

2020

JOINT BORDER ANALYTICS

Privacy Impact Assessment:

Joint Border Analytics (JBA) Single Agency Analytics Activities

28 May 2020

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Contents

1. Document control.....	3
2. About this PIA.....	4
2.1. Purpose and scope.....	4
2.2. PIA development process	4
2.3. Related documents	5
3. Background.....	5
3.1. Joint Border Analytics	5
3.2. Roles of the border agencies	5
3.3. The case for border analytics.....	6
4. Relevant legal and policy frameworks.....	7
4.1. Border agency legislation.....	7
4.2. Privacy Act.....	8
4.3. Principles for the safe and effective use of data and analytics.....	9
4.4. Risk-based approach: Preventing data <i>misuse</i> and <i>missed use</i>	10
5. Use of personal information.....	10
5.1. Personal information in scope for JBA analytics activities.....	11
5.2. JBA single agency products	11
6. Privacy and ethics assessment	12
6.1. Governance and accountability	12
6.2. Information privacy principles	14
6.3. Principles for the safe and effective use of data and analytics.....	25
7. Summary of recommendations and action plan	28
8. Appendix 1: Suggested single agency PIA process	32

1. Document control

Document verified by:

Name	Title	Date

Distribution list for review:

Version	Reviewed by
0.1	s 9(2)(g)(ii) OIA
0.2	As above
0.3	As above, and s 9(2)(g)(ii) OIA
0.4	

Document history:

Version No	Date	Updated by	Description of changes
0.1	10/4/2020	s 9(2)(g)(ii) OIA	Initial draft
0.2	25/4/2020		Update to incorporate V0.1 review feedback
0.3	28/5/2020		For circulation to NZCS legal, privacy and policy staff
0.4	20/6/2022		Update to reflect current operating environment and provide clarification around use of third party data.

2. About this PIA

2.1. Purpose and scope

A Privacy Impact Assessment ('PIA') is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.

This PIA analyses the potential privacy impacts of single agency analytics activities undertaken by Joint Border Analytics ('JBA') on behalf of a single border agency. It focuses on the privacy implications raised by a border agency using JBA to analyse its own data for the purposes of better managing and delivering its border enforcement responsibilities. It specifically excludes from scope any joint border analytics activities that might require border agencies to share personal information in order to meet joint border enforcement objectives.

The PIA considers these implications within a wide legal context, incorporating the border agencies' enabling legislation, the Privacy Act and the *principles for safe and effective use of data and analytics* adopted by the Privacy Commissioner. It also takes a risk-based approach, acknowledging that privacy is one of several risks border agencies must consider and address.

While information security is an important aspect of the wider privacy framework, this PIA is not a security assessment. It will highlight, at a high level, where security considerations arise and should be addressed, but it will not provide a detailed assessment of any security or technical risks that the use of JBA for single agency analytics might create.

The PIA will acknowledge privacy risks created by border agency use of JBA single agency products, but it will not address these in significant detail, as these are risks each border agency must manage according to its own enabling legislation, processes and risk appetite.

Finally, the PIA makes a number of recommendations that JBA has already addressed in its existing structure, process and procedure. It does this to ensure that the overarching risk assessment is comprehensive and complete. Where recommendations or risks have already been addressed, this will be acknowledged in the recommendations and actions table included at section 7.

2.2. PIA development process

This PIA has been developed based on:

- review of existing JBA documentation, including previous PIAs;
- conversations with JBA staff;
- feedback from border agency legal teams;
- feedback from border agency Privacy Officers;
- feedback from JBA leadership team; and
- conversations with the Office of the Privacy Commissioner.

2.3. Related documents

The following documents are relevant to this PIA:

- Initial Overarching JBA PIA (20 November 2017)
- PIA on Joint Border Analytics prepared for AISA (30 May 2019)
- Simply Privacy Memorandum on Facilitating Single Agency Analytics (11 March 2020)
- Existing JBA Standard Operating Procedures

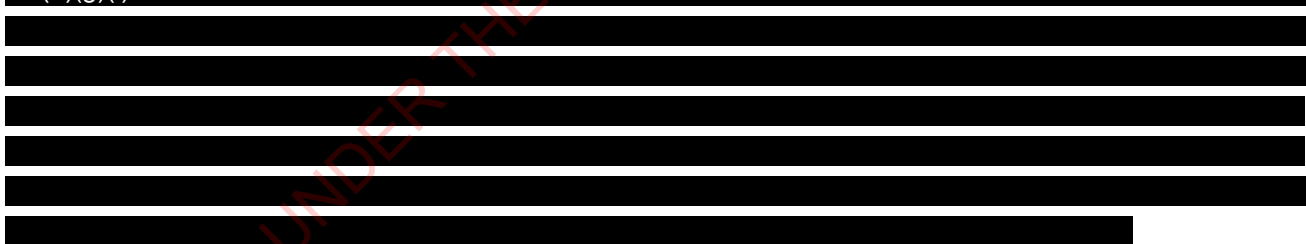
3. Background

3.1. Joint Border Analytics

JBA was initially set up with the intention of agencies delivery multi-agency data analytics projects which might involve the sharing of personal information between JBA agencies. For this reason, JBA set up an Offline Analytics Environment ('OAE') which was designed to ensure a high level of security, accountability and control. A set of comprehensive and restrictive Standard Operating Procedures ('SOPs') were developed and access to the OAE was strictly limited.

At this time, a PIA process was also developed for JBA that was intended to address the wider risks associated with delivering multi-agency data analytics projects that might require the sharing of personal information between a number of government agencies. The process used a general enterprise-wide Customs PIA template and required JBA to complete a PIA at the data ingestion stage and another PIA before deploying any outputs (such as identifiable risk profiles or tools) into operation.

s 9(2)(g)(i) OIA

A large section of the document is redacted with black bars, covering approximately seven lines of text.

3.2. Roles of the border agencies

Customs

Customs provides essential border services and infrastructure that protect New Zealand and advance our economy. It has three core functions:

- protecting New Zealand's border from a wide range of risks, such as illicit drugs, objectionable material and illegal weapons;
- promoting and facilitating secure and efficient trade and travel; and
- collecting Crown revenue.

MPI

The Ministry for Primary Industries ('MPI') plays a critical role (through Biosecurity New Zealand) in preventing unwanted organisms from establishing in New Zealand. It manages border and compliance activities as well as preparing for, and responding to, any biosecurity incursions that may occur. MPI is also responsible for:

- facilitating the entry of New Zealand-produced animal products into overseas markets by providing controls and official assurances of product safety;
- ensuring only registered wine exporters export safe and suitable wine;
- regulating food importers; and
- authorising the importation of veterinary medicines, agricultural chemicals and toxic agents.

MBIE

The Ministry of Business, Innovation and Employment ('MBIE') manages (through Immigration NZ ('INZ')) the immigration system, with the aim of balancing the national interest and rights of individuals. Immigration (the conditions on which New Zealand citizens travel to and from New Zealand) supports our economic growth and our relationship with other parts of the world. INZ's functions include:

- managing the border;
- working with industries and regions to help meet skill needs;
- deciding applications for visas and for protection;
- supporting migrant and refugee settlement;
- carrying out regulatory compliance services; and
- verifying the identity of non-New Zealand citizens.

3.3. The case for border analytics

Every day goods, craft or people that cross New Zealand's border are potentially carrying or represent threats that could damage New Zealand's wellbeing. Increasingly, border agencies are using information they receive in advance of goods, craft or people arriving to assess their risk. This approach helps them identify high-risk goods, craft or people before their arrival and to decide what level of intervention will be necessary.

Border security includes focusing resources into assessing, targeting, and intercepting incoming and outgoing goods, craft or people that pose a risk, while expediting processing of those that do not. To do this, the border agencies collect information from various sources before, as and after goods, crafts or people cross the border. The information collected is analysed and assessed against established risk profiles so that risks to border security can be intercepted and mitigated as early as possible.

In October 2018, the New Zealand Government completed an assessment of the use of algorithms¹ – described as automated decision-making processes used by computer programmes to identify patterns in data. Algorithms are a fundamental element of data analytics. Operational algorithms interpret large amounts of data to materially inform operational decisions or processes. The report noted that algorithms "have an

¹ Stats NZ (2018). Algorithm Assessment Report. Retrieved from <https://data.govt.nz/use-data/analyse-data/government-algorithm-transparency-and-accountability/>.

essential role in supporting the services that government provides to people in New Zealand and in delivering new, innovative, and well targeted policies to achieve government aims”.

