Privacy Commissioner
Te Mana Mātāpono Matatapu

Releasing personal information to Police and law enforcement agencies: guidance on health and safety and maintenance of the law exceptions

Updated April 2024

PURPOSE OF THIS GUIDE

This guidance deals with situations where **you have been asked** by Police or a law enforcement agency to release personal information.

Law enforcement agencies are public sector agencies that carry out law enforcement functions such as investigating and prosecuting criminal and regulatory offences.[1]

Government agencies, including Police and other law enforcement agencies, regularly request the release of personal information from private sector companies and public sector agencies. That information will often be sought as part of an investigation.

The Privacy Act places limits on the release of personal information. Principle 11 requires agencies holding personal information not to disclose it other than for the purpose for which it was obtained. However, an agency *may* release personal information on request if:

1. One of the exceptions in Principle 11 applies.
2. Another piece of legislation allows disclosure of the personal information to the law enforcement agency.

Personal information may also be obtained by **mandatory demands**, such as search warrants, production orders or the use of other specific statutory powers.

This guidance discusses the questions that often arise about when information *may* be released to Police and law enforcement agencies under the **health and safety** and **maintenance of the law** exceptions to principle 11.

[1] Law enforcement agencies include those that have a core law enforcement function e.g. NZ Police and the Serious Fraud Office, as well as agencies where law enforcement is part of their role e.g. MPI, MSD, ACC, IRD.

While this guidance refers to other Acts that enable or require personal information to be shared with law enforcement agencies, the references are not exhaustive. Agencies will need to consider the threshold for disclosure in the Act it is applying, as well as any other relevant considerations set out in any applicable legal, ethical, or professional standards.

Information sharing where there are concerns about the safety or wellbeing of children, and to prevent family violence, is an important example of where other legislative frameworks will be relevant. Read guidance about information sharing under the Oranga Tamariki Act 1989 and Family Violence Act 2018.[2]

Codes of practice

The Privacy Act 2020 gives the Privacy Commissioner the power to issue codes of practice that become part of the law. These codes modify the operation of information privacy principles, including principle 11, and set rules for specific industries, organisations, or types of personal information.[3]

Where an agency is covered by a code of practice, it must ensure that it complies with the requirements of the relevant rules. For example, where a health agency has been asked to disclose health information, rule 11 of the Health Information Privacy Code 2020 will apply and requires the health agency to consider whether it can obtain authorisation from the individual concerned before it can disclose under the "health and safety" or the "maintenance of law" exceptions (i.e it must have a reasonable belief that it is not desirable or practicable to obtain the individual's authorisation *and* that the exception applies).[4]

Telecommunications agencies must also be aware of and assess requests for telecommunications information under the provisions of the Telecommunications Information Privacy Code 2020, including the framework in Schedule 4 enabling the disclosure of emergency location information by network operators to emergency service providers when responding to an emergency.

Special rules also apply when a state of National Emergency has been declared.[5]

---

[2] https://www.privacy.org.nz/publications/guidance-resources/information-sharing-guidance-child-welfare-family-violence/

[3] Codes of practice are available on our website at: https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/

[4] Health Information Privacy Code 2020, rule 11(2).

[5] Civil Defence National Emergencies (Information Sharing) Code 2020.

VOLUNTARY REQUESTS AND MANDATORY DEMANDS

A **voluntary request** is a recognised way for law enforcement agencies to obtain information urgently (where there is a serious threat to health or safety), or where an investigation would otherwise be prejudiced (maintenance of the law).

Other Acts besides the Privacy Act enable voluntary and discretionary disclosures to law enforcement agencies. Where an agency is disclosing information under another Act, the relevant threshold for disclosure is set out in that Act rather than privacy principle 11.[6]

Personal information may also be obtained by **mandatory demands**, such as search warrants, production orders or the use of other specific statutory powers.

Law enforcement agencies rely on co-operation from other agencies assessing and responding to voluntary requests and releasing personal information where an important public interest would otherwise be harmed.

