LEDS/HOB Open Space:

Home Office Biometrics (HOB) Programme

Privacy, Data Protection and Ethical Assessments

[v1.0, 02/05/19]

Discussion Document

The HOB programme recognises the importance of balancing public safety with individual privacy. In addition, it is essential that the public have confidence that personal information contained in biometric systems will be properly protected and handled in accordance with the law. HOB also recognises that there are significant ethical issues in the collection and use of biometric information.

This Open Space paper outlines the approach that HOB takes to make sure that public trust in biometric systems can be delivered and highlights the risk assessments outlined in the published Privacy Impact Assessment.

It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to and viewed only by members of the LEDS/HOB Open Space for discussion at the LEDS/HOB Open Space workshop in May 2019.

Purpose

The purpose of this Open Space paper is to:

- Provide a recap on the approach taken by HOB for ensuring privacy and ethics are considered in biometric capabilities and Programme developments
- Provide an update on the risk assessment published in the overarching HOB Privacy Impact Assessment

Summary

From an early stage of its work, HOB recognised the importance of maximising public safety and efficiency of delivery to the public sector whilst protecting the privacy of the individual and addressing any potential impact of data aggregation. HOB made a commitment to undertake a programme Privacy Impact Assessment (PIA), consisting of a suite of individual PIAs for each project as well as an overarching programme level PIA in the Home Office Biometrics Business Case. This commitment is also repeated in the Home Office Biometrics Strategy.

HOB also recognises that there are significant ethical issues to consider in the collection and use of biometric information. At the request of HOB, in 2016 the independent Biometric and Forensic Ethics Group established a working group to provide robust ethical and privacy advice and challenge on each HOB project PIA.

With the Data Protection Act 2018 coming into force, the HOB Programme PIA and existing project PIAs (which have been developed and approved under the 1998 Act as the programme has been in existence since 2014) will be reviewed on a rolling schedule. All PIAs for capabilities going live after the new Act came into force on 25 May 2018 will be upgraded to the new Data Protection Impact Assessment (DPIA) before the go live date of the project and assessed against the new data protection principles. Any new developments and projects will be assessed using the DPIA template from the outset.

Key questions posed by this paper

- Does the approach taken by HOB provide Open Space with the assurance that privacy and ethics are being appropriately considered by the programme?
- Are there any privacy and ethical risks that Open Space feel should be included for further consideration by the HOB Programme?
- Do Open Space have any insights and/or feedback on privacy and ethics that they feel would be helpful for the HOB Programme to include in their approach?

Home Office Biometrics (HOB) Programme Privacy & Ethical Assessments

HOB approach to privacy and ethics

1. There is an extensive development and approvals process in HOB for all Data Protection Impact Assessments (previously Privacy Impact Assessments under the 1998 legislation):

   - HOB works closely with project teams in the development of the DPIA, including subject experts in security, technical and legal.
   - The HOB Ethics Working Group provides strong challenges to the DPIAs on ethical issues. The Information Commissioners Office is invited to attend the Ethics Working Group and receives all documents.
   - HOB undertakes a due diligence analysis of the touch points between the technology and front-line operations. This happens in parallel to the development of the DPIA (e.g. Strategic Mobile where work has been undertaken between the Programme and NPCC to develop operational guidance and scenarios for using mobile devices)
   - Post publication the DPIAs, the assessments will continue to be reviewed and updated as the Programme develops and transitions into a service.

   The full process is outlined in Annex A

Publication and review of HOB documents

2. Approved HOB PIA documents were published in July 2018 on the GOV.UK website. The published documents were:

   – HOB Overarching PIA (including the PIA Screening Questionnaire and legislative summaries)
   – Strategic Mobile PIA
   – Biometric Services Gateway PIA
   – Strategic Matcher PIA
   – Latent mark searches on immigration data PIA

3. With the Data Protection Act 2018 coming into force, the HOB Programme PIA and existing project PIAs (which have been developed and approved under the 1998 Act as the programme has been in existence since 2014) will be reviewed on a rolling schedule. All PIAs for capabilities going live after the new Act came into force on 25 May 2018, will be upgraded to the new Data Protection Impact Assessment (DPIA) before the go live date of the project and assessed against the new data protection principles. Any new developments and projects will be assessed using the DPIA template from the outset.

