Home Office National Law Enforcement Data Programme

Developing a process for dialogue between interested civil society organisations and the Home Office

Workshop one: 3rd July 2018

involve

Introductions

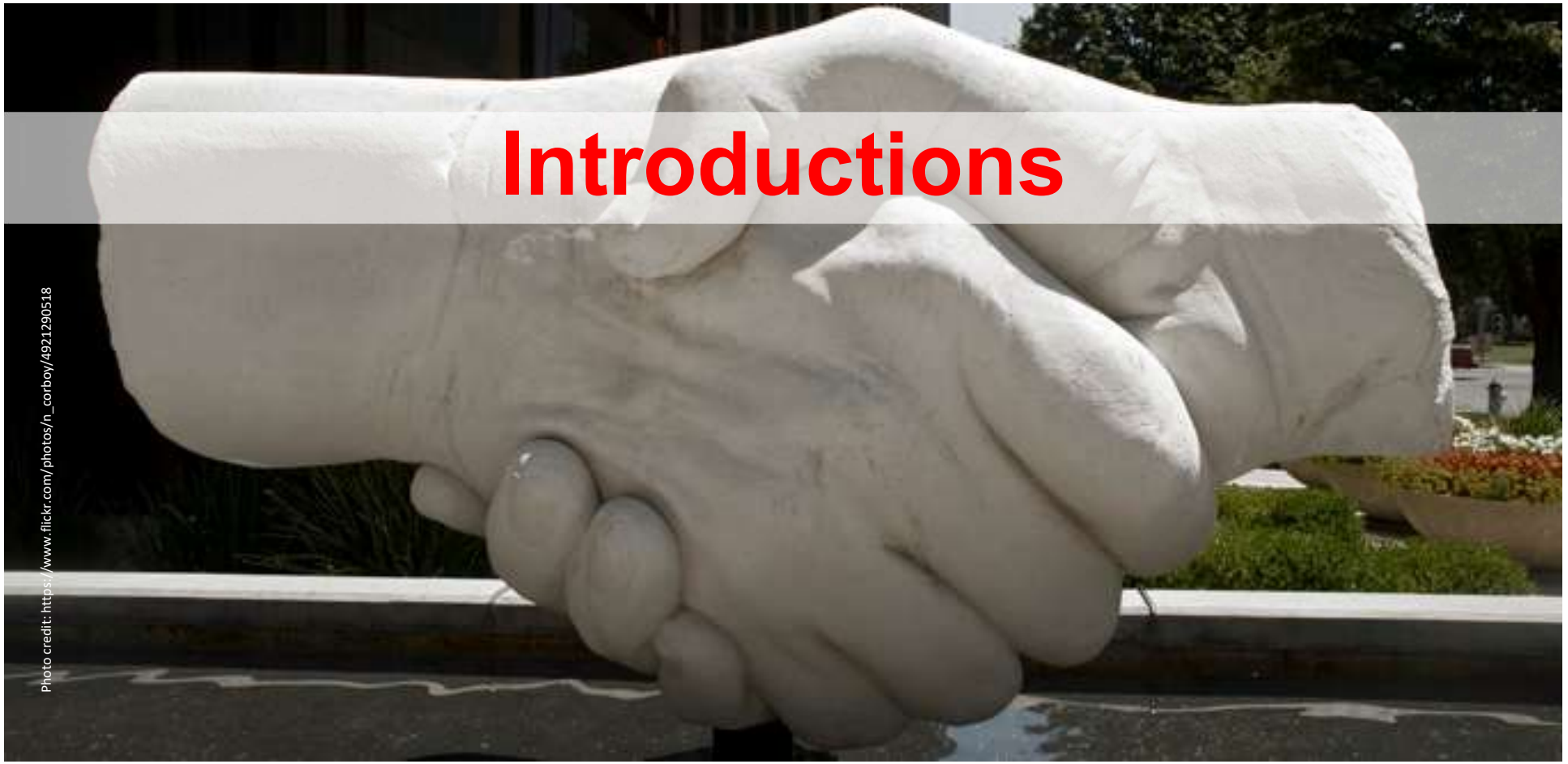


Photo credit: https://www.flickr.com/photos/n_corboy/4921290518

Introducing the ‘Open Space’ process

Purpose of process

to establish a productive space where the Home Office and Civil Society can have safe and productive conversations about the implications of the Law Enforcement Data Service

If successful, the proposed process will contribute to:

- effective civil society input into the transfer process of the PND and PNC;
- the development of a more robust Privacy Impact Assessment;
- the development of the code of practice; and
- the development of an ongoing process of collaboration between the Home Office, civil society organisations and organisations from other sectors.