On the other hand, agencies holding personal information, such as corporate service providers, need to be mindful of their duties and responsibilities to their customers to keep personal information confidential. Responding to a law enforcement request is therefore a balance between responsible assistance to law enforcement and custodianship of the personal information.

The privacy principles provide a guide for striking the right balance of when and what personal information should be released on a voluntary basis.

Proactive disclosures

There will be occasions where an agency proactively discloses personal information to a law enforcement agency, in the absence of a request.

This may be to report a matter such as suspected fraud or wrongdoing, that affects the agency concerned or affects others.

While this guidance specifically addresses disclosures *in response to law enforcement requests*, proactive disclosures also need to meet the statutory disclosure requirements under the Privacy Act, or the other relevant Act.

[6] See for example section 22C of the Health Act 1956 (enabling the disclosure of health information to certain agencies for certain purposes); section 20 of the Family Violence Act 2018 (enabling sharing of personal information between family violence agencies for certain purposes); and section 15 of the Oranga Tamariki Act 1989 (enabling the reporting of concerns about a child's wellbeing).

GUIDANCE

The first question to consider is whether you have been *requested* to provide information, or whether you are *required* to provide it.

Where personal information is *required under compulsory legal authority*

Where you are required to provide information under a search warrant or production order[7] or by the operation of a specific statutory power,[8] you must comply with the demand for the information specified, subject to any right you may have to claim privilege in respect of the information.[9]

What kind of personal information could be privileged?

There are different types of privilege that protect certain kinds of information, depending on the importance of the public interest at stake.

The main categories of privilege are:

(a) legal privilege (with a number of different types);[10]
(b) privilege for communications with ministers of religion;[11]
(c) privilege in criminal proceedings for communications between patients and medical practitioners or clinical psychologists (where the consultation relates to drug dependency or a condition or behaviour that amounts to criminal conduct);[12]
(d) the confidentiality of journalists' sources.[13]

If the law enforcement agency reasonably believes that the information being requested is privileged, then it should provide an opportunity for a claim of privilege to be made so that the information can be protected.

Scope of the demand is critical to how the Privacy Act applies

While the Privacy Act does not provide the legal basis for the release of information covered by a statutory power or demand, principle 11 of the Privacy Act will apply to the release of

---

[7] For example, under the Search and Surveillance Act 2012, the Intelligence and Security Act 2017, or other statute containing search powers.
[8] For example: Tax Administration Act 1994, s 17 (information to be furnished on request of Commissioner); Social Security Act 2018, sch 6 (power to obtain information for certain purposes); Intelligence and Security Act 2017, s 150 (business records direction).
[9] Section 24(1) of the Privacy Act means that another statute that requires the release of personal information will override privacy principle 11.
[10] Evidence Act 2006, sections 54-56. See also section 57 in relation to confidential settlement negotiations and mediations. Search and Surveillance Act 2012, s 136.
[11] Evidence Act 2006, sections 54-56. See also section 57 in relation to confidential settlement negotiations and mediations. Search and Surveillance Act 2012, s 136.
[12] Evidence Act 2006, sections 54-56. See also section 57 in relation to confidential settlement negotiations and mediations. Search and Surveillance Act 2012, s 136.
[13] Evidence Act 2006, sections 54-56. See also section 57 in relation to confidential settlement negotiations and mediations. Search and Surveillance Act 2012, s 136.

any personal information *outside the scope of the statutory demand* (i.e. if you provide more personal information than is lawfully demanded).

If you think an order or warrant is overly broad, you should clarify its intended scope with the requesting agency and seek legal advice, if necessary, about your obligations to comply with the order or warrant and grounds for challenging its scope.

Where personal information has been *requested*

Privacy Act

The Privacy Act applies when an agency is asked to release personal information on a voluntary basis. Even when that request is made by a law enforcement agency, you are under no compulsion to comply with it.

Although you are not legally required to release the information, you will not breach the Privacy Act if you are satisfied that a principle 11 exception applies in the circumstances, and you can justify the disclosure on the relevant ground.