JBA was established to assist in informing risk assessment at the border, creating efficiencies by leveraging the risk and intelligence capability, initiatives and tools available to Customs, MPI and MBIE. The output of this data analytics work is intelligence as well as analytics models, data enriched products, and forecasts. The products created by JBA will inform operational activities, such as the refinement of targeting rules or initiation of investigations. To date, several single agency analytics activities have been completed by JBA for border agencies.

4. Relevant legal and policy frameworks

Border agencies must consider a range of legal and policy frameworks in order to determine whether analytics activities are legitimate and lawful. In some cases, border agencies are permitted by their enabling legislation to use personal information for the purpose of analytics that supports their statutory functions. Such statutory provisions override the Privacy Act in respect of data use. However, border agencies must also consider the application of broader legal frameworks – including the information privacy principles (‘IPPs’) – to the entire information lifecycle of an analytics activity. Further, frameworks are now emerging to set guard rails around the use of analytics, algorithms and artificial intelligence. Border agencies must also ensure that their analytics activities, while lawful, meet these higher ethical standards.

4.1. Border agency legislation

Customs and Excise Act

The Customs and Excise Act 2018 (‘C&E Act’) gives Customs a wide mandate to collect and use personal information for the purposes of carrying out its functions under the C&E Act or any other enactment. This statutory authority overrides principles 2 and 10 of the Privacy Act and permits Customs to collect and use any personal information it deems necessary for these broad purposes. Importantly, section 303(2) of the C&E Act states quite clearly that the information privacy principles in the Privacy Act do not limit the use or disclosure of personal information by Customs in the carrying out of its functions.

This means that any analytics activities undertaken for the purpose of detecting, understanding and targeting border risk would be permitted by the C&E Act. Further, the C&E Act would generally permit – subject to natural justice considerations – Customs to use the outputs of such analytics for operational enforcement purposes.

Biosecurity Act

Like the C&E Act, the Biosecurity Act 1993 gives MPI a wide mandate to collect and use personal information, including information held in the Joint Border Management System (‘JBMS’) for the purposes of carrying out its statutory functions. This statutory authority overrides principles 2, 3 and 10 of the Privacy Act and permits MPI to collect and use any personal information it deems necessary for these broad purposes. Interestingly, sections 41(4) and 142(H) of the Biosecurity Act expressly permit MPI to use personal information, including

border information obtained from the JBMS, for the purpose of examining risk patterns and risk profiles in relation to goods, people, craft, imports or exports.

This means that any analytics activities undertaken using data collected under the Biosecurity Act, for the purpose of identifying risk patterns or creating risk profiles, in order to target enforcement actions and generally carry out statutory functions, would be permitted by the Biosecurity Act.

Immigration Act

While the Immigration Act 2009 does not provide INZ with equivalent wide powers to *share* personal information with other border agencies, it does provide INZ with express statutory authority to collect and use personal information (including biometric information) in certain circumstances. Part 8 of the Immigration Act is intended to enable the collection and use of personal information to detect immigration fraud and identify people who are failing to comply with their immigration-related obligations, including visa conditions. It also facilitates controlled information sharing, where this is required for INZ to administer the Immigration Act.

It is likely, therefore, that any analytics activities undertaken for the purpose of detecting immigration fraud and identifying non-compliance would be permitted by the Immigration Act.

4.2. Privacy Act

In the absence of specific legislation that permits border agencies to collect or disclose personal information, the Privacy Act and IPPs apply, and any information use must comply with them. The IPPs are a flexible set of principles intended to ensure that agencies can achieve their goals in a privacy protective way. In summary, they require an agency to:

1. **Scope** – Collect only the personal information it needs for a lawful purpose connected with its functions.
2. **Source** – Collect personal information directly from the person concerned, unless an exception applies.
3. **Notice** – Tell people certain things when collecting personal information directly from them.
4. **Manner** – Collect personal information in ways that are lawful and, in the circumstances, fair and not unreasonably intrusive.
5. **Security** – Take reasonable steps to protect personal information from harm.
6. **Subject access** – Give people access to the personal information it holds about them.
7. **Correction** – Let people correct personal information if it is incorrect.
8. **Accuracy** – Take reasonable steps to ensure personal information is accurate and up-to-date before using it.
9. **Retention** – Retain personal information for no longer than is required.

10. **Use** – Use personal information only for the purposes for which it was collected, unless an exception applies.
11. **Disclosure** – Not disclose personal information, unless an exception applies.
12. **Unique identifiers** – Take care when assigning or using unique identifiers.

Single agency analytics activities that are not operated under clear statutory authority must comply with principle 10 in particular. Regardless of the legal basis for the analytics, all activities must comply with principle 5, principle 8, and principle 9. While most single agency analytics activities will use personal information already collected by the border agency, any activities that require the collection of new personal information will also need to comply with principle 1, principle 2 and principle 4.

Many IPPs – including principles 2 and 10 – contain exceptions that ensure legitimate information processing is possible. Thus, even where a border agency’s enabling legislation is silent on the matter of using personal information for analytics activities, the Privacy Act is likely to permit it, provided that it is necessary and proportional and relates to the agency’s lawful functions.

Compliance with principles 1, 2, 4 and 10 will generally need to be assessed at the *activity level*, whereas compliance with principles 5, 6, 7, 8 and 9 should generally be assessed at the *JBA level*. This is reflected in the privacy and ethics assessment below.

4.3. Principles for the safe and effective use of data and analytics

In May 2018, the Privacy Commissioner and Government Chief Data Steward released a set of *principles for the safe and effective use of data and analytics* (“Analytics Principles”),² intended to promote transparency and a best-practice approach to the use of data and analytics for supporting operational decision-making.

1. **Deliver clear public benefit** – it’s essential government agencies consider, and can demonstrate, positive public benefits from collecting and using public data.
2. **Ensure data is fit for purpose** – using the right data in the right context can substantially improve decision-making and analytical models, and will avoid generating potentially harmful outcomes.
3. **Focus on people** – keep in mind the people behind the data and how to protect them against misuse of information.
4. **Maintain transparency** – transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.
5. **Understand the limitations** – while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.

² <https://www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/>.

6. **Retain human oversight** – analytical processes are a tool to inform human decision-making and should never entirely replace human oversight.

As with principles 1, 2, 4 and 10 of the Privacy Act, compliance with the Analytics Principles will generally need to be assessed at the *activity level*, though JBA's general processes and procedures should be designed to facilitate such compliance.

4.4. Risk-based approach: Preventing data *misuse* and *missed use*

The Privacy Act anticipates a risk-based approach. Section 14 of the Privacy Act requires the Privacy Commissioner (when performing his or her functions) to have due regard to “social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way”.

This recognises that, while clearly important, privacy is one of many risks border agencies must manage. Where agencies are under a statutory duty to deliver critical public services - such as border protection, anti-terrorism initiatives, and public safety - they must also ensure that they take all reasonable and lawful steps to deliver these services effectively and efficiently.

Border agencies have a responsibility to protect personal information against *misuse*, but they also have a duty to avoid the *missed use* of data legitimately collected or generated for lawful border protection purposes. The line between preventing misuse and tackling the risk of missed use is set, to some extent, by public acceptance and expectation. It is determined by the ability to show clear public benefit. Transparency is therefore important.

On balance, border agencies should embrace data analytics, as a way to better deliver their statutory functions, but should do so openly and safely, being mindful of the people behind the data.

5. Use of personal information

JBA will be provided with secure access to information, including personal information, held by the border agency that has requested analytics. JBA might use *any* personal information held by that border agency for the purposes of the analytics activity, subject to the agency's enabling legislation and any limitations set by the Privacy Act. JBA will then use this information to create the analytics products outlined below, as requested by the border agency.

Border agencies provide JBA with access to the personal information they hold only to enable JBA to analyse and process this data on their behalf, and develop the products set out below. JBA does not use the information for its own purposes, and makes no decisions about how the products it creates with the information should be used or operationalised. In this way, JBA operates as an analytics *service provider* for the border agencies.

For single agency analytics activities, JBA will access and manipulate border agency data within the relevant border agency system, including cloud-based platforms procured by that agency for the purposes of an analytics activity. No data will be transferred to another border agency system for the purposes of an activity.

