LEDS & HOB OPEN SPACE WORKSHOP WRITE UP - TUESDAY 14TH MAY 2019

CONTENTS

INTRODUCTION

The fifth workshop in the Law Enforcement Data Service (LEDS) and Home Office Biometrics (HOB) Open Space process with civil society organisations was delivered on 14th May 2019. This write up covers the discussion areas from the workshop which included:

- reviewing previous Open Space actions and progress to date;
- an update on the National Law Enforcement Data Programme (NLEDP);
- discussion around next steps for a proposed Open Space Annual Report and review of the Open Space terms of reference;
- update and discussion around the drafting of the LEDS Code of Practice;
- review of plans for the next LEDS Data Protection Impact Assessment (DPIA);
- update on progress of the custody image review and;
- discussion on the granular detail of the HOB programme and its current Privacy Impact Assessments (PIAs).

The workshop was facilitated by Involve and attended by a variety of civil society organisations, Home Office officials, England & Wales Policing and a representative from the Biometrics Commissioner's Office.

Summary of Workshop Actions

#	Action	Owner	Deadline	Status	When from?
35.	HO to provide summary of all industry consultation that has happened and is planned around LEDS to provide more clarity to existing Action 35.	[redacted]	July 19	**Not started**	Created in July 18 and updated in May 19 asking for more detail.
112.	Involve check with other CSOs not in the room that they are happy for the Annual Report to happen and check what involvement they would want. Involve will follow-up with participants individually to confirm their position.	[redacted]	June 19	**In progress**	May 19
113.	HO to share definition of official and sensitive information with CSOs to determine what materials from the Open Space can be shared in the Annual Report.	[redacted]	June 19	**Not started**	May 19
114.	HO to confirm if all information included in papers is publicly available and where it is publicly available. This will determine whether an Annual Report can be produced or not. Involve to share these identified places for this information with CSOs.	[redacted]	June 19	**Not started**	May 19
115.	HO to produce public summary of programme to go in Annual Report.	[redacted]	July 19	**Not started**	May 19
116.	Involve to lead on the drafting process for the first Annual Report if all dependency factors raised in the Write Up are met.	[redacted]	Sep 19	**Not started**	May 19
117.	[redacted] to speak to [redacted] from [redacted] re. ESMCP.	[redacted]	July 19	**In progress - Meeting arranged for July**	May 19
118.	Involve to schedule yearly review, during the May workshop, of what is in/out of scope of the Open Space.	[redacted]	May 2020	**Not started**	May 19
119.	Explore pulling in ICO & other statutory organisations to give them responsibilities in the Code of Practice – check these are part of statutory responsibilities.	[redacted]	July 19	**Not started**	May 19
120.	HO to consider including what bad practice is in the Code of Practice.	[redacted]	July 19	**Not started**	May 19
121.	HO to confirm when Open Space can next see Code and public section of the document specifically. HO to confirm if it's possible to see it before it goes out to public consultation.	[redacted]	July 19 – before next workshop	**Not started**	May 19
122.	HO to produce and share "language of LEDS" document.	[redacted]	July 19 – before next	**Not started**	May 19

			workshop		
123.	HO to carry out further consultation with judicial services on the Code and explore how judges would interpret the Code.	[redacted]	July 19	**Not started**	May 19
124.	HO to send a link to the current system Technical Document that is available online.	[redacted]	June 19	**Not started**	May 19
125.	HO to explore role of how the Open Space will be involved in the data sharing process and confirm this before the next Open Space. Artefact 1 covers some of this.	[redacted]	June 19	**Not started**	May 19
126.	HO to confirm if Open Space can involve local data controllers to help understand different paths being taken?	[redacted]	Sep 19	**Not started**	May 19
127.	HO to clarify answer to the question of whether a private facial image company could get a data sharing agreement with a local force, therefore by-passing the HO and their data sharing agreements?	[redacted]	Sep 19	**Not started**	May 19
128.	HO to share information on buckets of data and criteria using for deletion of custody images.	[redacted]	July 19	**Not started**	May 19
129.	HO to update on progress of custody image review process and legislation and governance around this.	[redacted]	June 19	**Not started**	May 19
130.	HO to confirm number of images that could be deleted through proposed process.	[redacted]	July 19	**Not started**	May 19
131.	HO to update on process for how slightly higher risk images will be deleted when HO get closer to migration.	[redacted]	July 19	**Not started**	May 19
132.	HO to provide update on why deletion will be based on risk and not on custody status in interim update on custody image review.	[redacted]	June 19	**Not started**	May 19
133.	HOB to demonstrate Strategic Mobile equipment used at future workshop and hold a discussion on when these capabilities might be used.	[redacted]	July 19	**Not started**	May 19
134.	Set up a discussion on policy frameworks of future biometric and facial recognition work at a future Open Space session.	[redacted]	Sep 19	**Not started**	May 19
135.	HOB to review idea of making information sharing agreements public as a rule.	[redacted]	July 19	**Not started**	May 19
136.	HOB to build in review points for the Open Space going forward in the development of future DPIAs.	[redacted]	July 19	**Not started**	May 19
137.	Involve to reach out to wider CSOs to invite them to join the NRMP conversation at the July 2019 workshop.	[redacted]	June 19	**In progress**	May 19
138.	HO to look into GMCNgine system and include in discussions in July if appropriate.	[redacted]	July 19	**Not started**	May 19

Progress, Outputs & Action Log

Summary of conversation

The Open Space action log is a record of all actions from the Open Space process (1.1 Action Log Update Paper). It is divided into three sections:

- “Ongoing actions” that the HO and Involve are still working on;
- “Proposed completed actions” which the HO and Involve are presenting to the Open Space for participant agreement that they are completed and;

- “Completed actions” which is a log of all finished actions for the Space.