Workshop 1: Introducing and scoping

Purpose

- To provide an introduction and a chance to shape:
  - NLEDP
  - the privacy impact assessment
  - key issues arising
  - the process
  - the scope of the discussion (and principles behind deciding this)
- To agree the purpose of the process and the principles of working
- To agree and prioritise the key issues to focus on
- To identify additional participants missing from the process

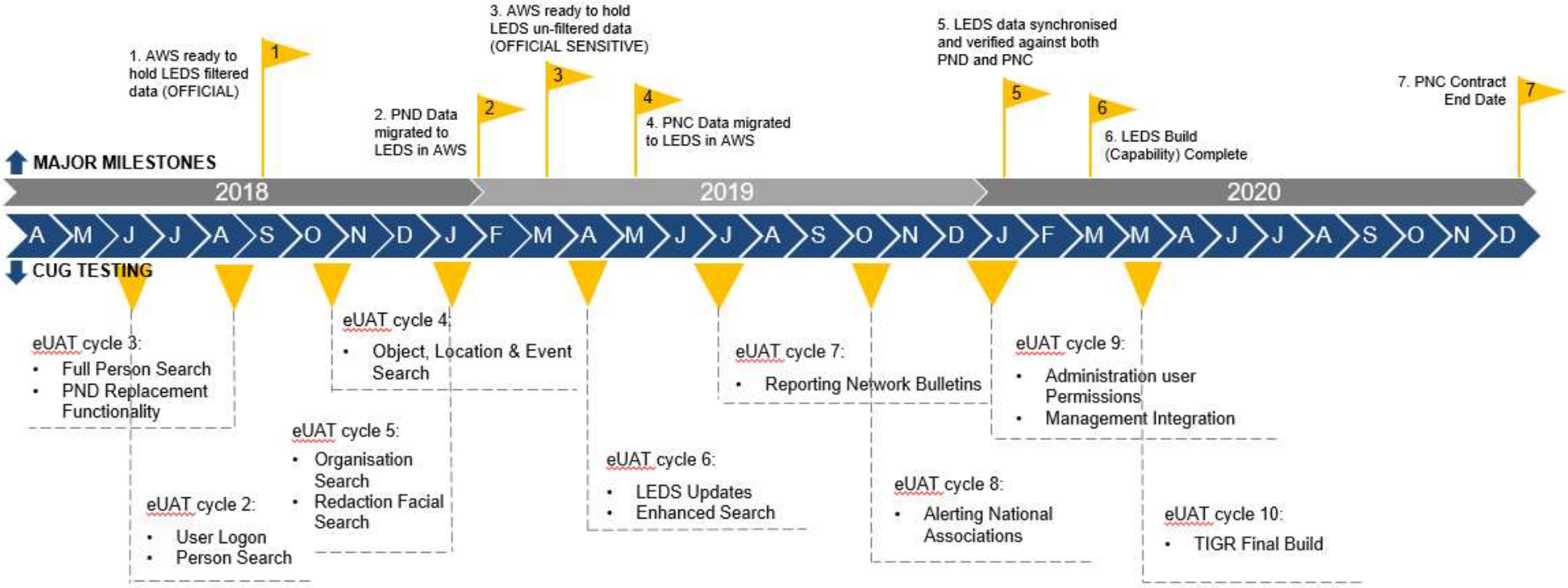
Agenda

- Introduction
- Working effectively together
- The scope of the process
- The LEDS Privacy Impact Assessment