5.1. Personal information in scope for JBA analytics activities

Existing single border agency data

The types of personal information JBA has access to will depend on the requirements of the border agency, and will be limited to that information that may lawfully be used by the relevant border agency for the purposes of the analytics activity it is intended to support. This will include, for example (and depending on the border agency that has requested services), information relating to:

- enforcement actions/fines including deportation orders and seized goods or detained persons;
- movements of goods, craft and people;
- biometric information;
- unaccompanied baggage and passports left on craft;
- Information associated with intelligence activities;
- applications for visas;
- applications to import/export agricultural machinery, compounds, veterinary medicines, animal products, food, wine and animals; or
- applications to import or export marine mammals, endangered species and wildlife.

More detailed information for identity resolution

In some circumstances, additional biographical information may be needed to assist with resolving the identities of individuals. If the identities are too broad (e.g., just a first and last name), there is a risk that a model will not match individuals correctly across the various border agency datasets – resulting in defective analytics models. In most cases, the more detailed information will only be used for the purposes of identity resolution. As noted below, identity resolution is an important accuracy safeguard, for the purposes of principle 8 of the Privacy Act.

External datasets

For the most part, the personal information JBA uses for the purposes of analytics activities will be information the border agency has already collected under its enabling legislation. However, it is anticipated that occasionally JBA or the border agency might identify the need to collect and use new information, including personal information, for the purposes of the activity. For example, an activity might require the collection of standalone datasets from equivalent overseas border agencies, or open source data s 6(c) OIA

5.2. JBA single agency products

JBA offers the following analytics products to single border agencies:

1. **Data enriched products** – Raw data – which may include personal information – that has been refined, enhanced, improved or enriched using tools to help improve quality issues in data entry.

2. **Analytics models and forecasts** – Models that can identify a class of goods, craft or people that present an increased or decreased risk at the border and forecasts that identify probable risk patterns or likelihoods. While personal information may be used to develop these products, the outputs will not be identifiable.
3. **Identifiable intelligence products** – Products that identify relationships and behaviours that may indicate specific offending by individuals, entities and industries. Personal information will be used to develop these products and the outputs will usually be identifiable.

All these products may use identifiable personal information but only the third category is likely to result in the provision of identifiable intelligence (such as lists of individuals presenting a particular risk) to operational units of the border agency. The border agency will determine how it may lawfully use these products, in accordance with its enabling legislation, the Privacy Act, and its own processes and risk appetite.

JBA data scientists and modelling analysts use the Cross Industry Standard Process for Data Science (CRISP-DM) on the data. CRISP-DM is an open standard process model that describes common approaches used by data mining experts. It is the most common methodology used by analytics teams worldwide. The CRISP-DM process has six stages – business understanding, data understanding, data preparation, modelling, evaluation, and deployment.

6. Privacy and ethics assessment

The following assessment considers the impact JBA single agency analytics activities may have on compliance with the Privacy Act, the IPPs and the Analytics Principles, and makes recommendations to address any risks or gaps identified.

6.1. Governance and accountability

JBA will only act on the request of a border agency, and will not use border agency data for its own purposes. Section 3(4) of the Privacy Act states that, where an agency holds and processes personal information solely on behalf of another agency, the information is deemed to be held by that other agency.

The practical effect of this provision is that the sharing of personal information with JBA (as a service provider) is deemed to be a use by the border agency, not a disclosure. However, because JBA is not an independent entity – it is located within a Customs building and infrastructure and is staffed by employees of Customs, MPI and MBIE - it is important that this service provider status is demonstrated in practice, through clear agreement, policy and process.

Rec-001: Develop a Service Level Agreement between JBA and each border agency that clarifies roles and responsibilities and captures the parties' agreement to these.

Each border agency must be accountable for the way it uses JBA to carry out analytics activities with the personal information it holds. It must be independently satisfied that an analytics activity is lawful and necessary and that any outputs from the activity are used lawfully and proportionately. As the subject matter expert, JBA is in a strong position to, and must, assist the border agencies to assess the lawfulness of activities. However, it cannot make this assessment on their behalf. Ultimately, the border agency must own and be

accountable for this risk. The border agency's own operational or project governance procedures will apply here.

In practice, this will require JBA and the border agency to collaborate to ensure that reasonable steps are taken to assess privacy risk at the activity level. Such an assessment can be conducted in an efficient manner and it is suggested that a Single Agency PIA³ should take place where the activity is likely to result in the development of identifiable intelligence products. The border agency's privacy officer or privacy team must be involved in this process. Activity sign-off levels should be proportional to risk.

Rec-002: Develop a collaborative PIA process that ensures JBA and the border agency properly assess privacy risk and clear lines of accountability are maintained. See Model Process at Appendix 1.

In some circumstances, JBA may be requested by a border agency to deliver identifiable outputs urgently, such as in response to specific tactical needs, where operational business units require identifiable risk profiles or intelligence products immediately in order to respond to an existing or imminent border threat. It is reasonable to expect that in these cases a less robust risk assessment process can be applied to the use of information. However, it is critical to note that the border agency requesting such an activity must be aware of, and accept, the higher privacy risks it creates.

It is suggested that the single agency PIA process developed in accordance with Rec-002 should provide for the ability to record urgency and capture a clear decision by the border agency to suspend the privacy risk assessment. However, where practicable, the border agency should be encouraged to resume and complete that risk assessment after the fact. Such decisions should require manager level (or above) authorisation from the requesting border agency.

Rec-003: Allow for the suspension of a PIA for analytics requests that have clear operational urgency, subject to senior authorisation from the requesting border agency.

The characterisation of JBA as a service provider does not absolve it of privacy or ethical obligations. As the subject matter expert, JBA must ensure that the analytics activities it undertakes on behalf of the border agencies comply with the IPPs and Analytics Principles. With respect to many of these principles, JBA will be in a better position to ensure compliance than the border agency. Further, JBA must be as transparent as possible about the data used and the algorithms developed, to enable the border agencies to make meaningful decisions about the lawfulness, fairness and proportionality of the analytics.

Rec-004: Ensure that JBA Standard Operating Procedures (SOPs) reflect and maintain JBA's role and responsibilities, including limitations on data use and obligations to assist border agencies with the assessment of privacy and ethical risk.

The responsibilities of both JBA and the border agencies in respect to each privacy and ethical requirement or risk is outlined in detail below.

³ Using the Single Agency Privacy Impact Assessment Template - (DATA OUT) module.

6.2. Information privacy principles

Principle 1

Principle 1 states that agencies should collect only personal information that is necessary for a lawful purpose connected with their functions. There are no exceptions to this principle.

In the vast majority of cases, single agency analytics activities will not require the collection of new personal information. Rather, these activities will use and analyse existing datasets held by the requesting border agencies. In these cases, principle 1 will not be engaged.

However, as noted above, occasionally JBA or the requesting border agency might identify external datasets, not currently held by the border agency, that may be useful for the purposes of the activity. Where these datasets do not contain personal information, principle 1 will not be engaged. Where they do contain personal information, JBA and the border agency must ensure that the information collected for the activity is limited to that which is necessary for the purposes of the activity. This is an assessment that must be made at the *activity level*.

Rec-005: Ensure that the single agency PIA process requires JBA and the border agency to limit new personal information collected to that which is necessary for the activity.

In some cases, even where no new personal information is collected from another source, data enrichment and entity resolution processes may result in the *creation* of new personal information by, for example, making connections between individuals and records that did not previously exist, or by generating new identifiable risk profiles. This is lawful, and permitted by principle 1, provided that the creation of this new information is demonstrably necessary for the purposes of the activity.

Rec-006: Ensure that new information created as a result of an analytics activity is necessary for the purposes of the activity. If it is not, delete it or remove it from the analytics dataset.

While principle 1 focuses on the collection or creation of new personal information by a border agency (rather than access to or use of existing personal information), similar data minimisation concepts apply across the information life cycle (that is, an agency should only use or share the minimum amount of personal information necessary to achieve its purposes).

In the initial stages of an analytics activity, JBA will need to explore and assess relatively wide datasets, to establish how relevant or useful each dataset, or field of personal information, will be. Provided that some effort is made in later stages of the analytics activity to remove datasets or data fields that are not found to be of value, this would still comply with general data minimisation principles.

It should also be noted that an activity's data needs could evolve as data exploration progresses, and so it may be identified that an activity will require more datasets, not less. Provided that some connection can be made between the additional datasets and the lawful goals of the activity, this would be lawful.