Involve and the HO outlined the management process of these actions. This includes weekly HO review meetings checking in on progress to date and next steps required for ongoing actions. The HO provides an interim update on progress between workshops which is reviewed and cross-referenced by Involve who then circulate an updated action log to the Open Space members.

The HO updates the Progress and Outputs document (1.2 Products and Progress Update Paper) for each Open Space workshop which lists the key issue areas the Space covers; progress to date on each area and when the next Open Space discussion on that topic will be held.

Participants were invited to raise questions on the progress tracking of the Open Space or about specific actions. The following key points were raised:

- When were the principles for deletion of data updated in relation to the Data Retention Project?
  - HO confirmed they are trying to change the HO and Policing mindset away from retention. This has been HO’s aim for a while and they need to support continued cultural change to succeed.
  - HO confirmed this exists in legislative framework for DNA and fingerprint retention and they are hoping to expand this framework to other areas.
- A question was raised referring back to Action 35 asking what discussions and consultations are being carried out with the Aerospace Defence Security (ADS) about LEDS and when are these happening?
  - The HO outlined they hosted discussions with ADS last year and will revert to the Open Space with details of other engagements they have had with commercial suppliers.
  - The Home Office is creating a sandpit for the new system to ensure users have the right connectivity and are able to thoroughly test appropriate new concepts. These users do not and will not have access to real, live data though.
  - The HO is also aiming to develop data standards to improve data quality. This will help with suppliers providing services.
- Some civil society organisations (CSOs) have been approached by the media asking for their position on the HO combining biometrics with other data. The news story presented it as “bundling data”. The concern from CSOs was raised that there needs to be a clear way for them to be taking part in the process without being seen to endorse the work and decisions the HO takes, or necessarily having to correct misconceptions. This was picked up further in the Open Space Annual Report and Terms of Reference discussions below.
  - The HO clarified that the media approach was about cloud services. They explained there is no presumption that Amazon Web Services (AWS) will always be used. At the time of contract award, AWS was considered to be the best provider for the programme’s needs. The Home Office considers all bids that meet the technical requirements set out in a contract and do not stipulate the use of a certain hosting provider.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
35	HO to provide summary of all industry consultation that has happened and is planned around LEDS to provide more clarity to existing Action 35.	[redacted]	July 19	**Not started**	Created in July 18 and updated in May 19

					asking for more detail.

Programme Update

Summary of conversation

The HO provided the following outline for this report summarising the Programme Update they provided at the workshop:

The Programme has completed its extensive replanning following the previous reviews. The plan remains to deliver the National Register of Missing Persons in 2020 in what will be the first capability of LEDS. This will be joined in 2021 by information currently on the Police National Computer (PNC) and in 2022 by information on the Police National Database (PND).

Aligned to the programme is work on the provision of Images at the Roadside. The pilot of Police Accessing DVLA Images at the Roadside is due to go live over the next couple of months. The National Law Enforcement Data Programme (NLEDP) is working with the DVLA, Surrey Police and Sussex Police in a three-way partnership to permit operational police officers to access the Driver's Licence picture on their force issued mobile devices to assist with confirming identity when dealing with road traffic.

The pilot will run initially for three months from June 2019 and involve a number of the officers from the Surrey and Sussex's Joint Road Policing Unit. It will allow officers to access the Drivers Licence photo as well as data that they can already receive from a person's Driver's Licence. NLEDP and Surrey Police have found that officers spend an average of 16 minutes at the roadside confirming driver identity per incident in addition to fewer arrests where identity cannot be confirmed. This pilot will give detailed evidence of the scale of the potential benefits, if rolled out Force wide and, in due course, nationally. The access will be strictly limited to Road Traffic Policing roles.

Changes & actions required as a result of discussions

There were no changes or actions required from this discussion other than to ensure the above update was included in this report.

Open Space Annual Report

Summary of conversation

Involve presented a paper (2. Annual Report Terms of Reference Discussion Paper) to the Open Space outlining a proposed plan for an Open Space Annual Report. The key question posed to Space participants was whether they were happy for an Open Space Annual Report to be produced following the suggested structure and content outlined in the paper.

The ensuing discussion raised the following key points:

Publicly Available Materials

CSOs asked the HO to confirm all of the publicly available materials presented to the Space as they would expect the report to link to everything publicly available. CSOs questioned whether people would be able to get to the substance of information needed if not all of the materials were publicly available. This was a deciding factor for CSOs whether the report is produced or not.

The HO took away actions (outlined in more detail below) to review and publish as many of the artefacts produced for this process as possible and to provide a public summary of the programme to go in the report. They will also clarify a definition of official and sensitive information with CSOs.

CSO involvement

Another key area was whether CSOs would be anonymous in the report or not. Some CSOs made clear that they do not want the report to suggest their involvement and were very clear that they did not wish to be seen as approving or endorsing Home Office programmes.

The initial proposal for the report suggested CSOs would be anonymous (in line with the initial ToR for the Open Space). Some CSOs in the room stated they would want to publish responses to the report acknowledging and explaining their involvement and their position on this work.

The HO also explained that they would make a very strong argument why they could not share the names of those involved in the Space if a Freedom of Information request asking this was submitted. This would be on the basis of the clear understanding that some information was supplied to it (including the participation of the organisations) in confidence.

The HO made clear they do not expect the CSOs to defend the HO and emphasised the need for this Space to be constructively critical.

There was general agreement in the room that the names of organisations taking part in the process could be published in the report if those organisations were content. A number of participants were happy in principle, but will need to get formal approval. Involve will follow-up with participants individually to confirm their position.