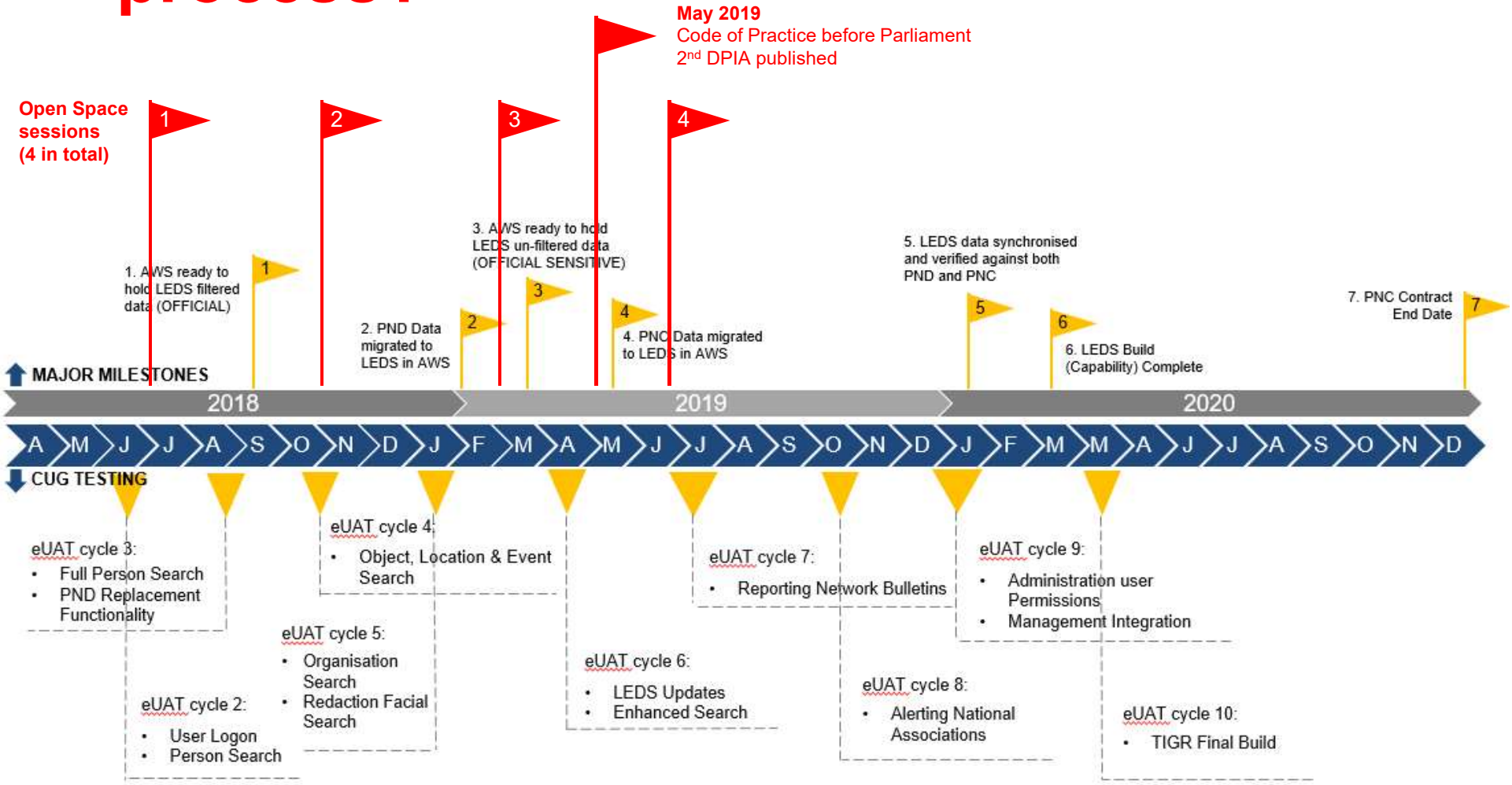
Lunch

- Identifying and prioritising key issues for discussion
- Who else is needed
- Next steps

How does this fit into the wider process?

