Feedback from Consultation on Ministerial Policy Statements: Publicly available information

Paragraph/ Section	Agency	Feedback	DPMC Response
General	Police	Reference to the use of 'leaked' information available to the public should be referenced in this MPS (even if out of scope or in another document). Consider a Principle of not granting less 'access' to government agencies working in National Security than is afforded to the standard capability of a reasonably savvy internet user?	This was removed from 'authorisation procedures' of current MPS as many sources of very widely publicly available information was once leaked or gained from information that was hacked or obtained unlawfully. The agencies have said they will include this in their internal guidance on issues that might cause an issue to be raised to the legal team.
General	IGIS	*Section 19 ISA* introduces a 'firm limit' on the agencies taking any action against a person merely because they are engaged in expressive conduct. In our view the phrase 'does not in itself justify' in s19 only allows the agencies to collect against a person or class or persons where there is something about them and/or their expression, besides its mere occurrence, that creates a cogent 'intelligence and security' reason to take action. We suggest the PAI MPS include more guidance on what is sufficient. This could be by further example – eg public expression of extreme or radical views is not sufficient justification in itself for collection, but such expression in a forum verifiably frequented by groups or individuals advocating violence might be.	Have included an example under the section 19 heading.
General	GCPO	In the new Privacy Act 2020 the Privacy Commissioner may take account of cultural perspectives on privacy with regards to any statutory function or duty, and in exercising any statutory power. It is reasonable to expect that the subjects of	Noted – we have passed this on to the GCSB and NZSIS, and they may choose to get in touch with the Ministry of Ethnic Communities to discuss different cultural

Paragraph/ Section	Agency	Feedback	DPMC Response
		information being collected may have a different cultural perspective on privacy, such as concepts of collective identity and attributes, that may differ to the OECD-centric view of the Privacy Act 2020. We believe that the soon-to-be-formed Ministry for Ethnic Communities may have the ability to provide valuable input for the NZ intelligence community with regards to personal information data collection.	perspectives on privacy to inform their operational practice.
Para 6	OPC	This has been generalised from the 2017 version (the original version includes specific examples such as an open social media group or a public Tweet). The revised version states more generally that people would not have a reasonable expectation of privacy in information they share in a manner that makes it accessible to the public. However, this doesn't reflect that publicly available information is not confined to information that people share about themselves online. Information can be made public by other actors without the knowledge or consent of the individual (including by data breaches or criminal acts or by individuals posting information about other people on public social media sites including defamatory information and misinformation). The MPS should not be read as implying that there is no expectation of privacy in publicly available information, and the revised statement in para 6 should include balance given the range of situations in which information is made public. For example – "caution as to the provenance and source of the information is required when collecting information from publicly available websites and social media as there may be a persisting expectation of privacy in certain circumstances, for example where information is made publicly available without	Have added 'would not necessarily have'. Although here we are talking about information that people have made public themselves. Have added examples to be clear what we are talking about here.

Paragraph/ Section	Agency	Feedback	DPMC Response
		an individual's knowledge or consent, or where the data has been de-identified to protect the privacy of individuals."	
Para 7	Police	Amending paragraph 7 relating to online communities. Although some communities require 'approval' to join, these groups still run completely anonymously meaning privacy is inherent. I'm not sure these should sit outside the MPS, and the extent to which there exists a reasonable expectation of privacy.	Noted. The intent of specifying this is to note that this MPS would not apply to this information as it doesn't meet the definition of what we consider 'public'. However, this information can still be accessed by the agencies, but this MPS would not apply (covered in Humint MPS).
Para 10	OPC	Please retain the note from the 2017 version that special precautions may need to be taken to protect sensitive information once collected. As well as IPP 8, this section should include the principle of data minimisation and the obligation to limit the collection of personal data to that which is necessary for lawful intelligence purposes (IPP 1). We also recommend that the MPS reflect that publicly available information should generally be current information and that aged information requires a particular reason or purpose for collection, rather than a general purpose. This is to reduce the risk that information is out of date and not fit for purpose. This section should highlight the need for Privacy Impact Assessments in relevant circumstances. Where the intelligence agencies are using automated means to collect publicly available personal information (e.g. via website scraping or algorithms), a Privacy Impact Assessment should be carried out	IPP 1 is included in para 10. Level of detail re PIAs is more appropriate to be included in the internal policy on bulk data use (which is now set out in the MPS).

Paragraph/ Section	Agency	Feedback	DPMC Response
		before adoption of this automation and regularly reviewed to ensure respect for privacy. Where the collection of publicly available information contributes to privacy impacts such as profiling and surveillance or for use in privacy intrusive technologies such as facial recognition, this should also be subject to a Privacy Impact Assessment. The re-identification of individuals from de-identified public data or statistics should be subject to a Privacy Impact Assessment and privacy mitigations to ensure that the extent of re-identification is limited by strict necessity and proportionality, given the privacy interests involved, particularly if data is manipulated to override privacy protections applied to anonymise individuals.	
Para 10 Para 17	GCPO	Can note and link this as section 28 of the Privacy Act 2020 (optional inclusion).	
Para 12 – on	GCPO	Should the sections be ordered in order of the information privacy principles?	Noted. The sections are ordered consistently across MPSs so wouldn't want to reorder by IPPs.
Para 14	OPC	Para 14 has been added to the principle of 'Necessity'. It notes that the agencies may need to collect more than the target data to disguise the target. That is matter of operational necessity, rather than the principle of Necessity i.e. that the information being collected is necessary for a lawful purpose. It is also in tension with the principle of proportionality. We recommend para 14 is removed from the MPS and dealt with as a matter of operational procedure. As	The MPSs have the dual purpose of increasing transparency in the agencies activities. This para is intended to signal that this is something the agencies do.