Drafting & sign off process

The drafting and sign off process was agreed as follows:

1) Involve produce factual draft 2) HO comment on factual errors 3) Involve review 4) Involve send to CSOs asking for comments and anything missed 5) Involve incorporate changes 6) Final HO fact check

It was agreed that the HO could make changes to factual errors but not matters of CSO opinion. It was also agreed the CSOs would individually decide what input / response they will give to the report.

Overall, there was agreement in the room for the report to be produced depending on the factors mentioned above and the agreement of those CSOs not in the room that Involve will follow up with.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
112.	Involve check with other CSOs not in the room that they are happy for the Annual Report to happen and check what involvement they would want. Involve will follow-up with participants individually to confirm their position.	[redacted]	June 19	**In progress**	May 19
113.	HO to share definition of official and sensitive information with CSOs to determine what materials from the Open Space can be shared in the Annual Report.	[redacted]	June 19	**Not started**	May 19

114.	HO to confirm if all information included in papers is publicly available and where it is publicly available. This will determine whether an Annual Report can be produced or not. Involve to share these identified places for this information with CSOs.	[redacted]	June 19	**Not started**	May 19
115.	HO to produce public summary of programme to go in Annual Report.	[redacted]	July 19	**Not started**	May 19
116.	Involve to lead on the drafting process for the first Annual Report if all dependency factors raised in the Write Up are met.	[redacted]	Sep 19	**Not started**	May 19

OPEN SPACE TERMS OF REFERENCE

Summary of conversation

There was only a brief conversation around the Terms of Reference (3. Open Space Terms of Reference Discussion Paper) for the Open Space which raised the following specific questions and responses from the HO:

- A question was raised around the principle of confidentiality of the Space and suggested that whatever is decided for CSO anonymity or not in the Annual Report needs to be reflected in the principle of confidentiality.
    - It was confirmed that CSOs can inform people they are involved in the Space, but they are not able to confirm who else is without asking their permission first.

The conclusion of this discussion was a proposed yearly review of what is in scope of the Space. It was discussed that CSOs should continually review and challenge at what level the conversations in the Space are being had and whether the right areas are in scope.

- There was also a brief discussion about the content of the space. What is the context of the Emergency Services Mobile Communications Programme (ESMCP) and LEDS / HOB?
    - The HO explained they are part of the same family. If there is better access to data, then there is an improved chance to put more data onto police devices when this is needed operationally e.g. Airwave replacement.
    - Data on the devices will follow the same security and access aspects whether through ESMCP or not.
- A follow up question was asked around the scope of ESMCP and how this and other areas like this should fit with the two programmes?
    - The HO explained that these link with the Code of Practice and data sharing and data aggregation conversations so there will be multiple chances for CSOs to feed in on these areas.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
117.	[redacted] to speak to [redacted] from [redacted] re. ESMCP.	[redacted]	July 19	**In progress - Meeting**	May 19

				arranged for July	
118.	Involve to schedule yearly review, during the May workshop, of what is in/out of scope of the Open Space.	[redacted]	May 2020	**Not started**	May 19

Code of Practice Discussion

Summary of conversation

The Home Office team working on the drafting of the Code of Practice presented to the Open Space. They explained the timeline for the drafting process, progress made to date and the consultation involving potential law enforcement users of LEDS that has fed into the design of the Code. This is also outlined in the paper shared with participants (4. Code of Practice Discussion Paper).

Several clarifying questions were raised on Parliamentary scrutiny, the technical part of the Code and the wider structure and content of the document. These questions from CSOs and answers from the Home Office are detailed in Appendix A.

Table discussions then focused on the key questions from the paper that was circulated to the Open Space. The questions looked at any gaps in the proposed drafting process and the potential different audiences for the Code. These discussions are detailed in Appendix A too. A summary of the key themes are drawn out below:

- Concerns raised around how **legally binding** the Code will be if it remains top level and links to other documents. The HO explained it cannot be absolutely binding but will be strongly taken into account. There would need to be a strong justification for why it was not followed and then standard legal procedures would be followed.
- CSOs wanted to see reference to **more statutory bodies** and consultation with wider potential users including: ICO and the judicial services respectively.
- A recurring set of questions were raised around **how the Code would work for a member of the public** to help them understand their rights. There was a feeling from CSOs that the information shared so far does not show whether this would be possible or not.
- Several CSOs, when asked if they were content with the proposed drafting plans for the Code, said they would take a position of **"reserved judgement"** rather than agreeing that they were generally happy on the structure. CSOs said they would need more information first before being able to judge whether the plans for drafting were sufficient.

The HO shared an additional response to these discussions after the workshop to be included in this report to explain further detail in relation to the first bullet point above:

The Code of Practice, like the Highway Code will not be legally binding in its entirety. It will be statutory guidance. It will be admissible in a court of law and in disciplinary proceedings. In the case of the Highway Code only certain sections are legal requirements. Whilst failing to comply with the remaining sections within the Highway Code does not in itself cause a person to be prosecuted, The Highway Code, in whole or part, can be used in evidence in any court proceedings.

There is also a relationship between the Highway Code and other legislation requirements, for example the MOT. *"You MUST NOT drive a motor vehicle without an MOT certificate when it should have one."* The Highway Code refers to the Road Traffic Act 1988 for further details.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?