Rec-007: Ensure JBA continuously reassesses and refines the personal information used for an analytics activity, to support data minimisation.

Principle 2

Principle 2 states that agencies should collect personal information directly from the individual concerned, unless an exception applies.

In the vast majority of cases, single agency analytics activities will not require the collection of new personal information. Rather, these activities will use and analyse existing datasets held by the requesting border agencies. Existing datasets may also include third party datasets that have been collected by the border agency in accordance with a lawful power **s 6(c) OIA**

In these cases, principle 2 will not be engaged.⁴

However, as noted above, occasionally JBA or the requesting border agency might identify other external datasets, not currently held by the border agency, that may be useful for the purposes of the activity. Where these datasets do not contain personal information, principle 2 will not be engaged. Where they do contain personal information, the border agency must ensure that it has a lawful basis to collect this information from a source other than the individuals concerned. This is an assessment that must be made at the *activity level*.

Usually, this will be permitted by the border agency's enabling legislation (for example, section 302 of the C&E Act states that Customs may collect any border information, despite principles 2 and 3 of the Privacy Act). Where it is less clear that the enabling legislation applies, the border agency will need to establish that an exception to principle 2 would apply to permit the collection. Relevant exceptions to principle 2 would include:

- **Principle 2(2)(a)** – that the information is publicly available information. This may apply to the collection of information already in the public domain.
- **Principle 2(2)(d)(i)** – that the collection from another source is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation and prosecution of offences. This may apply to the collection of information for the purposes of generating identifiable intelligence.
- **Principle 2(2)(g)(ii)** – that the information will be used for statistical or research purposes and will not be published in a form that will identify the individual concerned. This may apply to the collection of information for the purposes of generating risk forecasts and analytical models.

Rec-008: Ensure that the single agency PIA process prompts border agencies to ensure that they have a lawful basis to collect new personal information from a source other than the individual concerned.

Principle 3

Principle 3 states that, when collecting personal information from individuals directly, agencies should provide notice about how that information will be used and who it may be shared with.

JBA will never collect personal information directly from the individuals concerned. It is also highly unlikely that requesting border agencies would collect personal information directly from individuals for the sole

⁴ The focus on compliance will be oriented to IPP10; whether the use is compliant.

purpose of a single agency analytics activity. Rather, and as noted above, these activities will usually use personal information that is already collected and held by the requesting border agencies.

However, while individual analytics activities will not generally require the development of specific notices pursuant to principle 3, border agencies should provide the public with some indication in their existing privacy notices that the personal information they collect may be used for data analysis, algorithm develop and risk profiling, for the purposes of carrying out their statutory functions, including border enforcement activities.

Rec-009: Border agencies should review their public privacy notices to ensure that they are generally open about the use of personal information for data analytics and profiling.

Principle 4

Principle 4 states that agencies should collect personal information in ways that are lawful and, in the circumstances, not unfair or unreasonably intrusive. The Privacy Act 2020 also introduced an additional requirement for agencies to consider the vulnerability of young people when deciding how to collect personal information.

In the vast majority of cases, single agency analytics activities will not require the collection of new personal information. Rather, these activities will use and analyse existing datasets held by the requesting border agencies. In these cases, principle 4 will not be engaged.

However, as noted above, occasionally JBA or the requesting border agency might identify external datasets, not currently held by the border agency, that may be useful for the purposes of the activity. Where these datasets do not contain personal information, principle 4 will not be engaged. Where they do contain personal information, JBA and the border agency must ensure that the information is collected in a manner that is lawful, fair and not unreasonably intrusive. It is unlikely that the collection of personal information from most sources will breach principle 4, but this is an assessment that must be made at the *activity level*.

Rec-010: Ensure that the single agency PIA process requires JBA and the border agency to ensure new personal information is collected in compliance with principle 4.

Principle 5

Principle 5 states that agencies should take reasonable steps to protect personal information from loss, unauthorised access and disclosure, or misuse. The Privacy Bill will introduce an additional requirement to notify the Privacy Commissioner and affected individuals of any failure to do so that is likely to cause serious harm.

JBA intends generally to conduct single agency analytics activities within the relevant border agency's systems. This will reduce the information security risk as datasets will not need to be transferred out of the border agency's systems, and will not be stored or accessed in third party systems.

However, JBA must still address several remaining security risks that will be present even where analytics datasets are manipulated within border agency systems.

Managing JBA access to border agency systems

Currently, specific border agency staff working within the JBA team will access information held by their employer border agency for the purposes of completing the analytics activity. This model is highly privacy protective, and clearly removes any risk of the disclosure of personal information to non-border agency employees.

s 9(2)(g)(i) OIA

s 9(2)(g)(i) OIA

- Section 271 of the C&E Act permits the Chief Executive of Customs to authorise a suitable person who is not a Customs Officer to carry out the functions of a Customs Officer.
- Section 103 of the Biosecurity Act permits a chief technical officer appointed by the Director-General of MPI to appoint an authorised person to administer and enforce the provisions of the Biosecurity Act.
- Section 388 of the Immigration Act permits the Chief Executive of Immigration NZ to designate employees of other NZ government departments as immigration officers, and may specify the functions and powers of that officer.

s 9(2)(g)(i) OIA

Rec-011: Consider whether border agencies can use their legislative powers to expressly authorise JBA staff employed by other border agencies to access their systems and data.

Rec-012: Set appropriate limits on JBA staff access to border agency systems, to mitigate the risk of misuse of personal information.

Applying general organisational and technical security measures

Regardless of the approach JBA and the border agencies choose to take to managing JBA staff access to border agency systems, JBA must be able to meet general organisational and technical security measures expected of all public sector agencies. JBA should:

- Ensure that all staff within the JBA team have sufficient organisational clearance levels to view and use border agency data for analytics purposes, and that they are appropriately vetted and security checked before being provided with system access.
- Include in employee or secondment contracts a strict confidentiality clause that requires all JBA staff to maintain the confidentiality of any information they access and use on behalf of a specific border agency, and to refrain from sharing information or outputs with another border agency unless such sharing has been specifically requested by that border agency.
- Set restrictions in the JBA SOPs on JBA staff access to border agency systems or data, to ensure that such access is only for the purposes of a specific border agency analytics activity.
- Develop appropriate privacy and information security training for all JBA staff, including data handling and classification requirements.
- Ensure that JBA understand and adhere to the information security policies and processes of the relevant border agency while working within its systems, and to the more general NZISM and PSR requirements.
- Ensure physical access to the JBA space in Auckland Customhouse is appropriately restricted by policy, process and physical access restrictions, and ensure that all computer terminals and mobile devices are password protected.
- Periodically audit JBA staff access to border agency systems (and particularly JBA staff access to the systems of border agencies other than their employer agency) to ensure that such access is necessary for a specific border agency analytics activity.

Rec-013: Ensure that appropriate policies, processes and controls are in place to meet general organisational and technical security requirements.

Rec-014: Develop and maintain training for all JBA staff that addresses general security requirements and enables staff to recognise and manage a privacy breach in accordance with Rec-016.

Ensuring JBA does not prejudice border agency privacy breach management procedures

The Privacy Act 2020 introduced new mandatory privacy breach notification requirements. From 1 December 2020, all agencies (including public sector agencies) must notify the Privacy Commissioner and any affected individuals of any privacy breach⁵ that it is reasonable to believe is likely to cause serious harm to the affected individuals.

As outlined above, JBA will not generally transfer information to, or store information in, its own systems (unlike in the joint agency analytics activity context). This means that, for the most part, any privacy breaches that occur in respect of a border agency's data will occur *within* that border agency's systems. However, JBA

⁵ Privacy breach is defined as unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information; or an action that prevents an agency from accessing personal information on either a temporary or permanent basis.

staff must be enabled to recognise a privacy breach, so they can notify the border agency of the breach and assist with the management of it.

As a service provider, JBA should not make the assessment as to whether or not a privacy breach should be notified to the Privacy Commissioner or affected individuals. Similarly, JBA should not make the notifications. However, JBA must be able to work with the relevant border agency and assist with such notifications.

Rec-015: Ensure Service Level Agreement provides assurance that JBA will notify an affected border agency of any privacy breach that might impact that border agency's personal information.

Rec-016: Develop a JBA process to manage the identification, management and notification of a privacy breach within a border agency system.

