of each section throughout the note for those with less time as well.

The workshop set up the space in which this process will work. This included principles of working, the scope of the process and touched on who was missing from the room.[1] The session also discussed the recently published Privacy Impact Assessment (PIA) for the new LEDS at the heart of this process. This led onto discussions to prioritise key areas and issues that this space needs to tackle. Those will feed into a revised Data Protection Impact Assessment (DPIA) to be consulted on more widely. The workshop was concluded by a summary of next steps and actions.

A brief introduction to the process was provided by Involve and [redacted] Director of Policy on Data & Identity at the Home Office.

Questions and actions/responses arising from this section are outlined below:

Discussion/Questions	*Response/Actions*
• What level of technical detail will be covered about the system?	**Action 1**: HO to arrange demonstration of the new system.
• Is the ADS process still on going?	**Action 2**: Involve & HO to link up with this process.
• How accurate will the data be in LEDS?	**Action 3:** HO to clarify level of accuracy of data in DPIA.
• Impact of LEDS on training of officers.	**Action 4:** HO to look into how new system will impact officer decision-making and therefore training.

[1] This will be followed up in detail with CSOs as explained later in the notes.

4. THE SPACE

4.1. Principles of working together

There was general support from participants for the proposed principles of working together. After a brief discussion, a few amendments were raised and discussed as a group. The detail and actions from this discussion are outlined below and the updated Principles of Working Together are in Appendix A:

Discussion/Questions	*Response/Actions*
• Maintain Confidentiality: What is public knowledge and what isn't? Need to make this clear in the Principles. Confidential documents shared with CSOs need to be released into the public domain at some point.	HO response: if a document is in the public domain then HO welcomes comments/feedback as normal if an organisation has more to add.
• Agree to Disagree: CSOs asked to know how high does support go in the HO/government? CSOs requested that no statements are made about their involvement without their sign off – how to make future references to the work will be covered in workshop 3.	
• New Principle suggested of "No Surprises". CSOs stated that they have had previous experiences where changes to legislation/decisions were made last minute that contradict whole process and asked for this not to be repeated.	**Action 5:** HO engaging with non-CSO actors early too to avoid last minute amendments.
• What degree of understanding can be shared with CSOs about conversations with law enforcement organisations?	**Action 6:** HO to add headline issues to the timeline that are being discussed with law enforcement and any other relevant organisations such as the Disclosure and Barring Service, Her Majesty's Inspectorate of Constabulary (HMICFRS) and circulate to CSOs.
• Highlighted by CSOs that if they require increased technical knowledge at any point, it is the HO's responsibility to bring that information to the CSOs.	

4.2. The Scope of the Process

This section of the workshop outlined for participants the scope of the process from the HO. These two principles were introduced to guide participants as to when something is beyond the remit of this process:

- The data/capability is not accessible through LEDS
- The policy is not within the gift of NLEDP to change

Several organisations asked for more information on new data sources not currently due to be in/accessed by LEDS and explained their organisations need to raise these areas if the sources are likely to be included in the near future. Some CSOs also explained their need to make a marker for their organisation by raising certain issues on areas near the edge of the scope if particularly relevant for their organisations.

The HO confirmed they want a comfortable space where pressing issues (out of scope) can still be raised. The HO offered to link up CSOs with the correct colleagues for relevant conversations in these areas where possible.

Overall there was agreement and understanding of the need for the scoping guidelines but general acknowledgement in the room of the thin line between what is in scope and what isn't which raised several further questions. These questions are captured along with commitments and actions for participants around the remit of this process as follows:

Discussion/Questions	*Response/Actions*
• HO explained that the programme still needs to do prioritising of data/capability that may/may not be in LEDS.	**Action 7:** HO committed to giving early warning to this space if AFR and other areas are due to become part of LEDS. [HO has confirmed AFR is not in the scope of LEDS]
• HO need to be transparent on legitimate requirements placed on them re. capabilities of LEDS – when these become clear.	
• What are the ramifications of use of AWS?	Ramifications of the use of AWS will be discussed in conversations informing the next DPIA.
• Who else should be involved in this process?	**Action 8**: Involve to follow up with Defence Lawyers & Law Enforcement organisations.
• CSOs requested discussion on where mission creep exists and that this process could allow for discussion on how HO decides what's in and out of LEDS going forward.	
• Discussion also had around ethical basis HO makes decisions on. Some CSOs stated that for them to assess the privacy impact, they need to know HO ethical basis for making decisions and requested to discuss this in detail during this process. Request from CSOs for a clear HO definition of "ethics", "law" and "human rights".	**See Action 9**.