119.	Explore pulling in ICO & other statutory organisations to give them responsibilities in the Code of Practice – check these are part of statutory responsibilities.	[redacted]	July 19	**Not started**	May 19
120.	HO to consider including what bad practice is in the Code of Practice.	[redacted]	July 19	**Not started**	May 19
121.	HO to confirm when Open Space can next see Code and public section of the document specifically. HO to confirm if it's possible to see it before it goes out to public consultation.	[redacted]	July 19 – before next workshop	**Not started**	May 19
122.	HO to produce and share "language of LEDS" document.	[redacted]	July 19 – before next workshop	**Not started**	May 19
123.	HO to carry out further consultation with judicial services on the Code and explore how judges would interpret the Code.	[redacted]	July 19	**Not started**	May 19
124.	HO to send a link to the current system Technical Document that is available online.	[redacted]	June 19	**Not started**	May 19

Data Protection Impact Assessments Discussion

Summary of conversation

Progress to date and plans for the drafting of the next LEDS DPIA were presented to the Open Space. A paper had been circulated prior to the Open Space outlining these plans and the timeline for drafting (5. DPIA Drafting Discussions Paper). The paper also highlighted the current risks from the programme that the HO are aware of that will become the basis of the next DPIA. There were very detailed table discussions reviewing the content of the paper which are outlined in Appendix B.

In summary, the discussion looked at questions around data sharing, automated decision-making and a review of the risks highlighted in the paper. CSOs raised areas they felt were missing from the list of risks and shared suggestions for how this list could be prioritised. CSOs also questioned why potential capabilities are acknowledged as risks within the DPIA when the HO says they will not be used. The HO explained they have to make potential capabilities transparent in this context because others have flagged concerns about certain potential capabilities. To mitigate the possibility that individuals will concern themselves unnecessarily about potential capabilities that might not exist or not even being considered, the Home Office wants to make proactive statements to address those concerns. To that end where something is not being considered the Home Office will state this and will not assess the capability any further under the DPIA.

Prioritisation of risks criteria

The key criteria discussed for helping the HO to prioritise their work on the risks highlighted in the DPIA are summarised below. It's important to note here that some CSOs questioned: why would any of these risks be de-prioritised? The HO clarified the question asking: are there parts the HO should focus on first and in greater detail. Some CSOs responded saying they felt it is for the HO to prioritise their work around these risks. Several areas are highlighted below still as key issues for the HO to keep high on the agenda that came from the discussions.

- Start with **data protection principles**. For example, lawfulness – does the DPIA address all data protection requirements/principles? It needs to make clear that it is doing this. Recommended to use ICO principles and then do a further review with CSOs.

- **Public acceptance is not sufficient.** Using public acceptance as a mitigation doesn't make any sense in terms of data protection; it should not be used as a reason for identifying reduced risk.
- **Data access.** Who gets access to what data in what circumstances?
    - Needs to go beyond role-based approach, but it's also about context – i.e. what is relevant for the user in that context? Therefore, make the DPIA more granular.
- Use **risk identification and impact on wider rights** and what this means in legal and practical terms.
    - Ensure text gives clear statement of intent.
    - Need to clearly delineate between law enforcement vs data protection especially for organisations outside law enforcement.
    - Need to remember DPIA is about impact on individual and not a wider academic discussion about clashing of rights.
    - Could there be a box to explain for individual cases and their flow through the system and the infringement of their rights might help?
- **Ethical considerations.** One CSO stated it was good to see ethical and policy consideration statements in the DPIA paper – they would want to know when these would be published as it would be very positive to see.
- **Sharing learning.** One CSO emphasised that risk number 7 (referring to "dissemination of learning throughout the Law Enforcement community as analysis is conducted for the DPIA") needs to be addressed early as this CSO had lots of experience of Police saying their job is to stop crime.
- **Academia.** There should be further review of, and discussions with, academics about the DPIA.
- **Data quality and standards**. The importance of these areas were emphasised as essentials.
- The DPIA should focus more on questions about, and the risks of, poor data quality and how data minimisation might conflict with need to collect more data to ensure quality.

The HO will share a draft of the DPIA with Open Space participants for them to review for the September 2019 workshop.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
125.	HO to explore role of how the Open Space will be involved in the data sharing process and confirm this before the next Open Space. Artefact 1 covers some of this.	[redacted]	June 19	**Not started**	May 19
126.	HO to confirm if Open Space can involve local data controllers to help understand different paths being taken?	[redacted]	Sep 19	**Not started**	May 19
127.	HO to clarify answer to the question of whether a private facial image company could get a data sharing agreement with a local force, therefore by-passing the HO and their data sharing agreements?	[redacted]	Sep 19	**Not started**	May 19

Custody Images Update

Summary of conversation

The policing representative seconded to the National Police Chiefs Council (NPCC) and attached to the HO who is leading on the Custody Image Review work (from a policing perspective) outlined progress to date and confirmed first stages of deletion of custody images. This was also outlined in the paper circulated to participants prior to the workshop (6. Custody Image Part 3 Update Paper). A plenary discussion was held focusing on the progress of the review; criteria for deleting this first phase of images and how this deletion process will actually be implemented (especially in local forces). These discussions are detailed under those sections below:

Progress of CIR

- **Quantity:** CSOs asked how many images are likely to be deleted in this proposed first phase of deletion of "low-risk images".
    - The HO explained it is likely to be in excess of images relating to about 1 million individuals that can be deleted under this process.
    - The HO clarified these are all individuals.
- **Timeframes:** If automatic-deletion is not happening until 2023, CSOs asked when will manual deletion happen?
    - The HO outlined it will be as soon as they know numbers of images and which images are involved. This was likely to be known in July/Aug/Sep 2019. Further deletions will start after the criteria for deletion is determined. This is likely to be at the start of 2020.
- **Link with LEDS:** The HO confirmed low risk images will not be migrated to LEDS. Next level up (slightly higher risk) might be migrated. CSOs stated they would want to know process for how slightly higher risk images will be deleted when HO get closer to migration. When the Custody Image Review (2019) is complete it will have been approved by policing and therefore the determination of either manual or bulk automated deletion can be taken. The activity to delete the images will be detailed to Open Space after the Custody Image Review is impact assessed.
- **Open Space discussions:** Proposed next conversation on this at July 2019 Open Space
    - The HO offered to share minutes and actions from the FACE Board (Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board).