Voluntary requests for information are a routine feature of criminal investigations. These requests form an important preliminary step in investigations and are voluntary in the sense that they require the cooperation of the disclosing agency (as opposed to compulsion of the information under a search warrant or production order). Often, a law enforcement agency will make a request citing the Privacy Act, and a specific principle 11 exception.

As the disclosing agency, you will have to justify the disclosure if a complaint is made under the Privacy Act. The responsibility under principle 11 for ensuring there are adequate grounds to release the information rests with you, as the disclosing agency.[14] If you haven't been given sufficient information by the requester to enable you to make that assessment, you should ask for it.

Before you can decide whether to release the information, you have an obligation to assess whether there are grounds to release it. You must not fulfil a request without first assessing if you can justify the disclosure under principle 11.

Reasons for declining a request

If you are not satisfied that the grounds for release are met, you will **not** have a legal basis under the Privacy Act to release the information and you should decline the request. You may consider that the request is too broad in the circumstances and asks for too much information about too many people. You must only provide the information you are satisfied is necessary to meet the request.

You can also decline the request for other reasons. For example, you may have assured your customers that their information will be kept confidential, or you may be subject to other legal, ethical, or professional standards that require you to maintain confidentiality.[15]

[14] The requesting agency has separate obligations in relation to the manner of collection under principles 1, 2, 3 and 4.

[15] For example, the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008.

The importance of documentation and keeping good records

It is important to keep good records. The request, your decision whether or not to disclose the requested information to law enforcement, and the reasons for that decision, should be well documented. If you are disclosing information in reliance on an exception, your documentation should make it clear which exception you are relying on, what you have considered, your reasons for disclosing, and what you have disclosed.

Recording reasons at the time helps to support good decision-making and promote accountability. It also helps you to explain and justify the decision if the individual raises concerns about the disclosure, or makes a complaint to our office.

Belief on reasonable grounds that an exception applies

Principle 11 of the Privacy Act says that where an agency holds personal information, the agency shall not disclose that information unless one of the exceptions applies.

To rely on an exception, you must believe on reasonable grounds that one of the exceptions applies at the time the information is released. You must actually believe that the relevant exception applies, and your belief must be reasonably held, i.e. there must be a reasonable basis for that belief.[16]

Your belief must be based on proper consideration of the relevant circumstances. An explanation constructed afterwards will not meet this test. You need to turn your mind to principle 11 and the relevant exception when deciding whether to release the information requested.[17]

Whether there is a reasonable basis will depend on what you know and what you have been told by the requester about why the information is required. For example, have you been made aware of the relevant circumstances that provide reasonable grounds for your belief that the exception applies?

A request from a law enforcement agency pointing to an exception in the Privacy Act may support your belief that the exception applies, but you will also need to check that the request provides you with a reasonable basis for that belief.

For example, the Human Rights Review Tribunal heard a case where an informant's identity was disclosed and that resulted in harassment of the informant. The Tribunal looked for evidence that the decision-makers had reasonable grounds to rely on principle 11(1)(a), (disclosure for a relevant purpose), and principle 11(1)(d), (the disclosure was authorised by the person concerned). However, no evidence was available to demonstrate reasonable grounds for the belief that principle 11 exceptions applied.[18]

---

[16] "Reasonable grounds" is a mixed subjective and objective test. See *Geary v Accident Compensation Corporation* [2013] NZHRRT 34 [201]-[203].

[17] *Tan v New Zealand Police* [2016] NZHRRT 32, [99], citing *Geary v Accident Compensation Corporation* [2013] NZHRRT 34, [201]-[203].

[18] *Deeming v Whangarei District Council* [2015] NZHRRT 55.

Which exception applies?

Principle 11 has different exceptions that can be used in a variety of circumstances where the voluntary release of personal information is requested.

For example, personal information can be released where disclosure of the information is one of the purposes in connection with which the information was originally obtained or is directly related to that purpose.[19]

This guidance focuses on when information can be released to law enforcement agencies to prevent or lessen a serious threat to health or safety (principle 11(1)(f)) or to avoid prejudice to the maintenance of the law (principle 11(1)(e)(i)).