Taking care when using new cloud providers

As noted above, some analytics activities may require JBA, on behalf of the relevant border agency, to use third party cloud-based software or platforms to store or process personal information for the duration of the activity (and possibly beyond). While these providers will be used from within the border agency environment, JBA must ensure that it complies with the relevant border agency's third party procurement policies and procedures. These will generally require a robust risk assessment that should take into account the sensitivity of the data being stored or processed by the provider, the jurisdiction within which the data will be stored or processed, and the privacy and security protections the provider can offer.

Rec-017: Ensure that the use of third party cloud providers for the purposes of an analytics activity complies with border agency procurement policies and procedures, is risk-assessed and has been approved by the relevant border agency.

Principle 6

Principle 6 provides individuals with the right to request a copy of the personal information an agency holds about them.

It is possible that individuals may become aware of particular analytics activities as a result of enforcement action against them that has been informed by identifiable outputs. Further, if an individual makes a request to a border agency for *all the personal information* that agency holds about them, this would capture any identifiable outputs produced by JBA on the agency's behalf. These individuals would be entitled to request a copy of any analytics outputs that identify them, though border agencies may in certain cases be able to withhold this information.

Thus, it is critical that JBA and the border agencies establish a process to ensure these requests can be managed lawfully and efficiently. The decision on whether or not to release the information to the requester must be made by the border agency, not JBA (which is acting as a service provider). However, JBA must be capable of assisting the border agency to manage and respond to the request, including meeting the 20 working day timeframe required by the Privacy Act.

Rec-018: Border agencies should review and amend their subject access request processes to take into account any personal information created by JBA analytics activities.

Rec-019: Ensure subject access requests are referred to the relevant border agency and JBA is able to assist border agencies to collate personal information and respond to such requests.

Principle 6 and algorithmic transparency

While there may be other reasons to provide some level of algorithmic transparency (and these are discussed further below in respect to the Analytics Principles), it is unlikely that principle 6 would be interpreted as giving individuals the right to request an explanation of the algorithm used by JBA to generate identifiable outputs. The algorithm itself would not be personal information about the requester, though it is arguable that in some cases provision of the algorithm might be required in order to provide an individual with *meaningful access* to the output.⁶

In any event, even if it was determined that an individual should be entitled by principle 6 to access an algorithm used to profile them, it is likely that a border agency could withhold this information on the basis that releasing it would be likely to prejudice the maintenance of the law.

Finally, it should be noted that individuals may be able to request information about algorithms under the Official Information Act 1982, in addition to requesting reasons for enforcement or other decisions (including potentially automated or manual decisions to include individuals in intelligence outputs) in accordance with the Ombudsmen Act 1975. Again, however, equivalent law enforcement withholding grounds may apply to protect algorithms from release in certain circumstances. As with Privacy Act requests, such decisions should be made by the relevant border agency.

Principle 7

Principle 7 provides individuals with the right to ask an agency to correct the personal information it holds about them, or to attach a statement of correction to that information.

Where an individual is provided with a copy of analytics outputs that identify them, it is possible that they will seek to challenge these outputs, or the information used to create them, using principle 7. For example, an individual might allege that the information the border agency held about them was out of date or incomplete. The border agency would need to consider this request and either correct the information at issue, or add a statement of correction to it. This could have implications on any previously completed analytics or outputs.

⁶ In *Naidu v Royal Australasian College of Surgeons* [2018] NZHRRT 23, the Human Rights Review Tribunal held that an individual was entitled to the formula or mechanism by which a referee score was reached, on the basis that he could not decipher his score (which was included in a table of scores of other people) without it. The Tribunal stated “[w]hile the scoring mechanism or formula is not personal information, its provision is a condition precedent to being able to access the personal information which is in the table. Without an access key it cannot be said access to the personal information has been given in terms of Principle 6. The access for which that principle makes provision is meaningful access.”

This case can be distinguished from the present circumstances however. Unlike a numerical score, the inclusion of an individual in an intelligence output would not be meaningless in isolation. While the provision of the algorithm might help the individual understand how they ended up being included in such an output, understanding the fact of their inclusion on it would not be contingent on this algorithm.

It should be noted that proper management of individual correction requests constitutes a reasonable step to ensure compliance with principle 8, discussed below.

As with the principle 6 access right, JBA and the border agencies must establish a process to ensure these requests can be managed lawfully and efficiently. The decision on whether or not to correct the information must be made by the border agency, not JBA (which is acting as a service provider). However, JBA must be capable of assisting the border agency to manage and respond to the request, including meeting the 20 working day timeframe required by the Privacy Act.

Responding to a principle 7 request – or indeed a complaint about an alleged breach of principle 8 from an affected individual – might require the border agency to provide some information as to why an individual was identified in an intelligence product. However, the release of such information would need to be managed in accordance with the agency's legitimate need to protect its law enforcement methods and processes, as noted above.

Rec-020: Border agencies should review and amend their correction request processes to manage and respond to requests to correct any personal information created by JBA analytics activities.

Rec-021: Assist border agencies to respond to correction requests, including correcting or updating disputed information and affected outputs.

Principle 8

Principle 8 states that, before using or disclosing personal information, agencies should take reasonable steps to ensure that it is accurate, up-to-date, complete, relevant and not misleading.

Principle 8 is important in the context of data analytics, automated decision-making and the use of algorithms to develop risk profiles that affect individuals. This principle is about data quality, and requires agencies to put processes in place to make sure data is up to standard before using or sharing it, and particularly relying on it to inform operational decisions. It recognises that the failure to use accurate and up to date information can have significant negative impacts on individuals. It is essentially equivalent to Analytics Principle 2 – ensuring data is fit for purpose.

While JBA must, to some extent, rely on the accuracy of personal information held by the border agencies it is delivering services to, there are a number of reasonable steps it can and should take to ensure data is fit for purpose:

- JBA should commit to ensuring that the most recent personal information is used for an analytics activity.
- Where activities require ongoing data analytics, or take a long time to deliver, JBA should regularly refresh the personal information used, to ensure that outputs are based on the most up-to-date and complete information available.
- JBA should apply robust identity resolution processes to minimise the risk of individuals being incorrectly connected with offending, risk patterns or other entities. This may require the collection of additional personal identifiers (as noted above) and the use of unique identifiers to ensure that information and people are correctly matched.

- JBA should assist border agencies to ensure that unwanted biases are removed from datasets before they are analysed, recognising that some lawful bias may be legitimate in certain circumstances, to ensure that an activity is properly targeting risk groups or attributes.
- JBA should ensure that the predictors or attributes used to weight analytics models do not produce unfair or unlawfully discriminatory outcomes. If this is not checked, analytical models could produce personal information that is inaccurate, irrelevant or misleading. This could result in harm to individuals.
- JBA should ensure that analytics datasets are updated in accordance with any corrections made to the source data as a result of individual correction requests made to border agencies (see Rec-021 above).

Rec-022: Ensure personal information gathered and used for an analytics activity is up-to-date and regularly refreshed for the duration of the activity.

Rec-023: Apply robust identity resolution processes to ensure individuals are accurately matched with events, entities or other adverse information.

Rec-024: Ensure datasets identified for use in an analytics activity are assessed for unwanted biases.

It should also be noted that the use of JBA to enrich existing datasets, including by better matching existing data fields and resolving data entry errors, will generally improve the accuracy of personal information relied upon by the border agency. Data enrichment products, therefore, are often likely to lift border agency compliance with principle 8 of the Privacy Act.

Principle 9

Principle 9 states that agencies should retain personal information only for as long as it is required for a lawful purpose.

All border agencies are required to comply with principle 9 of the Privacy Act, and most should have data retention schedules in place that outline retention periods for categories of personal information, that comply with the requirements of their enabling legislation and the Public Records Act 2005. JBA must ensure that analytics activities it manages on behalf of a border agency comply with that border agency's data retention rules. This will be particularly important where datasets are duplicated within the agency systems for the purposes of the activity, or where an analytics activity is ongoing.

In some cases, where there are statutory limitations of the retention of information – such as in relation to PNR data – JBA must ensure that analytics activities are designed and managed in a way that meets these limitations. For example, regular data refreshes and purges can ensure that datasets with limited retention periods are compliant.