Criteria for deletion

- **Risk based approach reasoning:** CSOs asked why deletion will be based on risk not custody status? Is it the same as under the Protection of Freedom Act (PoFA)?
    - The HO explained it is likely to be the same but they will confirm this. They also outlined it is not feasible for the link to custody status to be used for deletion at the moment. Risk links to proportionality of retention. There are a number of images whose retention is not justified and this needs to be addressed as rapidly as possible. There will therefore need to be a regime for deleting existing images that will be different from the future image retention regime. Deleting on the basis of risk goes further and therefore deletion will be faster than were deletion to be based upon custody status. In future it might be that a PoFA style deletion regime is adopted.
    - They will use criteria to draw down data that is low risk.
- **Process for legacy data:** A follow up question from CSOs asked whether this will be the hard and fast rule for the process of deletion and why, if the HO has a plan for deletion going forward, can they not use the same process for legacy data?
    - The HO explained they are taking this approach in order to speed up the process with the resources they have to do this work.
    - There are also still ongoing discussions on how deletion will happen in future – this is the proposed best solution for now.
- **Conviction status:** If a custody image is linked to an individual with no conviction, will this image be kept?
    - The HO confirmed this will be kept in line with proportionate risk

  - A further question was asked about what happens to images of people who display patterns of crime that suggest risk of a crime being perpetrated in the future? The HO confirmed these images will be under group 2 category convictions and not deleted in the first phase of deletion.
  - An additional question was raised asking what is the difference between one off arrestee and someone who's a prolific arrestee and if this will form part of the criteria? The HO confirmed they will outline the data buckets that will be used for deletion criteria with the Space before the July workshop.

Implementing the deletion process

- **Local forces:** Police will be obliged to do this deletion. The HO will use Daily Activity Files going to local forces to help ensure this process is followed.
- A follow up question was asked whether local forces will be given resources to support them to do this. The HO confirmed they are speaking to Capita, Northgate, RMS and others who supply forces with custody managements systems whether they can programmatically support bulk deletion. This is also part of broader data protection issues identifying what local forces need to do.
- **Legal basis:** If the Gochran case is lost then this will require changes to the whole custody image regime.
- **Notifying individuals:** Will efforts to notify people whose images could be deleted be made? It was suggested this could help with speeding up deletion too.
  - The HO confirmed this might happen but at present there are considerable practical challenges to contacting, searching and checking of contact details that might be outdated. This will form part of the comms work around this process too. The Custody Image Review 2019 will consider if a more modern approach to contact management would be of assistance or not.

During the Actions conversation at the start of the workshop the following question referring to custody images was also raised: what did the Minister outline at the recent Select Committee they attended?

The HO shared this link after the workshop to the transcript of the Select Committee meeting including Baroness Williams' contributions to the meeting.

The overall CSO response to this discussion outlined that taking this proposal from the HO at face value, it seems a sensible first step but CSOs also outlined fears that things may still fall through the gaps.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
128.	HO to share information on buckets of data and criteria using for deletion of custody images.	[redacted]	July 19	**Not started**	May 19
129.	HO to update on progress of custody image review process and legislation and governance around this.	[redacted]	June 19	**Not started**	May 19
130.	HO to confirm number of images that could be deleted through proposed process.	[redacted]	July 19	**Not started**	May 19
131.	HO to update on process for how slightly higher risk images will be deleted when HO get closer to migration.	[redacted]	July 19	**Not started**	May 19
132.	HO to provide update on why deletion will be based on risk and not on custody status in interim update on custody image review.	[redacted]	June 19	**Not started**	May 19

Home Office Biometrics Granular Detail & Privacy Impact Assessments

Summary of conversation

HOB presented further granular detail to explain more about the systems that the Programme uses. They outlined the Privacy Impact Assessments they have carried out for this work too. The detail of these presentations is included in the two papers circulated prior to the Open Space workshop (7.1 HOB Extra Granularity Discussion Paper & 7.2 HOB Privacy Ethics Assessments Discussion Paper). A plenary discussion was held where CSOs raised questions and concerns they had on this area. This discussion covered the suppliers HOB uses; the implementation of the capabilities by local forces; Programme timeframes; public consultation about the Programme; the Immigration and Asylum Biometric Systems (IABS) and IDENT1 Automated Fingerprint System; policy considerations and data use by the Programme. These are all outlined in more detail below:

Suppliers

The CSOs in the room had several questions around the contracts for the new HOB systems and whether these would be decided by July and where these systems would be held. HOB plan to publicly announce the successful Strategic Central and Bureau Project (SCBP) supplier in late July, with a contract start date of 1st October 2019. The output-based requirements set out in the contract include the use of cloud services, but does not stipulate how this should be delivered or the use of any specific provider. Details of the contract remain commercially sensitive.

Local force implementation of Strategic Mobile

Questions were also raised around whether HOB were rolling out capabilities at force level and not national level and what remit do forces have to do this. HOB explained they have created a platform for police force providers to build solutions to replace the mobile devices which had proven expensive, difficult to use and reliant on out-of-date technology. HOB outlined it is each force’s decision to adopt this capability, and this approach has enabled police forces to deploy their own mobile biometrics application via their existing device or provider, reducing costs and making quicker identifications. HOB also explained they are only rolling out the Strategic Mobile capability that checks fingerprints, not facial images. Each force must complete their own DPIA, Community Impact Assessment (CIA) and meet the security certification requirements needed to access the biometric data through their mobile provider.