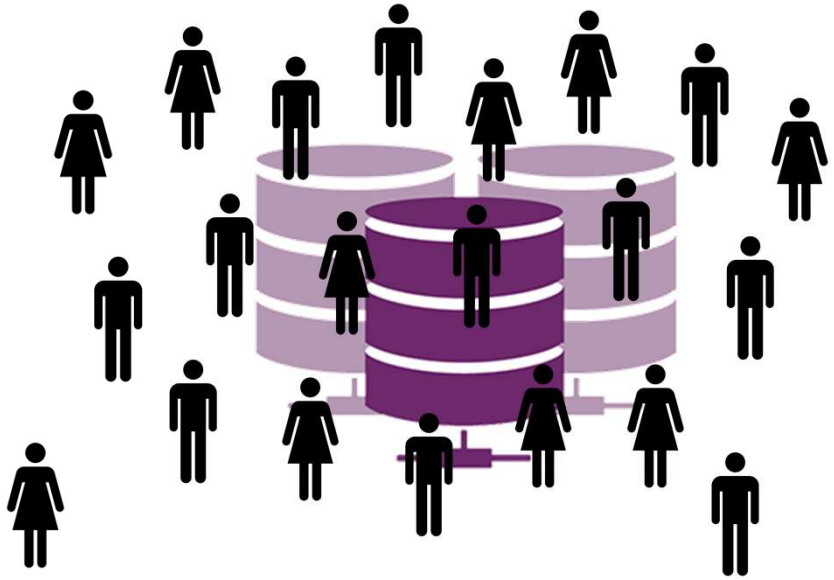


How does this fit into the wider process?



Home Office Data & Identity Director

Data is an asset



Data is an asset, its digitisation supports efficiency and new ways of working. In particular bringing data together can provide new insights.

We need to determine how we want to harness and deploy these data driven capabilities.

Within Home Office we aim to work with the sector to support **world leading use of data**, **build public trust** and create a **safe and secure society**.

Increasing digital and data capacity

To meet the changing nature of crime, policing needs better digital and data capability. There is a mix of local, regional and national investments with a focus on supporting policing in its change, replacing old technology and bringing new capabilities to policing. Presents the opportunity to integrate some of the steps and also significantly **improve public trust** and **personal data protection**.

Law-Enforcement Data Service

Public trust

Changes in the way we collect, use and share data will change the relationship with policing and government. New technologies can both increase *and* challenge public trust and confidence in the institutions that use them.

DPA 2018 requires us to understand what data we collect, how we use it, who we share it with and how we dispose of it *and* to make that clear to the public. Effective implementation is key.

As new data uses are considered we need to develop clear understanding of public and political acceptability at the same time. Will need to **listen to** and **shape the public debate** on the change that innovations bring to society and the individual.

Questions we should ask ...

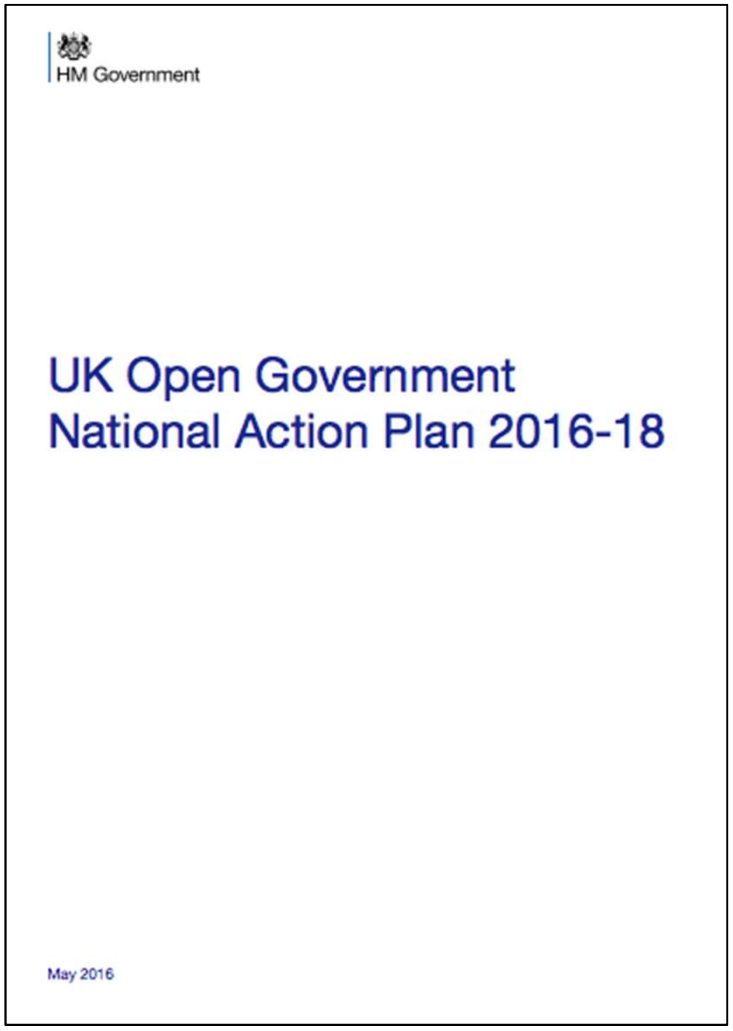
The policies, guidance, professional standards and culture all affect the opportunities and the risks.