PRINCIPLE 11(1)(f): PREVENT OR LESSEN A SERIOUS THREAT

Under the Privacy Act, you can disclose personal information to an appropriate agency if you believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to health or safety. This exception applies to any person, body, or agency, not just law enforcement agencies, and is often relevant to requests made by Police.

To rely on principle 11(1)(f), you need to:

- be satisfied that a serious threat exists, and
- believe on reasonable grounds that disclosure is necessary to prevent or lessen that serious threat.

You should only disclose information to the person, body, or agency that is able to do something to prevent or lessen the threat. This will not usually be an issue when the request is being made by Police.

Is there a serious threat, as defined in the Privacy Act?

A "serious threat" is a threat that an agency reasonably believes to be serious, having regard to the likelihood of the threat being realised, the severity of the consequences and the time at which the threat may be realised.[20]

For example, a modest risk that is about to happen might count as serious, as might a more severe risk that is some distance in the future.

A threat is serious based on an assessment of the specified factors. The Privacy Act sets out the three factors that need to be considered.[21]

1. The likelihood of the threat occurring – is there a good chance this thing will actually happen?
2. The severity of the consequences if the threat occurs – if it happens, how bad will it be?
3. The time at which the threat might occur – how soon could this happen?[22]

---

[19] Privacy Act 2020, s22, Principle 11(1)(a). Agencies can also disclose when the source of that information is a publicly available publication and it would not be unfair or unreasonable to disclose it (principle 11(1)(b)); or where the disclosure is authorised by the individual concerned (principle 11(1)(d)). There are also other grounds which relate to the sale of a business and anonymised and statistical information.

[20] See the definition of "serious threat" in section 7(1).

[21] See the definition of "serious threat" in section 7(1).

[22] This exception used to require a threat to be both serious and imminent. That was changed by the Privacy Act Amendment Act 2013 and the new definition of "serious threat" now treats imminence

Note that not all of these factors need to be present in order to reach the threshold of a serious threat. For example, if there is a real risk of harm to an individual (factors 1 and 2), but it is unclear when the risk may eventuate (factor 3), a high score on factors 1 and 2 will mean the threshold is met. In other words, a threat could be serious, despite not being imminent.

A serious threat assessment is context specific and should take account of all relevant circumstances, including those of the individual concerned. A serious threat can arise in one case based on the relevant risk factors for the individual concerned (and could be triggered by factor 2 alone) but may not meet the threshold in relation to a different individual.

For example, a threat of harm to a child will more readily meet the serious threat assessment due to the child's vulnerability and limited agency (i.e. an ability to act independently and make their own choices) compared to an adult of full capacity that may require additional factors to be present before the threshold is met.

Checklist – Principle 11(1)(f)

1. **Do I have a reasonable belief that there is a serious threat to public health or safety or to the life or health of an individual?**

   What are the relevant circumstances (including the circumstances of the individual concerned)? Do they establish that there is a risk of serious harm to an individual or to the public?

2. **Is the release necessary?**

   Is the information sought relevant or needed to address and lessen the serious threat? How will releasing the information assist to do this?

3. **Is the release to the appropriate agency?**

   Is the agency requesting the information in a position to use it to respond to and lessen the serious threat?

4. **Would there be harm if the information was not released?**

   What is the likely consequence if the information is not released? Would non-disclosure increase the serious threat or reduce the chances of responding to or lessening the serious threat?

---

as one factor that may contribute to a threat being assessed as serious, rather than as a factor independently controlling whether the exception applies.

Practical Example: Principle 11(1)(f)(ii)

Disclosure to the Police – no breach of principle 11

The Police are trying to locate a vulnerable person who has been reported missing by her family after failing to turn up to a planned family event. The person has not been seen or heard from in over 24 hours and has a history of mental health issues.

The missing person does not have her phone with her, so Police have been unable to obtain location data from her telecommunications provider. Police make a request to her bank for information on any transactions that have been made since the last confirmed sighting of the person, to assist them with their attempts to locate the individual.