Programme timeframes for DPIAs

CSOs asked what the timescales are across the different steps outlined for completing project DPIAs. HOB explained some can be weeks, for others, it can be months. CSOs asked if HOB can build in consultation contingency to bring in feedback from Open Space into these steps. HOB confirmed they have done something similar with the Ethics Working Group and will consider putting review points for Open Space, where possible, in their plan for publishing DPIAs for the systems.

CSOs asked for Open Space privacy and ethics considerations to be included in next HOB DPIA. They also asked what wider consultation is happening on this? Some CSOs only feel aware of consultations because of the Open Space. One CSO offered to share findings from a consultation they have done on this area with HOB.

Overall, it was emphasised by the Space that HOB need to involve the public and review how and the most appropriate time to do this.

Immigration and Asylum Biometric Systems (IABS) and IDENT1 Automated Fingerprint System checks through Strategic Mobile

HOB confirmed IABS is a standalone database after this was raised by CSOs. They explained that in any check made through Strategic Mobile, the Police are only given biographical details of the individual where there is a match in IABS, but no more information is shared such as immigration status. The police officer will however receive the photo of the individual from their visa application. The officer will have to phone through to a Home Office team for extra detail on immigration status if that is required. HOB also explained the Biometrics Services Gateway (BSG) manages the Strategic Mobile access to the biometric databases and for the foreseeable future access to these systems will remain the same as it is.

HOB explained further that when an officer requests a fingerprint search on the street this will just be for identification purposes and through the Strategic Mobile solution, they will be notified if the individual is on the immigration database. Concerns were raised about the implications for an individual whose identity was confirmed through the immigration database and the risk of further action being taken as a result of this. A better understanding of the implications for individuals in this situation was requested.

CSOs also asked whether the operational use of scanners is under HOB's remit. HOB clarified that it is not, and this comes under policing and individual forces.

HOB agreed to demonstrate the Strategic Mobile equipment at a future workshop and hold a discussion on when these capabilities might be used and what it would mean in an operational setting. Sets of questions around operational use of equipment were asked for by CSOs.

Policy considerations

A request was made for using the Open Space to discuss the policy frameworks of the HOB work and facial recognition etc even if they are not HOB / HO responsibility. The HO confirmed that this would be possible and key individuals working on this area could be brought into future sessions to discuss. This could cover Law Enforcement Facial Images and New Biometric Modalities Oversight and Advisory Board and the overlap with LEDS.

CSOs also asked if there are other government departments who have access to HOB data outside of HO. The list of organisations who have access to HOB systems is outlined in the paper shared for the workshop (7.1 HOB Extra Granularity Discussion Paper).

Data use

A final area of questioning was around data use by the HOB system. Specifically, CSOs asked about the aggregation of data and if this was separate between LEDS and whether there was a separate HOB framework? A concern was again flagged about the risk of stigmatisation that is created from these increased capabilities. HOB explained that there is a legal basis for the HOB capabilities, but a further discussion is welcomed around the potential impacts of new capabilities especially on specific groups.

CSOs also asked what types of usage of new capabilities is there and what's the legislative basis for this. HOB explained this is covered in the PIA on the gov.uk website and further questions raised from this are to be discussed at future Space meetings.

A further area of questions was raised around information sharing agreements and if they were applicable under Freedom of Information requests and could they be made public as a rule? HOB explained they were and that they would take this away and review this idea. It could be a topic to discuss at a future Open Space session. A CSO informed the Space that this is being discussed in Scotland.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
133.	HOB to demonstrate Strategic Mobile equipment used at future workshop and hold a discussion on when these capabilities might be used.	[redacted]	July 19	**Not started**	May 19
134.	Set up a discussion on policy frameworks of future biometric and facial recognition work at a future Open Space session.	[redacted]	Sep 19	**Not started**	May 19
135.	HOB to review idea of making information sharing agreements public as a rule.	[redacted]	July 19	**Not started**	May 19
136.	HOB to build in review points for the Open Space going forward in the development of future DPIAs.	[redacted]	July 19	**Not started**	May 19

Next Steps

Summary of conversation

National Register of Missing Persons

The HO proposed a substantive discussion on their planned National Register of Missing Persons (NRMP) at the July 2019 Open Space workshop. It was suggested that wider CSOs working around this area should be invited to that section of the July workshop. CSOs in the room confirmed this should be done. It was flagged by a CSO that a brief outline of the National Law Enforcement Data Programme and the HO structures around this would be needed for any new people being brought into Open Space conversations.

A specific question was also raised earlier in the workshop relating to missing people. The HO were asked if they were aware of a GMCNgine system that is a new international missing persons database that uses facial recognition. It was reported that the National Crime Agency are in discussions with them about whether the UK will become part of it. It is apparently run by Amazon Web Services (AWS), but it is not clear what this means and how thought through it is. The HO officials in the room were not aware of this and it was concluded they would investigate further and may need to expand the discussion across the HO in July to cover this too.

Another question that was raised during the HOB discussion asked about what happens to data once it gets into the immigration system. The HO explained this will be included in the NRMP discussion in July too.