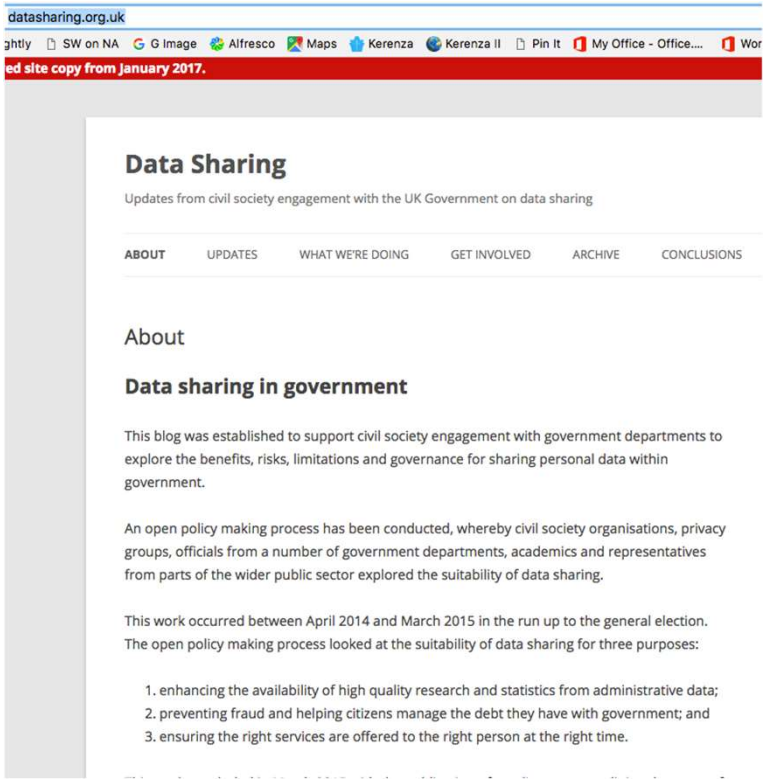
Will increasingly need to demonstrate we have considered these issues and ask the right questions, as well as consult the right stakeholders.

This is the foundation on which this Open Space will be run.

Working effectively together

Drawing on previous experience





involve

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation

All of which shape a set of principles for working together

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

- Draw on knowledge and expertise
- Provide advice and challenge on structure and content with aim of improving
- To represent organisation, wider civil society and public benefit
- Working collaboratively with officials
- Seek common ground without aiming for false consensus

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

- Role is advisory
- Role is not to decide
- Working with officials can shape discussion, questions asked, points considered
- Final outputs decided by Home Office

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

Data Protection Impact Assessment

- What is currently missing?
- How can it be improved?
- What must it cover next time?

Code of Practice

- What should the Code of Practice cover?
- How to ensure it is a strong as possible?

What next?

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

- DPIA – May 2019
- Code of Practice – May 2019

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

Two principles to shape what is in and out of scope

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

Principles for 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
- **Agree to disagree:** not expect consensus on every issue, and to accept conclusions as long as all parties are acting in good faith
- **Maintain confidentiality:** talking about the process and broad discussed as required without identifying individual positions or publishing confidential or embargoed material
- **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

Working effectively together

- What needs clarification?
- What needs amending?
- What needs adding?