• Technical session needed at workshops to provide insight/confidence with new system. • What happens after 9 months? Will the Code of Practice cover this? How does this impact on red lines?	**See Action 1**. **Action 9:** Ensure governance of LEDS is a key topic in workshop 4 covering future service/capability & future engagement on this area too and will be threaded throughout the other workshops.

5. Identifying & Prioritising Issue Areas

As a starting point for uncovering the key areas that will shape this process, a conversation was held on the 2018 Privacy Impact Assessment (PIA). The HO provided context and background to the PIA which had been shared with CSOs prior to the workshop.

The HO welcomed questions from those present and invited further detailed responses to the PIA following the workshop if organisations wanted to. However, the conversations at the workshop will still feed into the HO thinking and development for the next DPIA if organisations have limited time and resource for submitting detailed responses later.

A detailed account of the questions and answers on the PIA specifically, with actions noted and attributed where required, is below:

Discussion/Questions	*Response/Actions*
• What's the timeframe for written submissions on the PIA?	Responses within a month to feed into next workshop is preferred.
• The focus of the PIA seems to be on preventing crime & safeguarding the public instead of tackling crime – is this intentional or just stylistic?	HO confirmed this comes out more in mission statements – just stylistic and the DPIA will have a broader focus. **Action 10:** HO to share law enforcement mission statements with CSOs.
• Can the HO provide a list of competent authorities they are discussing LEDS with and highlight who will have access to LEDS?	**Action 11:** HO to share list with CSOs before next workshop and explain levels of access for those on the list.

• Will the HO be talking to driving organisations, for example, as a non-police user of LEDS?	**Action 12:** HO to share with CSOs a list of business services accessible through LEDS before next workshop.
• Is data still being shared with credit brokers? Why and will it be in future?	HO response: This is done to stop credit going to people buying stolen vehicles. List of stolen vehicles is released. **Action 13:** HO committed to providing provocation paper on data sharing in LEDS, including but not limited to the types of data shared and sharing of data with 3rd parties.
• Why does DVLA need to be updated regularly with extracts from the PNC?	HO clarified this is due to technical constraints but it is moving to new infrastructure.
• Systematic disclosure of data to 3rd parties – can this be discussed for next DPIA?	**See Action 13.**
• CSO raised concerns that what had been flagged previously, hasn't been addressed so finding it still difficult to understand how privacy risks are decided on by the HO. Asked what substantive changes have been made to PIA since December meeting? CSOs questioned value of future involvement and explained they will struggle to justify involvement if don't see changes implemented more quickly.	HO acknowledged the delays in publishing the PIA and that they have been in mobilisation phase for a very long time. Until now been focused on building relationships for the process. Now into delivery phase.
• CSOs requested that retention needs to be addressed again – does data due to be deleted need to go over to LEDS?	HO explained this is all being discussed still.
• CSOs requested a visual representation of the system and levels of access and overlap.	**Action 14:** HO confirmed they will provide visual representation of system to CSOs.
• CSOs asked the HO to be clear on timeframes for the whole programme and when CSOs will get chance to review changes. CSOs asked for a document tracking where the process has got to and what's changed to be shared regularly with CSOs.	**Action 15:** HO confirmed that they will provide this progress document to detail timeframes on the whole programme.
• CSOs asked for operational impact assessments of prioritised use cases i.e. how the potential future use of LEDS will assist the law enforcement case.	**Action 16:** HO to share prioritised list of operational impact assessments.

• CSOs requested clear list of data types from PNC/PND that will go across to LEDS. • CSOs asked if it is just the DPIA or will there be other impact assessments?	**Action 17:** HO need to review how they can share data types but will review and follow up. HO confirmed they will work with ethics committees on what's proposed for LEDS too. **Action 18:** HO to share outputs from these discussions with CSOs.

A number of issue areas were identified from the PIA by attendees requiring further discussion which were the following:

Automated Processing
Retention of Custody Images
Data Sharing
Security, Audit & Access Controls
Oversight, Inspection & Governance
Code of Practice
Facial Search Functionality
Public Understanding
Recording
Accuracy
Re-classification of data/LEDS on other Devices
Security - External

This list was prioritised with the top six in the list highlighted as those to focus discussions on first. Attendees were invited to discuss as many of these that were relevant for their organisation in more detail at six stations around the room. Outlined below are the key questions and overall themes that arose from those discussions.