Changes & actions required as a result of discussions

#	Action	Owner	Deadline	Status	When from?
137.	Involve to reach out to wider CSOs to invite them to join the NRMP conversation at the July 2019 workshop.	[redacted]	June 19	**In progress**	May 19
138.	HO to look into GMCNgine system and include in discussions in July if appropriate.	[redacted]	July 19	**Not started**	May 19

APPENDIX

Appendix A – Code of Practice: Clarifying Questions & Table Discussions

Parliamentary Scrutiny & Statutory Oversight

- What parliamentary scrutiny will the Code go through?
  - Code will be laid in Parliament under statutory guidance of 39A of police act i.e. not a Statutory Instrument (SI) and won't be debated. So the consultation is as laid out in the timeline presented at the workshop.
- What parliamentary scrutiny is there of NLEDP?
  - There's oversight in the way that Senior Responsible Owners (SRO) can be called to a select committee.
- Have there been any conversations with Ministers or MPs about discussing the programme in Parliament?
  - The HO outlined that it is Parliament's responsibility to call something for debate.
  - There are three responsible select committees the programme reports into which are: Home Affairs Select Committee, Science & Tech Committee (STC - more interested), Public Accounts Committee (PAC - in terms of spending).
    - STC discussed biometrics and this crosses over into NLEDP especially custody image review. A concern was raised at the workshop that the programme is avoiding encouraging more parliamentary scrutiny and involvement because of fears it will slow the programme down. HO responded that a drive from Parliament is more likely to push for speeding up/ensuring programme timelines are adhered to.
  - House of Lords Committee on Forensic Data? (Worried about volumes of data and capacity of Police Service to use).
- This prompted a further question from CSOs as to how Parliament knows the work is happening?
  - MPs as individuals alerted by CSOs. MPs likely to be interested in areas involving large amounts of data, highly contentious topics etc.
- In Part 1 there is only one statutory organisation mentioned (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services - HMICFRS). What about other organisations, e.g. ICO?
  - There will also be relationships with Police Investigation and Review Commission Scot, Police Ombudsman NI and Independent Office for Police Conduct (England & Wales).
- Feedback from CSOs that HO needs to avoid being prescriptive as the regulatory environment changes but also need to avoid gaps appearing.
- HO explained Data Sharing agreements will provide key regulation/guidance to ensure best practice too.

Technical Document

- Is the technical document going to be available?
  - The existing document, minus part that gives operational tactics, is available online.
  - For LEDS it will be rewritten and made much simpler than for PND. This will then be available online too.

Structure & Content of the Code

- How was the structure determined?
  - Part 1 was determined by what needs to be laid before parliament. Part 2 determined through consultation with users and looked specifically at how to improve current PNC guidance and Code.

- How specific will the Code be in terms of steps Police should be taking in an investigation?
    - It will be high level as it will be used beyond just the Police.
- How easy will the Code be to change?
    - There will be a clause saying the Code will be regularly updated, especially as other guidance will be revised regularly.
- Is there a plan to include what bad practice looks like?
    - HO explained their challenge is that LEDS is big so they need to keep each part of the Code short to cover everything. They agreed to consider this though.
- Will the policy about data inclusion and retention be referenced and how? Will it repeat language or just reference it?
    - HO confirmed it will be cited and they will ensure it is public if so. Therefore, if Authorised Professional Practice is updated the reference will not go out of date. HO explained that getting the layers of responsibility right is part of this work and that resolving this issue is at force level largely too.
- What will a member of the public see?
    - The Code will be high level but links will need to be made to ensure exact rules should be being applied.
- Key question is in terms of readership and audience – for some people structure will work. But public won't be able to understand rights, data retention etc as it is.
    - HO explained the Language of LEDS Document will describe why people are on LEDS.
- Covering right areas but question is how it relates to governance etc documents and until seen the full draft it's difficult to say. I.e. what processes are to be followed around audit. Timelines for approving users etc.
- This raised an additional question about the information about audit timelines and standards.
- How much detail do the Principles go into (purposes)?
    - This is being reviewed. HO are trying to create clear guidance on deletion and retention of data.
    - Code focus is high level and clear guidance linking to other existing regulation and guidance will be included.
- Oversight bodies should be included e.g. ICO, Biometrics Commissioner – CSOs expected to see those in there and an acknowledgement of the overlap in oversight.
- Will there be a process of notification to individuals of use of their data?
    - HO highlighted there's a section on recourse and this could be covered in a public facing document too. CSOs expected at least a statement on recourse.
- How prescriptive would the Code be around ethics instead of just being loose/high level Code? At the moment these are covered by super complaints process – could the Code challenge this?
    - HO responded that this is part of a broader conversation and they would like to set up a policy forum looking at how these are linked i.e. need a wider conversation confirming this which Code would reference.

Public Consultation

- CSOs interested to hear how it works for operational staff.
    - HO explained the consultation with users they have been doing has been part of this.
- HO to speak to professional standards departments to ensure Code informed by them too – should ask them very specific questions on it.

Use of the Code

- Need to distinguish between the Code and the operational manual. The Code is more about why something should be done and the ethical questions around the activity not how to do it. Therefore, don't conflate the Code with the operational manual and the document about rights. CSOs would like to know how all these documents relate to each other?
- Why is the Code needed if the data collection, retention etc is mandated or where are decisions going beyond this taken? E.g. for individual user, Police force etc.
    - HO confirmed LEDS is going to be less constrained to data to be collected. There are lots of fields, but they will not all be mandatory and therefore role of the Code will help support the national data standards document by building validation into the system.
    - Also given individual users have discretion about data they input, the Code becomes important.
- How will the HO ensure they prevent users using the system on behalf of someone else?
    - HO explained the Audit system catches this through random and automated checks.
    - LEDS will be provided to frontline officers to stop as many checks needing to be carried out on behalf of frontline officers when they are on the street.
    - Suggested that it will be clearly stated in the Code: "Do not give access to another user".