Where analytics outputs do not contain personal information – such as models and forecasts – principle 9 of the Privacy Act will not apply. These outputs can be retained in accordance with the border agency's own data retention rules. However, where outputs are identifiable, the border agency will need to ensure that they are retained only for as long as they are required for a lawful purpose. This will be up to the relevant border agency to determine.

Rec-025: Ensure that personal information is retained within border agency analytics environments in compliance with the border agency's data retention rules, and any statutory retention limitations.

Principle 10

Principle 10 states that agencies should only use personal information for the purposes for which it was collected, unless an exception applies to permit another use.

Border agencies must be able to establish that they have a lawful basis to use the personal information they hold for the purposes of an analytics activity. This is an assessment that must be made at the *activity level*.

The vast majority of single agency analytics activities will be permitted by border agency enabling legislation, as outlined in section 4.1 above. Where this is the case, the relevant provisions of the enabling legislation will override principle 10 of the Privacy Act to permit the use of data for analytical purposes. This will generally be the case in respect of non-identifiable outputs such as risk profiles or forecasts.

For the most part, the use of personal information in accordance with a border agency's legislative authority would likely also meet the requirements of principle 10, as border agencies generally collect personal information for the purposes of carrying out their statutory functions. However, where it is clear that an analytics activity is not authorised by enabling legislation, and is not directly related to the purposes for which the personal information was collected, other exceptions to principle 10 might apply:

- **Principle 10(1)(a)** – that the information is publicly available information. This may apply to use of information already in the public domain.
- **Principle 10(1)(c)(i)** – that the use of the information is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation and prosecution of offences. This may apply to the use of information for the purposes of generating identifiable intelligence.
- **Principle 10(1)(f)(ii)** – that the information will be used for statistical or research purposes and will not be published in a form that will identify the individual concerned. This will apply to the use of information for the purposes of generating risk forecasts and analytical models.

Taking a risk-based approach, and to ensure that JBA can deliver analytics services efficiently and effectively, it is recommended that an activity level assessment of use would be required only where personal information will be used to generate identifiable intelligence outputs. This will also require a consideration of proportionality – identifiable intelligence outputs should only be generated where the border risk warrants this level of data use.

Rec-026: Ensure that the single agency PIA process prompts border agencies to ensure that they have a lawful basis to use personal information for the purposes of generating identifiable intelligence outputs.

Issues around the subsequent use of personal information contained in identifiable intelligence outputs is addressed below in respect of Analytics Principles 5 and 6.

Principle 11

Principle 11 states that agencies should not disclose personal information, unless an exception applies that permits the disclosure.

Principle 11 of the Privacy Act is not generally engaged by single agency analytics activities. Personal information will be stored and manipulated within the relevant border agency systems, and outputs will be generated and shared only with that same border agency. Because JBA operates as a service provider, and does not hold or use border agency information for its own purposes, providing JBA staff with access to personal information does not constitute a disclosure. This can be made even clearer by taking steps to authorise JBA staff under enabling legislation as contemplated in relation to principle 5 above.

A border agency may choose to share both identifiable and de-identified outputs with other agencies. This is a decision each border agency must make in accordance with its own policies, operational requirements and risk appetite.

For this reason, it will be important to ensure that outputs not intended to contain personal information, such as risk profiles, models and forecasts, are meaningfully aggregated and anonymised (to minimise the risk of later re-identification). It is also important to ensure that sensitive outputs, or outputs generated out of sensitive datasets, are clearly identified as such with appropriate handling caveats or rules.

Rec-027: Ensure de-identified outputs are meaningfully anonymised, and protected against the risk of re-identification.

Rec-028: Ensure sensitive outputs are released with appropriate handling caveats or rules.

Principle 12

Principle 12 states that agencies should take care when assigning or using unique identifiers, and should not require an individual to disclose a unique identifier that was assigned by another agency.

Personal information used for the purposes of single agency analytics activities should generally include only unique identifiers already assigned by the relevant border agency. In cases where border information contained in the JBMS is used, this may contain unique identifiers assigned by another border agency. However, in this case, the use of these identifiers for border enforcement purposes will be permitted as this is one of the purposes for which such identifiers are assigned.

Further, JBA may generate new unique identifiers within the relevant border agency analytics environment, for the purposes of entity resolution. This would not breach principle 12 of the Privacy Act, provided care was taken in the generation of such identifiers, and these were not subsequently used by the border agency for operational purposes.

Privacy Act complaints

As noted throughout the above assessment, it is very possible that JBA, or the relevant border agencies, will be the subject of complaint to the Privacy Commissioner as these analytics activities become more known to the public. In particular, complaints may follow enforcement actions against individuals that have been informed by JBA identifiable intelligence outputs. They may also be prompted by subject access requests under principle 6 of the Privacy Act.

As with the management of access and correction requests, Privacy Act complaints about single agency analytics activities should be managed in the first instance by the relevant border agency. However, JBA may be required to assist the border agency to respond to a complaint, particularly if it escalates to the Privacy Commissioner or beyond. This will certainly require JBA to be open and clear with the border agency about how a particular algorithm has identified the complainant as high risk. It may also require some transparency with the Privacy Commissioner or even the individual concerned. However, this is a matter that should be managed by the relevant border agency.

Rec-029: Assist border agencies to respond to Privacy Act complaints about the use of personal information for analytics activities.

6.3. Principles for the safe and effective use of data and analytics

1. Deliver clear public benefit

This principle requires agencies to ensure, and demonstrate, that the use of data and analytics have clear and positive benefits for New Zealanders.

All New Zealanders benefit from an effective border security system. People, goods, and craft cross our border every day, potentially carrying prohibited or restricted items, such as drugs and weapons, or biosecurity threats. These could damage our social wellbeing, primary and tourism industries, natural ecosystems, and international reputation. Single agency analytics activities are always intended to facilitate data analytics that will enable border agencies to manage border risk more effectively, safely and efficiently, while ensuring that the movement of legitimate and low risk people, goods or craft is facilitated.

2. Ensure data is fit for purpose

This principle requires agencies to ensure that they use the right data, that can substantially improve decision-making and avoid potentially harmful outcomes.

Refer to content above in respect of principle 8 of the Privacy Act.

3. Focus on people

This principle requires agencies to be mindful of the people behind the data and to protect them against the misuse of information.

This is a very general principle, that supports and references most of the information privacy principles. It requires JBA and the border agencies to ensure that the policies, processes and procedures that drive and safeguard single agency analytics activities are focused to an appropriate extent on protecting individual privacy. The majority of recommendations outlined in this PIA will support compliance with this principle, by promoting concepts of data minimisation, information security, use limitation, fairness and transparency.

4. Maintain transparency

This principle requires agencies to be transparent about the use of data and analytics. Transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.

There must be some public transparency about the fact that JBA exists, that it is assisting border agencies to better use their data, and the general principles and safeguards that are in place to manage such activities. This will be an important step to ensure some social licence for JBA and the services it provides to border agencies. As noted in respect of principle 3 above, border agencies should also be transparent about the fact that they use algorithms to analyse the personal information they hold, to better identify risks and enforce their enabling legislation.

Customs already reports on the use of JBA analytics services in its annual report. This is positive and should be continued. Other border agencies which use JBA could do the same. In addition, JBA could consider developing a public webpage outlining in general terms the services it delivers and the high-level safeguards in place to ensure data analytics are lawful and ethical. This could include publishing this PIA, or a summary of it.

Rec-030: Consider developing a public webpage that provides a general overview of JBA, analytics activities, and the privacy and security safeguards in place.

Rec-031: Consider publishing a summary of this PIA to build public trust and social licence in border agency use of JBA.

Rec-032: Border agencies should be open about their use of JBA analytics services.

Algorithmic transparency is an important trust builder. It may not be appropriate in most cases for JBA or border agencies to be transparent with the public about the specific algorithms used in a particular case. There are legitimate arguments to be made that this could prejudice the objectives of the analytics and enable offenders to subvert intelligence activities.

However, the requesting border agencies must be able to understand the algorithms behind the analytics outputs they are receiving. Such transparency is particularly important where algorithms or analytics are used to inform legal decisions – such as law enforcement decisions – that affect individuals. Most decisions and adverse actions taken by public sector law enforcement agencies will be subject to natural justice requirements, and may be challenged in the courts.

Thus, JBA must be able to explain to a border agency why an identifiable intelligence product has identified, or an analytics model is designed to identify, particular people as presenting a particular risk. Otherwise, a border agency will be unable to meaningfully respond to a challenge to its exercise of a statutory power. Stating “computer says no” will not suffice.