4. The full set of published PIAs are currently under review with the aim to complete the review by July

HOB PIA high level risk assessment – updated April 2019

5. In the development of the overarching HOB Privacy Impact Assessment the main privacy risks to the HOB Programme were identified and considered as part of the PIA process. The table below outlines the risks and mitigations identified in the published PIA (the **Risk**, **Mitigation** and **Result** columns) and the risk update from April 2019 (the **Evaluation** column).

Risk	**Mitigation**	**Result** - is the risk eliminated, reduced or accepted by the Programme?	**Evaluation** – is the final impact on individuals after implementing each mitigation a justified, compliant and proportionate response to the aims of the project?
The aggregation of personal data and whether this might pose a risk of injustice	The HOB programme is a technical programme and will develop solutions that work within the policy and legal frameworks set out, and the rules that apply, working with policy and legal teams to achieve this. Where data is held for different purposes on a shared infrastructure business rules and security controls will clearly define which data collections can interact with one and other to prohibit unauthorised access and usage. Access to the data by automation or manual processes will be enforced through 'role based access control' which restricts access to a process or piece of data, and makes sure that only authorised people can access the data, and only for the right process Compliance with privacy guidelines is important to the Programme, as is the consideration of potential impacts on individuals and groups, and the ethics of using biometric information. PIAs	The risk is **accepted**	**April 19 update:** The biometric systems will remain separate for some time after the new Strategic Central & Bureau Project (SCBP) contract is awarded. However, the approach to the logical separation of data within the Strategic Matcher – where data will be combined – has been agreed and will continue to manage data along lines of business only and not aggregate personal records. The HOB Programme continues to complete and review DPIAs for biometric systems.

	(and future DPIAs) will always be used as a mechanism to address such concerns. Where technology is used by front line staff, HOB will work with policy and operational users to ensure that guidance reflects the capability that HOB is providing to the user.		
The biometric information collected is seen as unfair or intrusive	The HOB Programme is committed to undertaking DPIAs for all of its projects to identify potential impacts on individuals and groups. HOB will make sure that the technology implemented will address any recommendations highlighted through the DPIA and that the solutions work within the policy and legal frameworks set out, and the rules that apply.	The risk is **reduced**	**April 19 update:** The Programme is represented at operational and policy forums and boards to make sure that the requirements for data collection and retention requirements are met and maintained. The HOB Programme continues to complete and review DPIAs for biometric systems.
Biometric information is unnecessarily collected (and retained) without adequate justification	The current PIA outlines the legal powers through which biometric data is collected, used and retained on HOB systems. Where the retention of biometric data is stated within legislation, the technology will be designed to meet the retention requirements, alongside the operational actions to delete records.	The risk is **reduced**	**April 19 update:** The Programme is represented at operational and policy forums and boards to make sure that the collection and retention requirements are met and maintained. The HOB Programme continues to complete and review DPIAs for biometric systems.
People are not given enough information or warning about the purposes of the collection of biometric information from them	It is a key principle that people understand why their biometric information is being collected and the ways the information will be used. The current immigration and law enforcement processes (e.g. application forms, guidance, etc) do state the reasons for biometrics being collected and organisations have Fair Processing Notices that state how an individual's data will be maintained.	The risk is **reduced**	**April 19 update:** To meet the Data Protection Act 2018 requirements, Privacy Information Notices (including the Home Office Information Charter) have been updated to inform individuals of the data being collected. Guidance is also available where operational staff are dealing with individuals directly.