The scope of the process

Key components

Clarity about

- Role of participants
- Ability to influence
- Central questions
- Outputs and timeline
- Scope of conversation
- Principles for working together

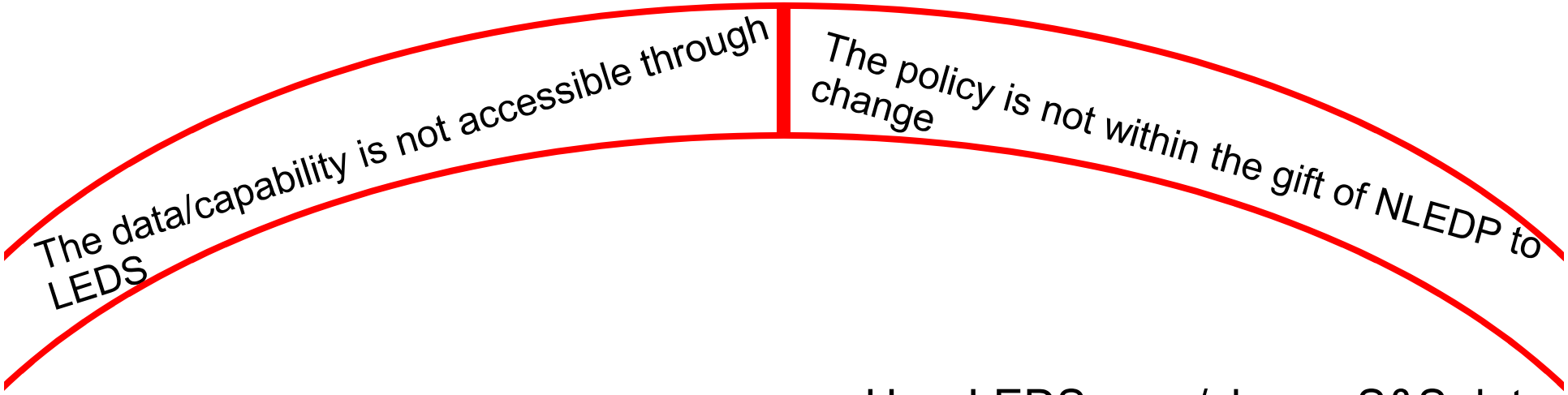
Two principles to shape what is in and out of scope

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

Ensuring discussions are productive

OUT

- Automatic Facial Recognition
- Policy grounds for Stop & Search



- Facial Matching
- How LEDS uses/shares S&S data

IN

The LEDS Privacy Impact Assessment

Rob Butlin, LEDS Policy Lead

LEDS Privacy Impact Assessment

- It is a PIA, not a DPIA
- It will be an regular publication – future iterations will be DPIAs
- Three sections:
  - PNC
  - PND
  - Future LEDS capability

Lunch

Photo credit: https://www.flickr.com/photos/149561324@N03/36000348854

Identifying and prioritising key issues

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**

LEDS' modern architecture will allow the ability to incorporate aspects of automated processing. Discussions around automated processing will include automated rules engines, including specifically triggered data deletion, and the benefits and risks from automated alerting – such as automated notification to family liaison officers when a harassment or stalking offender or violent suspect is released / provided with bail.

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**
- **Custody Images**

Images of individuals taken into custody are currently retained on the Police National Database and will be held in the LEDS. The Home Office conducted a review of the use and retention of custody images in February 2017, recommending that people not convicted of an offence are able to apply for their custody image to be deleted. The introduction of LEDS, including the incorporation of new technical solutions around the custody image data set, provides the opportunity to reconsider key policies around the data set, including retention, access to, deletion and the use of facial matching.

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**
- **Custody Images**
- **Data Sharing**

LEDS will operate as a platform facilitating users' access to law enforcement data. This means the LEDS user community will, in addition to policing, comprise of non-policing users that have a need to access and use law enforcement data – broadly for enforcement and penalty action. How, what, and why data is shared between policing and non-policing users should be considered, including particularly the exchange of data between policing and Immigration Compliance & Enforcement.
A specific area of potential discussion within this is the process by which LEDS incorporates new users and data sets; and by extension how LEDS interacts and shares data with other national or local systems.

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**
- **Custody Images**
- **Data Sharing**
- **Oversight, Inspection & Governance**

The LEDS Code of Practice will codify oversight and governance of LEDS. The design and content of this Code of Practice, including the Code's stated purpose, remit, powers and governance, are to be designed. The Programme seeks input into the development of this work. Specifically, there are additional policy questions regarding the inspection and governance process for LEDS – who oversees the Service, who inspects the operation and use of LEDS? Separately the Programme seeks additional input into the capacity for transparency around LEDS – whether this is at a public level in the form of annual publications, including of statistics from LEDS, or on a personal level in the form of LEDS facilitating privacy notices.