Paragraph/ Section	Agency	Feedback	DPMC Response
		your message notes, the MPS is not intended to include operational guidance	
Para 17	OPC	Para 17 – principle of 'Proportionality' – this no longer refers to the specific exceptions in IPPs 10 and 11 for the disclosure of publicly available information (i.e. that it must not be unfair or unreasonable) and only refers to the intelligence agency exceptions. We recommend that the specific exceptions should be retained alongside the intelligence agency exceptions. This MPS deals with publicly available information. The IPP exception has been designed for the disclosure of publicly available information and should be used, with resort to the intelligence agency exception as necessary. As we noted in our 2017 comments, unfairness and unreasonableness as relevant considerations in the specific exceptions to IPPs 10 and 11 are relevant to the overall proportionality assessment.	The 'where it would be unfair or unreasonable to do so' text was removed from the current MPS, because it did not reflect that these requirements only apply to certain subparts of 10 and 11. It could be interpreted as additional threshold tests that need to be formally documented whenever collection occurs.
Para 18	OPC	Para 18 – Least intrusive means – we recommend deleting the words in brackets. The collection of publicly available information can be intrusive (e.g. through scraping and extraction of personal data from publicly available databases and websites using automated tools), and is not apparent to the individuals concerned where collected covertly. Personal information may be publicly available through data leaks or dumps or as the result of privacy breaches, and the collection of that information would be intrusive. Least intrusive means should also link to the sensitive category individuals. For example the collection of publicly available information about children and young people will raise particular considerations, as their sensitive personal	Noted. The fact that the information is publicly available is one of the least intrusive in the range of info collection methods that the agencies use is undeniable. Sensitive category individuals have specific internal policy. This point can be captured within that.

Paragraph/ Section	Agency	Feedback	DPMC Response
		information may be publicly available and not subject to privacy protections due to the lack of maturity or capacity.	
Para 20	Police	Amend paragraph 20 relating to protests. The way this reads implies there is no ability to collect PAI on a protest for the purposes of assessing security concerns. The current wording limits collection to a known security concern.	Noted
Para 26	IGIS	At 26, second bullet, the draft MPS requires consideration of the impact of obtaining, collecting and using publicly available information on certain rights affirmed under the NZBORA. This section omits reference to s14 NZBORA, the right to freedom of expression. We suggest s14 is referenced.	OK – added
Para 26	IGIS	The rights listed are important and we take no issue with them being listed. Under s17(a) ISA, however, the agencies must act in accordance with all human rights obligations recognised by New Zealand law. We suggest the MPS recognise this and note that the listed BORA rights are likely to be particularly relevant. The draft MPS does not refer to the right to be free from unreasonable search and seizure (s21 NZBORA). In this context, this right is most likely to be triggered where the agencies engaged in a search. When collecting publicly available information, the agencies will not always engage in a search for NZBORA purposed. Despite this, we think this is a possibility and the MPS should include guidance as there is a risk a search could be unreasonable.	In revising the MPSs we have included this information in the cover sheet, to make it very clear that the MPS apply only to lawful activity. We are not convinced of the value of the MPSs generally stating that the agencies need to follow the law – repeating the Act.
Respect for Privacy section	IGIS	We suggest this section incorporate some high-level discussion about the relationship between a person's reasonable expectation of privacy and s21 NZBORA. We also suggest s21 NZBORA is recognised a para 26 along with other NZBORA rights.	OK – text added

Paragraph/ Section	Agency	Feedback	DPMC Response
Para 26	Police	In developing policies and procedures relating to obtaining, collecting and using publicly available *personal* information, - insert the word personal here.	No change as information may not be specific to one person.
Para 27	GCPO	We are happy to be noted as a source of advice. Example that could be added is "expert advice may include the GCPO function located with the Dept of Internal Affairs.	Noted – can be incorporated in the agencies internal policies
General	Police	Should the MPS include a consideration of the possible future use of any material collected? Sometimes collected items from open sources have made their way to Police and can prompt action. As an organisation with a public safety function, any received information that indicates a concern creates response demand. s6(c) Should the MPS contemplate disengagement from publicly available sources when they are no longer a priority? (as part of *Respect for Privacy* – consider not just up front collection but the length of collection)	These issues are better set out in internal policies.

Paragraph/ Section	Agency	Feedback	DPMC Response
		• s6(c) [redacted]	
Sensitive category individuals	IGIS	As drafted, the MPS would require authorisation when the agencies collect MPs speeches and media statements, tweets etc. This appears onerous. Of the groups listed, the ones we think should be the subject of a policy providing restrictions and protections are children, young people and those vulnerable by reasons of illness or incapacity.	Agree, although the internal policy could set out that MPs speeches etc are exempt and policy only applies to certain personal information.
General – bulk datasets	IGIS	We think the MPS should provide more guidance on bulk personal datasets, either by: • Specific guidance in the MPS • Requiring the agencies to implement policy to address the handling of this type of information	Our preference is to include guidance in internal documents, as easier to change as context continues to develop. Also the guidance can then be produced at a higher level of classification as required. Have included a section in 'Matters to be reflected in internal policies and procedures'.