5.1. Automated Processing

Key Questions/Themes

The discussions here focused on needing more information around the processes that will be automated. The below themes can be drawn out:

- Evaluation – what is the purpose of this processing and what is trying to be achieved? How will the necessity and proportionality of these processes be assessed?
- Technical detail – what kind of process/capability will the system have? What's the approval process for new functionality?
  - Discrimination & bias: how will the system be tested? How is the algorithm scrutinised?
  - What data analytics will be used?
- Human intervention – will there be human oversight?
  - Deletion regime & automated processing: can manual intervention refine the automated process? What are the rules around exceptions for deletion?

5.2. Retention of Custody Images

This area of discussion again focused on the need for more detail being required to inform further discussion. There was general agreement that retention of custody images needs to be considered but it was also acknowledged that retention in the wider context of the system needs to be addressed. Themes for these future discussions were:

Key Questions/Themes

- Deletion – process, timings & auditing.
- Retention policy – differentiation between data types, justification for retention, alignment with other retention regimes.
- Data controller – who has ownership of data and policy?
- Principles of retention.
- Transparency – could awareness of data use help explain retention/deletion policies, annual report from the system? Victims' data use?
- Sanctions – implications for failure to comply?

5.3. Data Sharing

Conversations at this station touched on the need to consider data sharing impact at a local, national and international level (or internal and external to the UK). The principle areas that were raised for further consideration were:

Key Questions/Themes

- Location of data sharing – internal or external to UK?
- Data protection rules – exempted? Data controller?

- Sanctions & liability – consequences of breaches, liability around data sharing capability.
- Regulation & oversight – auditing of data usage & sharing, security assurances, safeguards & controls.
- Proportionality – assess necessity of data shared.
- Access – maintenance, 3rd party access (contractors & LGAs), levels of access.
- Transparency.

5.4. Security, Audit & Access Controls

There were concerns raised under this area predominantly around access functionality and a need to see who and how people will access the system and what mitigating factors will be included to increase security. A full list of the issues discussed are as follows:

Key Questions/Themes

- Security standards – cyber security standards.
- Responsibility – by who? Internal &/or external audit?
- Security breaches – increasing risk due to increased points of access, prevention, mitigating noble cause corruption.
- Access controls – technical detail, efficacy? Process for future changes?
- Audit trail – process of logging? Technical expertise in audit?

5.5. Oversight, Inspection & Governance

Around this area, discussions concentrated on making suggestions for how the governance and accountability of the system could/should look. Key ideas included:

Key Questions/Themes

- Statutory – will there be Parliamentary oversight? Annual report to Parliament?
- Regulation – need for strong regulator. Will there be judicial oversight?
- Remit – the need to avoid mission creep.
- Exceptions – what happens in individual challenges to key aspects of the system?
- Sanctions – what will these look like? How will data loss/breaches/hacking be dealt with?
- Key Principles – to guide governance & oversight.

5.6. Code of Practice

There was general consensus that this area underpins and runs through the rest of the issue areas. It was concluded that recommendations from all issue areas need to then feed into the Code of Practice throughout this process.

5.7. Other Issues

The following other issue areas referred to at the beginning of this section were also explored in a plenary discussion:

Facial Search Functionality
Public Understanding
Recording
Accuracy
Re-classification of data/LEDS on other Devices
Security - External

Key Questions/Themes

Key themes that came from this discussion, and from further questioning on anything missing from the issues discussion, brought out the following areas not previously highlighted:

- Value of data – different biometric data stored in different ways.
- Legality – legal basis for holding data?
- Public understanding – how will the public be informed about the system?
- Terminology – clarity around “criminal record” requested by CSOs.
- Accuracy – how can accuracy of data in the system be ensured?
- Re-classification of data – clarification needed around process & impact.
- Data minimisation – vulnerability of big data sets, privacy & security by design?
- Privacy definition/understanding – the HO noted the case needs to be made further about this issue internally. Conversations then centred on how CSOs can help HO build understanding of privacy discussion and tangible impacts on people.
- Policy issues – context of policy issues feeding into/affecting system now and in future.

5.8. Sources of Further Information

During the session focussed on the issue areas arising from the PIA, attendees were asked to recommend sources where the HO could find further information and detail to dig deeper into each issue area. These are listed in Appendix B.