	These are being updated to comply with new Data Protection legislation. Where technology is used by front line staff, HOB will work with policy and operational users to ensure that guidance reflects the capability that HOB is providing to the user. Where the use, or re-use, of biometric data through the development of technological capabilities, may impact an individual, a DPIA will consider these risks. The DPIA will be considered through the appropriate governance to make sure that the risks are fully assessed and mitigated.		
Biometric information is used for purposes that are not what they were collected for	This is a very sensitive issue and is why the HOB Programme has undertaken PIAs for the projects to show that the biometric data is used for the purposes for which it is provided and within the policy and legal frameworks. HOB will continue to work with policy and legal teams to understand the policy and legal grounds on which the data is obtained and ensure rules are followed. Where there are changes in technology or legislation a DPIA will be completed to assess impacts on privacy. Where data sharing arrangements are set up with other agencies, Government Departments and International Governments, the appropriate Information Sharing Agreement (ISA) or Memorandum of Understanding (MOU) are produced.	The risk is **reduced**	**April 19 update:** The HOB Programme continues to complete and review DPIAs for biometric systems to make sure that the data is only used for the purpose for which it was collected. This is strengthened through the DPA18 where DPIAs are now completed for any data sharing requests alongside the necessary data sharing agreements. The HOB Programme continues to review and produce documentation that supports the management of data – e.g. HOB Retention Guide and other documents required under the DPA18 (e.g. processing schedules, MoUs, etc)

Biometric information is retained longer than necessary	Where the retention of biometric data is stated within legislation, the technology will be designed to meet the retention requirements through automation, alongside the operational actions to delete records. There are circumstances where manual actions are required to assess the retention and deletion of records.	The risk is **reduced**	**April 19 update:** A key element of the biometric systems is that the data is held only for as long as it is permissible, and the HOB Programme continues to manage this closely through its contracts and services. The completion and review of DPIAs for all biometric systems and projects make sure that the retention of data is a key consideration and the development of the HOB Retention Guide provides further documented guidance in the development of biometric systems and capabilities.
Information sharing arrangements with other agencies and organisations puts personal biometric information at risk	Where data sharing arrangements are set up with other agencies, Government Departments and International Governments, the appropriate Information Sharing Agreement (ISA) or Memorandum of Understanding (MOU) are produced.	The risk is **reduced**	**April 19 update:** The HOB Programme continues to complete and review DPIAs for biometric systems to make sure that the data is only used for the purpose for which it was collected. This is strengthened through the DPA18 where DPIAs are now completed for any data sharing requests alongside the necessary data sharing agreements.
Outsourcing to external suppliers does not adequately protect biometric information	Privacy considerations are included in any tendering processes, negotiations and contracts for outsourced developments and handling of biometric information. Supplier contracts will be monitored to ensure that the privacy responsibilities are fully met. New data protection laws will strengthen the rules by which personal data is held and HOB is working with suppliers to be compliant with the new arrangements.	The risk is **eliminated**	**April 19 update:** The HOB Programme continues to make sure that privacy considerations are included in any tendering processes, negotiations and contracts for outsourced developments and handling of biometric information. All existing and new contracts include data protection clauses and schedules, strengthened through the DPA18.
Extra expense is incurred because systems are not	HOB is committed to “privacy by design” for all biometric developments and projects are supported by the	The risk is **reduced**	**April 19 update:** All HOB programme developments are based on “privacy by design” principles and

designed with privacy considerations	development of privacy impact assessments at an early stage HOB is working to understand and act upon the impacts that the new EU Data Regulation and Directive will have on projects since implementation in May 2018.		“defence in depth” for added protection to the sensitive personal data held on biometric systems. HOB has invested a lot of work to make sure that it is compliant with the DPA18 and continues to work with the Home Office Data Protection Officer and ICO.
Authorisation to access biometric information is not controlled and there is unauthorised access to the data	There is a clear security governance in place for central HOB technology Where necessary access to technology will be through Role Based Access Controls.	The risk is **reduced**	**April 19 update:** There is no change to the clear security governance in place for central HOB technology Where necessary access to technology will be through Role Based Access Controls.
Loss of biometric information	HOB ensures that the biometric technology and service management has appropriate security environment for biometric information. As the new suppliers are brought on board this will continue to be a key feature of the contract arrangements Protocols are, and will continue to be, in place for the storage and handling of biometric information. Contingency plans are, and will continue to be, in place to address any security breaches. HOB is working to understand and act upon the impacts that the new EU Data Regulation and Directive will have on projects when implemented in May 2018.	The risk is **reduced**	**April 19 update:** HOB has invested a lot of work to make sure that it is compliant with the DPA18, in particular the breach control processes, and continues to work with the Home Office Data Protection Officer and ICO. The internal governance within HOB, through the Security Working Group (SWG) network, monitors any incidents that arise and works through mitigations and lessons learned. HOB also has a Data Protection Practitioner (DPP) embedded within the Programme to provide advice and support on DPA18 issues.
Biometric information is incorrectly linked with a person which could lead to that person having an	There are processes for handling false negatives and false positives when matching biometrics.	The risk is **reduced**	**April 19 update:** As stated above, the biometric systems will remain separate for some time after the new Strategic Central & Bureau Project