The bank assesses whether it should release the information to the Police, relying on principle 11(1)(f)(ii) (serious threat to an individual). The bank asks itself the following questions:

Do I have a reasonable belief that there is a serious threat to an individual's health or safety? **The person has been missing for over 24 hours and she may be at risk of serious harm if she cannot be located.**

Is the release necessary? **The banking transactions could help the Police locate her and help prevent a serious threat to her wellbeing. There is evidence that the request is urgent as the sooner the person is located the more likely the risk of harm can be avoided. The request is limited in scope to bank records that may provide relevant information (i.e. where she has been since she was last seen),**

Is the release to the appropriate person/agency? **The Police are in a position to find the missing person and bring her home.**

Would there be harm if the information was not released? **There may be a delay in the Police finding out where the missing person is, which could have been serious, even fatal consequences for that person.**

Outcome**: Having satisfied itself that the disclosure is consistent with principle 11(1)(f)(ii), the bank decides to release the information requested to the Police.**

PRINCIPLE 11(1)(e)(i): AVOIDING PREJUDICE TO THE MAINTENANCE OF THE LAW

This exception allows you to release information if you believe on reasonable grounds that non-compliance is necessary:[23]

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences.

A public sector agency, as defined in the Privacy Act, includes the Police and other government departments.[24] The definition is limited to New Zealand agencies, and does not include overseas agencies.

What does the maintenance of the law exception encompass?

This exception lets you disclose personal information in circumstances where there would otherwise be prejudice to the maintenance of the law. It supports the maintenance of criminal and regulatory enforcement processes.

The maintenance of the law exception does not give Police or other law enforcement agencies the right to access any information they would like in order to maintain the law. Nor does it allow agencies to give general assistance with law enforcement investigations by providing relevant information on request. It only applies to situations where *not* providing specific information would prejudice or be detrimental to the maintenance of the law.

Voluntary request as a first step in an investigation

At an early stage of an investigation, a law enforcement agency may have insufficient information or grounds to apply for a compulsory order to compel the release of the relevant information. This can make it difficult, if not impossible, to progress any criminal investigation. In this context, a voluntary request can be a necessary prerequisite to obtaining compulsory orders. A request may be the only practical means of obtaining the information in order to effectively investigate (and avoid prejudice or harm to the maintenance of the law), particularly at the initial stages of an investigation.

Is the disclosure necessary to avoid prejudice to the maintenance of the law?

Whether a disclosure is *necessary* has been described in the case law as "being needed or required in the circumstances", or "required for a given situation". It is a relatively low test.[25]

It must be clear how the disclosure will avoid prejudice to the maintenance of the law.[26] You need to be satisfied that there is direct connection between the disclosure and prejudice to the maintenance of the law that would otherwise arise.

---

[23] Principle 11(1)(e) provides further grounds for disclosure where non-compliance is necessary:
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation).

[24] A "department" is defined as a government department named in Part 1 of Schedule 1 of the Ombudsman Act 1975.

[25] *Tan v New Zealand Police* [2016] NZHRRT 32, [78].

[26] See *K v Police Commissioner*, unreported, Complaints Review Authority / Decision No 33/99, 26 November 1999 (Case Notes 1994-2005).

For example, ask yourself what the effect would be if the information requested was not provided – would it prevent an investigation commencing or continuing? Are there circumstances that mean an investigation would be prejudiced without access to the information sought?

What information should the Police or other law enforcement agency provide?

The Police or law enforcement agency must provide enough information to enable you to form a view about whether there are reasonable grounds to believe disclosing the information is necessary to avoid prejudicing an investigation. How much information is required will depend on the circumstances.

The Police (or other requesting agency) must indicate the link between the offence being investigated and the relevance of the requested information. Without adequate detail from the requester, you cannot be satisfied that the principle 11(1)(e)(i) exception applies.

The Police or law enforcement agencies do not need to explain why they are seeking information through a voluntary request rather than by a search warrant or production order. However, they *do* need to provide enough information to support the information request and justify disclosure under the Privacy Act. This explanation should not prejudice the investigation or make an unwarranted disclosure of personal information.