Audiences of the Code

- How does an individual user identify all their sections?
    - HO outlined the design is aimed at identifying different users and they may only need to look at four pages for example.
- Difficult to see how the Code works for public or organisations interested in ethical law. They could look at the different users but aren't currently mentioned. Suggested that if the focus is on the why, then it might help.
- Is there a need to include analysts or those applying data into the Code? Also, HO needs to consider how should the Code apply to repurposing of data (i.e. beyond the specific purpose collected) and where purpose of collection is applying law (therefore use could be very broad, raising risks of mission creep).
- Some CSOs felt the Code was still too high level. Others felt it was quite clear who will be reading it. The point was made that for CSOs who will want to engage fully with this and do full critique, the detail is still too high level.
- Others questioned if there should be more detail in case it makes it more inaccessible to the public? It was suggested a simple summary for the public could be produced.
- If the Code is very clear and simple it allows members of the public to easily cross-reference and check what's happened to them.
    - HO flagged their concern that the danger of including more detail will cause some users (not involved in auditing) to switch off from the Code and no one will read it.
- Call from CSOs to see more detail and where they can access that detail if needed and the linked regulation/guidance.
- CSOs flagged that oversight bodies need to know what they're looking for from the Code.
- Question raised as to how would judges interpret the Code? This has been captured as an action.

Impact of the Code

- Flagged that the DPIA will identify risks and Code is one way to mitigate risks.
- If Code is successful, there will be a move from collection and retention of all data to a more risk-based approach (within confines of volume of data). This raised a follow up question of: is there data collected on individuals that doesn't relate to statutory responsibilities?
- Can the Code be used to ensure protection/prevention of misuse of system by perpetrators?

    - The HO explained the Audit section can help this but points like this are covered in multiple sections too.
- Authorised Professional Practice (APP) is not statutory so officers would not have to follow the Code. The Code needs to be clear on this.
    - HO confirmed the Code will stipulate minimum requirements on each areas from APP.
- APP's referenced are not binding – CSOs called for these to be strengthened.
    - Language of LEDS plays role here to inform use of system too. Question of how binding this is though was raised. HO action noted to share this with CSOs.

Appendix B – DPIA: Clarifying Questions & Table Discussions

Data Sharing & Access

- Who drafted the current data sharing agreements?
    - These are agreements written by HO to a template agreed with the internal Home Office legal department and they give access to specific fields of data.
    - These will be replaced by joint controller agreements and sharing agreements giving other organisations permission to use that data.
    - If only taking data out, the access will be controlled by sharing agreements, if putting data into LEDS the access and sharing will be controlled by the joint agreements (broadly).
    - These are quite detailed including a legal section and a Code setting out standards to be made.
- What role will the Space have over these data sharing agreements and who has access?
    - HO outlined that at the moment access and sharing is not consistent, there are questions around proportionality of access. Many of those questions can be answered satisfactorily but some might not be.
    - Possible role for Open Space in criticising the rationale for data sharing.
    - The Police Information Access Panel (PIAP) currently governs access to information sharing. Future arrangements for LEDS might see this change to a LEDS Information Access Panel.
- Joint Data Controller includes England, Scotland, Wales – will they develop own DPIAs?
    - They may need to adapt and change it and produce DPIA for own intelligence systems for e.g.
    - Sharing data is different to using APIs.
- Specificity needed on review of proportionality of data access rights on who does that review, what would it look like?
- CSOs asked for new data sharing agreements to be published in the first place when new agreements signed.
- A CSO flagged that a fear of data sharing contributes to a lack of data sharing for safeguarding purposes. They emphasised that data sharing agreements need to cover this.
- Need to publish data sharing agreements raised.
- A question was raised over whether a private facial image company could get a data sharing agreement with a local force, therefore by-passing the HO and their data sharing agreements?
    - HO confirmed they would follow up and clarify this with the CSOs.

Automated Decision-Making

- Big data – does it mean automated decision-making?
    - HO response: Yes.
- A follow up question was asked whether the question in the DPIA could be reframed as automated decision making rather than big data?

    - HO response: Yes.
- Will the DPIA identify the automated decision-making systems which will be considered/used?
    - HO Response: Yes.
- Does the discussion need to cover what planning to do or what's possible?
    - HO response: The former. The DPIA will cover the activities that are planned and/or in existence. Statements will cover the activities that are not planned.
- Data Protection Act requires subjects to be notified if automated decisions are taken if they might want to exercise their rights (not in every case). Will this be done?
    - The Home Office is looking at publishing not only a Code of Practice but also a Public Guide so that there is greater transparency over how data is processed. This will start with "why an individual is on LEDS" and include "how that individual's data might be used"
    - Notification of data deletion will only likely to be possible in certain circumstances typically where ongoing dialogue has been maintained. This is because of the difficulties in sending out personal data to an address on file where the data subject might no longer be living.
- So CSOs raised that the DPIA will need to deal with how people will be informed about this and about what.
- Facial matching and automatic decision-making: is there anything addressing profiling in DPIA? Or algorithmic decision-making? CSOs flagged this needs to be formally covered in DPIA to make it clear, CSOs emphasised the importance of this area to them.
    - The HO explained in the DPIA template there's a section on automated decision-making.

Risks

- Has cloud contract been awarded?
    - The HO confirmed yes it has.
- Where has predictive policing come from? Why does DPIA need to cover it?
    - HO explained they want to cover concerns that exist. If there is a concern about the programme, even if they're not doing it, they still must mitigate against it.
- What's being done must be covered. CSOs asked for the HO not to hypothesise in order to reduce risk of public concern.
- Risk of local forces using system in different ways and using huge amounts of data should be a focus.
    - The HO confirmed the DPIA will clarify what users can/can't do with data.
- Risks around contractors and access not clearly identified. A follow up question was added to this of who will run the system?
    - HO explained that IBM is the build partner at the moment, but this does not automatically mean they will be in future. The strategic intention is for the Home Office to run LEDS in-house.