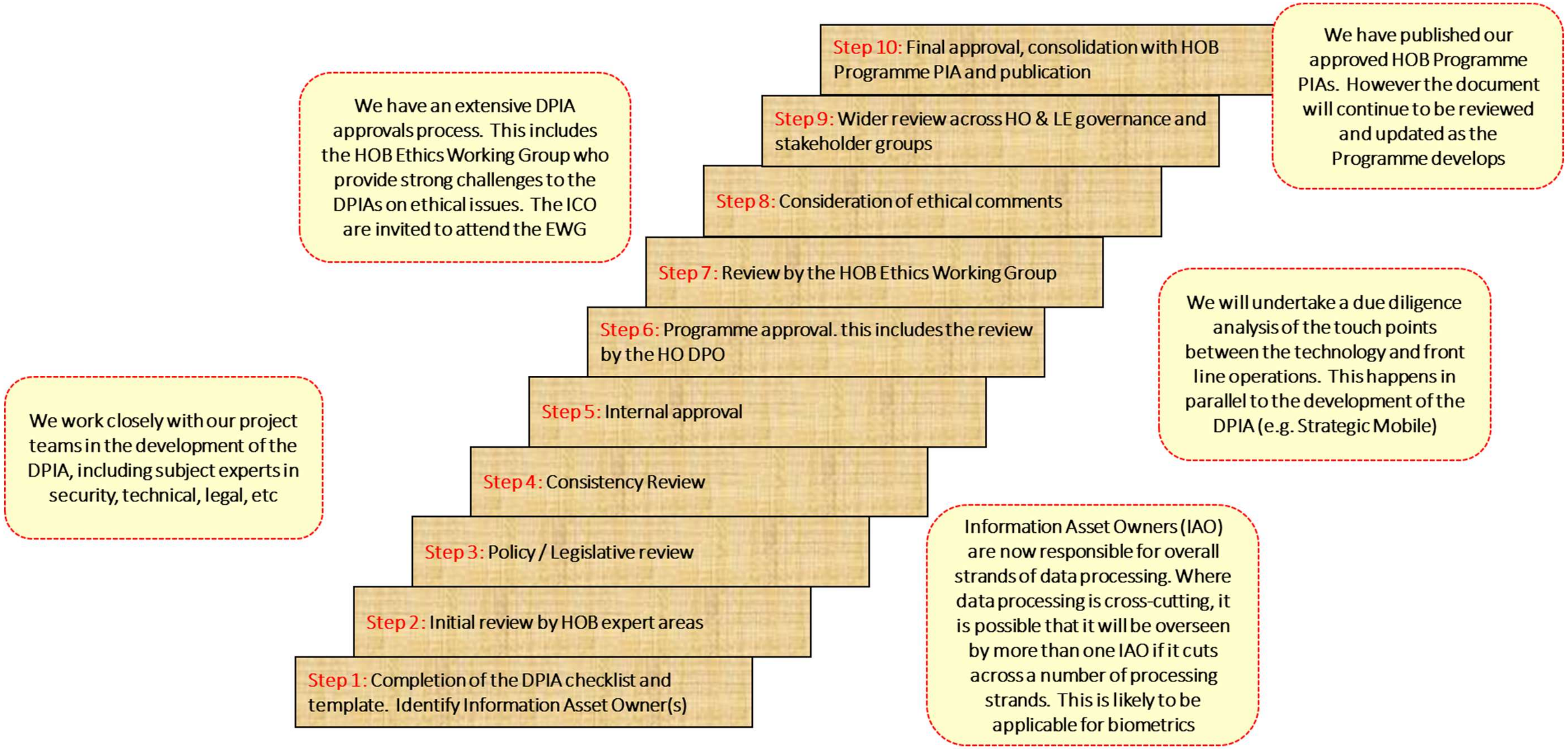
incorrect decision made against them	However, the risk of error is very important. There will be ethical consideration of each project to identify any aspects of the technology (or process) that might impact on an individual through their information being incorrectly linked to another. The risk assessment will identify any mitigating actions that a project might need to address. The technology is designed to enable records to be amended and/or deleted as appropriate where cases of incorrect information are identified.		contract is awarded and the logical separation of data within the Strategic Matcher – where data will be combined – will continue to manage data along lines of business only and not aggregate personal records. The technology is designed to enable records to be amended and/or deleted as appropriate where cases of incorrect information are identified.
There is not a consistent, central Programme overview of personal information management or privacy risk	Privacy is a prime consideration for the HOB Programme and all HOB projects and a DPIA is developed in all cases. Governance is in place with HOB and the wider Home Office and operational businesses where privacy matters are considered.	The risk is **eliminated**	**April 19 update:** The HOB Programme continues to complete and review DPIAs for biometric systems and put these through the wider approvals route which now incorporates the Home Office Data Protection Officer. HOB has invested a lot of work to make sure that it is compliant with the DPA18, and continues to work with the Home Office Data Protection Officer and ICO. HOB also has a Data Protection Practitioner (DPP) embedded within the Programme (and within the Home Office DPP Network) to provide advice and support on DPA18 issues.
A hack into the HOB system could impact on the protection of personal information. The potential damage of a hack is greater within the integrated system, rather than the current smaller constituent parts in the siloed system	HOB ensures that the biometric technology and service management has appropriate security environment for biometric information. As the new suppliers are brought on board this will continue to be a key feature of the contract arrangements. Through the security features of technology every effort is made to	The risk is **reduced**	**April 19 update:** As stated at the time of publication, HOB ensures that the biometric technology and service management has appropriate security environment for biometric information. As the new suppliers are brought on board this will continue to be a key feature of the contract arrangements.