A law enforcement agency may not be able to say much more than that a particular offence is being investigated, that the information request is relevant to that offence, and some indication of why it is relevant. Simply asserting that the information is needed for a police investigation is not enough. For example, the following request would **not** provide an adequate basis for disclosure.

> "To assist Police with an investigation we are currently undertaking, information is sought in relation to the following addresses/persons."

You may need to seek legal advice to respond to a request for personal information that is privileged or subject to an obligation of confidence. If the law enforcement agency reasonably believes that the information being requested is privileged, it should provide an opportunity for a claim of privilege to be made so that the information can be protected. [see page 4 above]. To protect the privilege or confidentiality of the information in the particular circumstances, you should inform the law enforcement agency concerned that you may need time to assess and respond to the request or demand.

When should the law enforcement agency use a statutory search power?

A law enforcement request for a name or verifying details does not generally need the full process of a search warrant or production order. Investigative law enforcement depends on asking agencies to disclose useful information to enable criminal offending to be investigated.

However, if you receive a request for assistance from a law enforcement agency, this does not mean you should disclose all you hold about the person concerned. You should make sure you are only disclosing the details that have been requested, and only the details that are necessary for the relevant stage of the investigation.

Once the law enforcement agency has an investigation underway, more detailed information about persons of interest to the investigation should generally be sought by a search warrant, production order or other statutory power that authorises a lawful demand for the information.

Where the information being sought by law enforcement is sensitive in nature or broad in scope, it will be more appropriate to use statutory powers or search powers to require the information be disclosed, rather than making a voluntary request for it. That is because a law enforcement request for broad or sensitive information could be a "search",[27] necessitating a formal demand or order to authorise it.

If in doubt, you can decline the request, or seek legal advice.

How sensitive is the personal information?

Care should be taken in relation to the disclosure of intimate or particularly sensitive information i.e. information that tends to reveal intimate details of an individual's lifestyle and personal choices, or part of their "biographical core" of personal information.[28]

The relative sensitivity of the information requested will be relevant to whether, objectively there are the necessary grounds to justify its release. Certain types or categories of sensitive information would usually be sought by a production order or search warrant. These might include, for example, health information, telecommunications data or customer transaction data held by banks.

Confidential or privileged information

If you have made someone a promise of confidentiality, or you are obliged by other legal, ethical or professional obligations to maintain confidentiality of their personal information, or you can claim privilege in respect of the information, you should seek legal advice before making any disclosure.

Practical Example: Maintenance of the law – principle 11(1)(e)(i)

> ***Case 1: Disclosure to the Police – no breach of principle 11***
>
> **The Police were investigating how contact by letter had been made with victims of criminal offending and asked a District Health Board[29] if a relative of the offender employed by the DHB had accessed the NHI database without authority (potentially an offence under the Crimes Act 1961).**
>
> **The Police did not have sufficient grounds to apply for a search warrant or production order and asked the DHB for voluntary co-operation. The Police request included a certain amount of detail so that the DHB could understand the purpose and importance of the request, mindful that without the information sought, the inquiry would be seriously compromised along with the ability to assess and mitigate potential risks to the victims.**
>
> **The DHB provided the information to the Police under principle 11(1)(e)(i) of the Privacy Act (maintenance of the law).**
>
> ***Tan v New Zealand Police [2016] NZHRRT 32.***

---

[27] A "search" may trigger legal protections for the information under the Search and Surveillance Act and the New Zealand Bill of Rights Act 1990, s 21 (the right to be free from unreasonable search and seizure).

[28] https://privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

[29] District Health Boards have been replaced by Te Whatu Ora (Health New Zealand).

Not limited to investigations

While this guidance has focused on requests made by law enforcement for investigatory purposes, the maintenance of law exception also encompasses disclosures necessary to prevent prejudice to the prevention of offences and other responsibilities that the agency may have to maintain the law.

In all cases, it must be clear how the disclosure will avoid prejudice to the maintenance of the law.[30] You need to be satisfied that there is direct connection between the disclosure and prejudice to the maintenance of the law that would otherwise arise.