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**
- **Custody Images**
- **Data Sharing**
- **Oversight, Inspection & Governance**
- **Security, Audit and Access Controls**

LEDS will incorporate a number of security features around which policies must be developed. The decision to host LEDS on Amazon Web Services (AWS) has already been taken, however we would like to discuss and identify further risks posed by this decision, as well as adequate policies around the mitigation of these risk. Broader discussions around security will additionally include concerns around data breaches, whether this is the result of a loss of device or data interception, and policies to address any such breaches.

The way in which LEDS users are audited, including whether this is proactive or retroactive, and reliant on active oversight or automatic decision-making, will carry varying risks that should be up for discussion. The use of any audit logs, including the potential for logs to drive operational decisions, would be included in these discussions.

LEDS will incorporate a multitude of access controls, including Role-Based Access Controls (RBAC), Organisation-Based Access Controls (OBAC) and Attribute-Based Access Controls (ABAC). The design of these rules remains in development and the Programme welcomes discussions around the implications of opening versus limiting access to data, as well as the use of access controls to limit the exposure of certain data on individuals and any corresponding policies.

National Law Enforcement Data Programme (NLEDP)

Themes

- **Automated Processing**
- **Custody Images**
- **Data Sharing**
- **Oversight, Inspection & Governance**
- **Security, Audit and Access Controls**
- **Code of Practice**

- Statutory Guidance
- College of Police will write and own
- Recruiting associates to draft
- Place for input from interested parties
- Pre Research phase
- Iteration 1 - Sep 2018
- Circulate for comments - Oct 2018
- Iteration 2 - Dec 2018
- Formal Review - Feb 2019
- Parliament Code - May 2019
- Iteration 3 - Jan 2020
- Parliament Code - May 2021

NLEDS areas for discussion

- Automated Processing
- Custody Images
- Data Sharing
- Oversight, Inspection & Governance
- Security, Audit and Access Controls
- Code of Practice

For each issue area:

- What key questions does the research need to focus on?
- What sources should it draw on?

Identifying and prioritising key issues

Reporting back

Identifying and prioritising key issues

Stepping back

- Is the big picture right?
- Are we missing anything?
- Where should emphasis be placed?
- What are the key priorities for focus in the next phase?

Who else is needed?

Criteria for identifying potential participants

- Have **an interest** in (some of) the issues being discussed
- Have **expertise in** (some of) the issues being discussed
- Are willing to **agree to the principles of working**
- Are willing to **commit to the purpose of the process**
- Are able to **speak on behalf of their organisation** (if they have one)
- Have **credibility in their wider sector**

- Are working in one of the following areas:
  - **Civil liberties/ privacy**
  - **On behalf of individuals/ groups in the criminal justice system**
  - **On behalf of victims**
  - **Legal expertise**
  - **Data/ database/ technical expertise**
  - **On behalf of young people**
  - **Relevant community issues**

Criteria for identifying potential participants

- Have **an interest** in (some of) the issues being discussed
- Have **expertise in** (some of) the issues being discussed
- Are willing to **agree to the principles of working**
- Are willing to **commit to the purpose of the process**
- Are able to **speak on behalf of their organisation** (if they have one)
- Have **credibility in their wider sector**

What needs clarification? What needs amending? What needs adding?

- Are working in one of the following areas:
  - **Civil liberties/ privacy**
  - **On behalf of individuals/ groups in the criminal justice system**
  - **On behalf of victims**
  - **Legal expertise**
  - **Data/ database/ technical expertise**
  - **On behalf of young people**
  - **Relevant community issues**

Can you identify any organisations or individuals who should be considered for inclusion?

Next steps

Photo credit: https://pixabay.com/en/stairs-wooden-ladders-emergence-838112/


THANK YOU
Photo credit: Alpha Stock Images - http://alphastockimages.com/

Overall NLEDP Open Space Process

- **4 workshops:** July, September, November & February 2019
- **Outputs:** Write up of each workshop produced & shared with all participants
- **Content of future workshops:** Next workshop designed from the conclusions of the previous workshop
- **Interim Workshops:** Some interim workshops in between the 4 core workshops on specific topics
- **Participants:** Additional recommended organisations involved from September workshop onwards
- **Mid-2019:** Next version of the DPIA publication deadline
- **2020:** Deadline for merging of PND & PNC

involve