Rec-033: Provide border agencies with an explanation of the algorithms used to generate identifiable intelligence products and assist them to understand specific methods and processes used for an activity.

5. Understand the limitations

This principle requires agencies to remember that, while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.

Border agencies must remember that JBA outputs are only an element of the wider intelligence picture. They can inform operational activities, and enforcement decisions, but they should not be relied upon in isolation. This is particularly important where identifiable intelligence outputs are produced. Operational decision-

making by border agencies must be fully informed and must be cognisant of potential biases present in any JBA models or outputs. Over-reliance on any analytical models or outputs risks perpetuating biases in the source data or harmful or discriminatory outcomes for individuals.

Rec-034: Ensure border agency units that receive outputs are made aware of the limitations of the data and analytics, and reminded to consider them only as an element of the wider intelligence picture.

6. Retain human oversight

This principle requires agencies to ensure that analytical processes are only a tool to inform human decision-making and do not entirely replace human oversight.

This principle requires border agencies to ensure that significant border enforcement decisions based on data analytics involve human judgement and evaluation. This ensures that, as noted above, agencies can continually assess whether the data and the outputs remain fit for purpose, can take into account the inherent limitations of the models or outputs, and can look for and identify errors or biases in the data. This also ensures that agencies can be properly accountable for their enforcement decisions, rather than hiding behind automation.

For the most part, border agencies do not automate the operational decisions and enforcement actions generally informed by JBA models or outputs. In fact, automated decision-making is specifically controlled by both the C&E Act and Biosecurity Act. This means that human oversight is generally present. However, border agencies should take care to ensure that that this remains the case.

7. Summary of recommendations and action plan

This section summarises the recommendations made above, and assigns actions to mitigate the risks identified.

Ref	This recommendation	Addresses these principles/risks	Requires these actions	By these people
Rec-001	Develop a Service Level Agreement between JBA and each border agency that clarifies roles and responsibilities and captures the parties' agreement to these.	Governance and accountability	Develop SLA Test with border agencies	JBA Border agencies
Rec-002	Develop a collaborative PIA process that ensures JBA and the border agency properly assess privacy risk and clear lines of accountability are maintained.	Governance and accountability, IPP 1, IPP 2, IPP 4, IPP 10.	Develop PIA process Develop PIA template Develop SharePoint site to manage process See Model Process at Appendix 1	JBA
Rec-003	Allow for the suspension of a PIA for analytics requests that have clear operational urgency, subject to senior authorisation from the requesting border agency.	Governance and accountability	Incorporate into process Incorporate into JBA SOPs Establish risk appetite with border agencies	JBA
Rec-004	Ensure that JBA Standard Operating Procedures (SOPs) reflect and maintain JBA's role and responsibilities, including limitations on data use and obligations to assist border agencies with the assessment of privacy and ethical risk.	All principles	Review and amend SOPs	JBA
Rec-005	Ensure that the single agency PIA process requires JBA and the border agency to limit new personal information collected to that which is necessary for the activity.	IPP 1, AP 2, AP 3	Include in PIA process Include in PIA template	JBA
Rec-006	Ensure that new information created as a result of an analytics activity is necessary for the purposes of the activity. If it is not, delete it or remove it from the analytics dataset.	IPP 1, AP 2, AP 3	Incorporate into JBA SOPs	JBA
Rec-007	Ensure JBA continuously reassesses and refines the personal information used for an analytics activity, to support data minimisation.	IPP 1, AP 2, AP 3	Incorporate into JBA SOPs	JBA

Ref	This recommendation	Addresses these principles/risks	Requires these actions	By these people
Rec-008	Ensure that the single agency PIA process prompts border agencies to ensure that they have a lawful basis to collect new personal information from a source other than the individual concerned.	IPP 2, AP 3	Include in PIA process Include in PIA template	JBA
Rec-009	Border agencies should review their public privacy notices to ensure that they are generally open about the use of personal information for data analytics and profiling.	IPP 3, AP 3, AP 4	Review border agency privacy notices and amend to address use of JBA	Border agencies
Rec-010	Ensure that the single agency PIA process requires JBA and the border agency to ensure new personal information is collected in compliance with principle 4.	IPP 4, AP 3	Include in PIA process Include in PIA template	JBA
Rec-011	Consider whether border agencies can use their legislative powers to expressly authorise JBA staff employed by other border agencies to access their systems and data.	Governance and accountability, IPP 5, AP 3	Discuss option with border agencies Address in SLA Incorporate into JBA SOPs	JBA Border agencies
Rec-012	Set appropriate limits on JBA staff access to border agency systems, to mitigate the risk of misuse of personal information.	Governance and accountability, IPP 5, IPP 11, AP 3	Incorporate into JBA SOPs Develop security training Establish audit controls	JBA
Rec-013	Ensure that appropriate policies, processes and controls are in place to meet general organisational and technical security requirements.	IPP 5, IPP 11, AP 3	Incorporate into JBA SOPs Develop security training Review JBA contracts Establish audit controls	JBA
Rec-014	Develop and maintain training for all JBA staff that addresses general security requirements and enables staff to recognise and manage a privacy breach in accordance with Rec-016.	IPP 5, IPP 11, AP 3	Develop security training	JBA
Rec-015	Ensure Service Level Agreement provides assurance that JBA will notify an affected border agency of any privacy breach that might impact that border agency's personal information.	Governance and accountability, IPP 5, AP 3	Address in SLA	JBA
Rec-016	Develop a JBA process to manage the identification, management and notification of a privacy breach within a border agency system.	IPP 5, AP 3	Incorporate into JBA SOPs Develop security training	JBA
Rec-017	Ensure that the use of third party cloud providers for the purposes of an analytics activity complies with border agency procurement policies and procedures, is risk-assessed and has been approved by the relevant border agency.	Governance and accountability, IPP 5, IPP 11, AP 3	Incorporate into JBA SOPs Review border agency procurement policies	JBA

Ref	This recommendation	Addresses these principles/risks	Requires these actions	By these people
Rec-018	Border agencies should review and amend their subject access request processes to take into account any personal information created by JBA analytics activities.	IPP 6, AP 3, AP 4	Review border agency process and amend to address use of JBA	Border agencies
Rec-019	Ensure subject access requests are referred to the relevant border agency and JBA is able to assist border agencies to collate personal information and respond to such requests.	IPP 6, AP 3, AP 4	Incorporate into JBA SOPs Develop privacy training	JBA
Rec-020	Border agencies should review and amend their correction request processes to manage and respond to requests to correct any personal information created by JBA analytics activities.	IPP 7, AP 3	Review border agency process and amend to address use of JBA	Border agencies
Rec-021	Assist border agencies to respond to correction requests, including correcting or updating disputed information and affected outputs.	IPP 7, AP 3	Incorporate into JBA SOPs Develop privacy training	JBA
Rec-022	Ensure personal information gathered and used for an analytics activity is up-to-date and regularly refreshed for the duration of the activity.	IPP 8, IPP 9, AP 2, AP 3	Incorporate into JBA SOPs Investigate automation of refresh	JBA
Rec-023	Apply robust identity resolution processes to ensure individuals are accurately matched with events, entities or other adverse information.	IPP 8, AP 2, AP 3	Incorporate into JBA SOPs	JBA
Rec-024	Ensure datasets identified for use in an analytics activity are assessed for unwanted biases.	IPP 8, AP 2, AP 3	Incorporate into JBA SOPs	JBA
Rec-025	Ensure that personal information is retained within border agency analytics environments in compliance with the border agency's data retention rules, and any statutory retention limitations.	IPP 9	Incorporate into JBA SOPs Review border agency retention rules Investigate automation options	JBA
Rec-026	Ensure that the single agency PIA process prompts border agencies to ensure that they have a lawful basis to use personal information for the purposes of generating identifiable intelligence outputs.	IPP 10, AP 3	Include in PIA process Include in PIA template	JBA
Rec-027	Ensure de-identified outputs are meaningfully anonymised, and protected against the risk of re-identification.	IPP 5, IPP 11, AP 3	Incorporate into JBA SOPs Develop de-identification training	JBA
Rec-028	Ensure sensitive outputs are released with appropriate handling caveats or rules.	IPP 5, IPP 11, AP 3, AP 5	Incorporate into JBA SOPs Develop standard wording	JBA
Rec-029	Assist border agencies to respond to Privacy Act complaints about the use of personal information for analytics activities.	All principles	Incorporate into JBA SOPs Develop privacy training	JBA