The issue areas and sources of further information highlighted above will now form the basis of the future workshops within this process. Additional elements will be brought in as and when required by participants as well as the outcomes from each workshop informing the next. However, Involve and the HO will build the process going forward around these areas to directly inform the development of the DPIA 2019. The actions and commitments outlined throughout the whole of this note will be brought into the next three workshops too.

6. Next Steps & Actions

The workshop concluded with a summary of next steps and actions presented by the Home Office. This summary is outlined below:

- Additional relevant information and documentation to be provided to CSOs before the next workshop.
- Acknowledged CSO desire for clarification of lawful basis of activity.
- Security concerns around LEDS on multiple devices.
- Overlap with other policy areas/concerns – request for HO to link these up.
- Recognised desire for faster forward momentum for the programme.
- Acknowledged CSO request for Parliamentary and judicial oversight of LEDS.
- Confirmed options paper will be provided on custody image deletion.
- Will look at Investigatory Powers Commissioner's Office (IPCO) as a model for LEDS oversight.
- Acknowledged importance of transparency & justification for organisations that have access to LEDS.
- HO to share timeline for taking decisions & highlight when they can share info with CSOs.
- HO to set up demonstration day of prototype for the new system & how it will be used by police.
- HO reflected on the need to demonstrate how they take impact of rights and privacy in to real consideration.
- Justice to share recent report as a good example/model.
- CSOs stated that the value of the process rests on HO bringing substantially different/detailed information and demonstrating progress. HO to provide list of themes where there is expected to be progress so CSOs can decide if they should be involved.

6.1. Who else is needed in the room?

Before closing the workshop, we heard from [redacted], a serving police officer seconded into the NPCC to support HO to work on this programme. His Team, Operational Communications in Policing, represents Policing interests in relation to LEDS working to convey policing views and requirements to the programme and acting as the Business Change function for Policing in its readiness to adopt LEDS. [redacted] explained his interest and willingness to be involved in this process.

There had originally been plans to have a final section of the workshop which was aimed to invite attendees to review and feedback on the criteria for inviting additional participants to this process. This will be picked up after the workshop as there wasn't sufficient time at the workshop to do this effectively.

Action 19: Involve will share the criteria with attendees as a Google Doc to provide an opportunity for suggestions of types and specific names of organisations that should be in the room.

7. Conclusion

Involve and the HO ended the day by thanking everyone for their time and efforts to join us for the start of this work. An evaluation form for the workshop was shared to gather suggestions and feedback to help improve this process further going forward.

8. APPENDIX

8.1. Appendix A - Principles of Working Together

All participants agree to…

- **Open collaboration:** engaging constructively in the process within the shared purpose of the process. In cases of significant disagreement, Involve will play a mediation role.
- **Engage early:** providing information, data and papers in good time, and identifying significant challenges and blocks as early as possible.
- **No surprises:** HO to engage with non-CSO actors as early as possible to prevent last minute amendments that could either contradict the whole process or bring substantive new issues in with little time for effective engagement. CSOs to raise issues and questions early to avoid last minute change requests that could create delays.
- **Agree to disagree:** not expect consensus on every issue, and to accept conclusions as long as all parties are acting in good faith. No public statements to be made by any participants about the process and those involved without sign off from those they are referring to.
- **Maintain confidentiality:** talking about the process and broad discussions as required without identifying individual positions or publishing confidential or embargoed material. HO to only share documents with CSOs that will be (if not already) released into the public domain.
- **Focus on the process:** engaging on issues of relevance for LEDS inside the process, engaging on wider issues and policies outside it.
- **Promote accessibility:** identifying and proposing the involvement of participants with a legitimate interest and expertise to engage.

8.2. Appendix B – Sources of Further Information

Automated Processing

- Equality & Human Rights Commission
- Big Data & Human Rights Team: [redacted]

Retention of Custody Images

- Fingerprint & DNA retention judgements
- Non-automated deletion models as exemplars
- Victims' Rights charities

[redacted]

- Gaughran – ECHR judgment on Custody Images
- S64A (4) PACE

Data Sharing

- Internal & External:
  - Other government departments
  - LEAs
  - 3rd Parties/Public

Security, Audit & Access Controls

- 2018 DPA

Oversight, Inspection & Governance

- ICO
- Biometrics Commissioner
- BFEG – Biometrics & Forensics Ethics Group
- IPCO – Civil Liberties Panel

Other Issues

- Link in with work by [redacted], LEDS Data Quality and Data Management Lead on “freshness of data” for accuracy
- Rights based approach
- EU court rulings