	protect HOB systems from an intrusive attack on personal data from hackers.		Through the security features of technology every effort is made to protect HOB systems from an intrusive attack on personal data from hackers. The internal governance within HOB, through the Security Working Group (SWG) network, monitors the security and protection of HOB systems.

Key questions posed by this paper

- Does the approach taken by HOB provide Open Space with the assurance that privacy and ethics are being appropriately considered by the programme?
- Are there any privacy and ethical risks that Open Space feel should be included for further consideration by the HOB Programme?
- Do Open Space have any insights and/or feedback on privacy and ethics that they feel would be helpful for the HOB Programme to include in their approach?

Annex A – the HOB approach to developing DPIAs



Step 1: Completion of the DPIA checklist and template. Identify Information Asset Owner(s)

Step 2: Initial review by HOB expert areas

Step 3: Policy / Legislative review

Step 4: Consistency Review

Step 5: Internal approval

Step 6: Programme approval. this includes the review by the HO DPO

Step 7: Review by the HOB Ethics Working Group

Step 8: Consideration of ethical comments

Step 9: Wider review across HO & LE governance and stakeholder groups

Step 10: Final approval, consolidation with HOB Programme PIA and publication

We work closely with our project teams in the development of the DPIA, including subject experts in security, technical, legal, etc

We have an extensive DPIA approvals process. This includes the HOB Ethics Working Group who provide strong challenges to the DPIAs on ethical issues. The ICO are invited to attend the EWG

We have published our approved HOB Programme PIAs. However the document will continue to be reviewed and updated as the Programme develops

We will undertake a due diligence analysis of the touch points between the technology and front line operations. This happens in parallel to the development of the DPIA (e.g. Strategic Mobile)

Information Asset Owners (IAO) are now responsible for overall strands of data processing. Where data processing is cross-cutting, it is possible that it will be overseen by more than one IAO if it cuts across a number of processing strands. This is likely to be applicable for biometrics