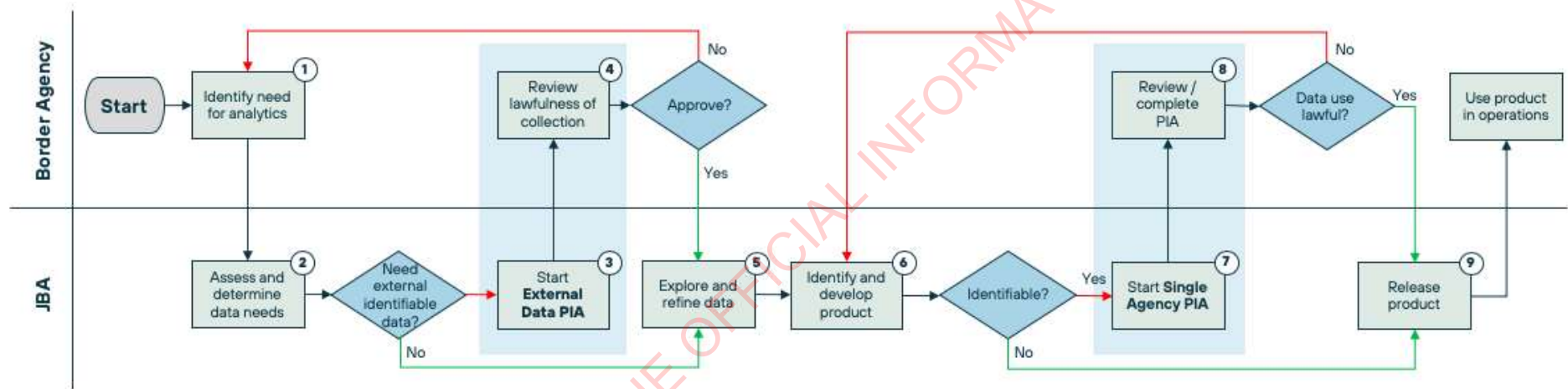
Ref	This recommendation	Addresses these principles/risks	Requires these actions	By these people
Rec-030	Consider developing a public webpage that provides a general overview of JBA, analytics activities, and the privacy and security safeguards in place.	AP 4	Develop JBA webpage	JBA
Rec-031	Consider publishing a summary of this PIA to build public trust and social licence in border agency use of JBA.	AP 4	Develop PIA summary	JBA
Rec-032	Border agencies should be open about their use of JBA analytics services.	IPP 3, AP 4	Investigate options for publication of analytics summaries (such as annual reports)	Border agencies
Rec-033	Provide border agencies with an explanation of the algorithms used to generate identifiable intelligence products and assist them to understand specific methods and processes used for an activity.	IPP 7, IPP 8, AP 3, AP 4, AP 5	Incorporate into JBA SOPs Develop standard wording	JBA
Rec-034	Ensure border agency units that receive outputs are made aware of the limitations of the data and analytics, and reminded to consider them only as an element of the wider intelligence picture.	IPP 8, AP 5, AP 6	Incorporate into JBA SOPs Develop standard wording	JBA

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1992

8. Appendix 1: Suggested single agency PIA process

This process is for any analytics activity that relates to a single border agency, and does not require the sharing of personal information between border agencies, including data enrichment, analytics models, forecasts and identifiable intelligence products. It assumes that the activity supports the border agency's lawful purposes. Activities intended to support other/new purposes would require an initial privacy risk assessment.

Process outline



1. Analytics activities should be initiated by the border agency that identifies the need for it. The border agency must make the policy decision to use JBA for purposes that align with its legislative mandate and lawful purposes. JBA might assist a border agency to identify potential activities, but the policy decision and request must come from the border agency that is responsible for the data.
- 2 & 3. JBA, as the subject matter expert in data analytics, will then work with the border agency involved to develop the analytics mandate and scope and determine the data needs for the activity. JBA might identify that it needs information from external data sources for the activity. It should be noted that if an external / third party data set has already been collected by the border agency in accordance with a lawful power (e.g. call record data that has been lawfully obtained from a telecommunications provider under a statutory power) then this is not considered to be an “external data source” as it has already been lawfully collected by the border agency and this information will be assessed at the DATA OUT stage. If this information is not

identifiable (such as WaterCare data) then no further assessment is required. If this information is identifiable (such as Police domestic drug seizures), then an External Data PIA will need to be completed.

4. This is an EXTERNAL DATA assessment. This assessment will require the border agency to establish that the external dataset is necessary (IPP 1), and a reasonable belief that an exception applies to permit the collection of the information from an external source (IPP 2). Step 4 is unlikely to be required often.
5. JBA will then access the datasets it identifies, within the relevant border agency's own systems, and will explore the datasets to determine what fields are required and begin analysing the data. This process may require the addition of new datasets or the deletion of datasets or data fields that are determined not to be relevant (in accordance with accepted data minimisation principles). To ensure the accuracy of the information used, relevant datasets would be refreshed on a regular basis during the analytics process.
- 6 & 7. JBA will then start to identify and develop products (outputs) as a result of the analytics activity. Where these outputs are not identifiable – which will be the case in respect of data enrichment, analytics models and forecasts, no privacy risk assessment is required, and JBA may develop the outputs and release them to the business. However, where the outputs will identify individuals, JBA must develop a single agency PIA which outlines the outputs and seeks approval from the border agency (see step 8 below).
8. This is the DATA USE assessment. Because the border agency is asking JBA to use its own data, no consideration around disclosure is required (note, JBA is acting on the border agency's behalf). This assessment will require the border agency to establish that it has a lawful basis to use its data for an identifiable output. This will require a consideration of the purposes for which the data was collected, and whether or not the output is permitted by either the agency's own legislation or IPP 10. It will also require an assessment of fairness and proportionality.
9. It will be up to the border agency to determine how the output will be operationalised, which must be done in accordance with the requirements of the border agency's own legislation and/or Privacy Act.

Single agency PIA questions

JBA to complete:

1. What were the initial goals for this analytics activity?
2. What personal information has this analytics activity used?
3. What is the identifiable output that has been identified, and what personal information will it contain?
4. What business unit/s will receive/use the identifiable output?
5. What security classification will the outputs require?

6. What steps have been taken to ensure the information is accurate and up-to-date before it was used to create identifiable outputs?

Border agency to complete:

7. Is there a lawful basis to use the information in this way? *(Please explain your answer)*

- a. Not sure, we need more information *[creates workflow for JBA to add detail]*
- b. No, we cannot identify a lawful basis *[creates workflow for JBA to reconsider output]*
- c. Yes, this output directly supports our functions under our enabling legislation
- d. Yes, this output is directly related to the purposes for which we collected the information (principle 10(1)(e))
- e. Yes, this output is necessary to avoid prejudice to the maintenance of the law (principle 10(1)(c)(i))
- f. Yes, this output is necessary to prevent or lessen a serious threat to life, health or public safety (principle 10(1)(d))

8. Are there any statutory restrictions on the use of all or some of the information that may impact on the lawfulness of the output?

- a. Yes *(please explain)*
- b. No

9. Have reasonable steps been taken to ensure that the information is accurate and up-to-date (particularly where the analytics activity has created new information)?

- a. Not sure, we need more information *[creates workflow for JBA to add detail]*
- b. No, we think the information needs to be reviewed and updated before the outputs are developed *[creates workflow for JBA to update the information]*
- c. Yes

10. Do the business units receiving the outputs have the necessary security clearance?

- a. Yes
- b. No *[creates workflow for business unit to organise necessary clearance]*

11. Do the business units receiving the outputs have processes in place to ensure that they are validated before being relied upon to take adverse actions against individuals?

- a. Yes *(please explain)*
- b. No *[creates workflow for business unit to organise necessary process]*

12. Do the business units receiving the outputs have processes in place to ensure that an individual can challenge an adverse action taken against them as a result of the outputs?
- a. Yes *(please explain)*
 - b. No *[creates workflow for business unit to organise necessary process]*
13. Could the outputs be considered unlawfully discriminatory?
- a. Not sure, we need more information *[creates workflow for JBA to add detail]*
 - b. Yes *[creates workflow for JBA to reconsider output]*
 - c. No

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982