Practical Example: Maintenance of the law – principle 11(1)(e)(i)

Case 2: Disclosure to the Police – no breach of principle 11

The Police contacted a university to obtain information about a student. They were attempting to serve him with a notice of intention to revoke his firearm's licence. The Police informed the university that they had serious concerns for his mental health and needed to know where he was.

The university disclosed the student's home address, but the Police could not find him there. Upon a further request by the Police, the university revealed when the student would be sitting his examinations. This enabled the Police to find him and serve him with the notice.

The Privacy Commissioner was satisfied that it was reasonable for the university to believe that it was necessary to give the Police the information in reliance on principle 11(1)(e)(i) of the Privacy Act.

There were growing concerns about the student and there was urgency in the Police's need to locate him.

Case note 97705 [2008] NZ Priv Cmr 3.

[30] See *K v Police Commissioner*, unreported, Complaints Review Authority / Decision No 33/99, 26 November 1999 (Case Notes 1994-2005).

OTHER RESOURCES

- Online FAQs – “Ask Us”: www.privacy.org.nz/Ask
- Case notes: https://privacy.org.nz/publications/case-notes-and-court-decisions/
- Enquiries line: 0800 803 909 (Monday to Friday, 10:00 am to 3:00 pm) or enquiries@privacy.org.nz
- Public statements: https://privacy.org.nz/blog/hager-and-westpac/ https://privacy.org.nz/publications/statements-media-releases/statement/
- Reports: https://www.privacy.org.nz/publications/commissioner-inquiries/transparency-reporting/
- Resources:
    - https://www.privacy.org.nz/publications/guidance-resources/information-sharing-guidance-child-welfare-family-violence/
    - https://www.privacy.org.nz/publications/guidance-resources/information-sharing-guidance-child-welfare-family-violence/escalation-ladder/
- Sensitive information guidance: https://privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

QUICK GUIDE

Responding to law enforcement requests for personal information – Applying principle 11(1)(f) ("serious threat") and principle 11(1)(e)(i) ("prejudice to maintenance of the law").

1. **Have you received a *demand* or a *request* for information?**

   Mandatory demands

   If you have received a valid and lawful demand for personal information under a specific statute, or under a search warrant or production order, you are legally required to comply and to produce the information sought, subject to any right you may have to claim privilege over the requested information.

   A mandatory demand may take a number of different forms. Sometimes it could be a request that you are required to comply with. If you are not sure if compliance is mandatory, ask the law enforcement agency for clarification or seek legal advice. For guidance and examples, refer to pages 3-4. For information that may be subject to privilege, refer to page 4.

   Voluntary requests

   Without a lawful demand from a law enforcement agency, your co-operation is **voluntary**. You can elect to decline the request, or you can check whether you can provide the information requested if there is a basis for doing so under the Privacy Act or another Act.

   If you have received a voluntary request to release personal information, the Privacy Act, or another Act applies – go to question 2. This could be either an oral request or a request in writing that is not a legal demand.

   If you are not sure about the basis on which the information is being sought, read the guidance on pages 5-6 and ask the law enforcement agency for clarification or seek legal advice.

   Remember, if you're being asked for information on a voluntary basis, it's your decision whether to provide it and how much information you provide. There are some questions to work through before you release the information to a law enforcement agency.

2. **Is it clear what personal information is being sought?**

   Yes → go to question 3

   No → ask the law enforcement agency for clarification

3. **Does the request for information explain why it is needed?**

   Yes → go to question 4

   No → ask the law enforcement agency why the information is needed

   If you are not sure, ask for clarification.

4. **Is the request for disclosure under the Privacy Act?**

   Yes → go to question 5

   No → go to question 9

   If you are not sure, ask the law enforcement agency for clarification about the basis on which the disclosure of personal information is requested or seek legal advice.

5. **Do you have reasonable grounds to believe that releasing the information is necessary to prevent or lessen a serious threat to public health or public safety or to the life or health of an individual (principle 11(1)(f))?**

   Yes → go to question 8

   No → go to question 6

   If you are not sure, read the guidance to see if you have the necessary grounds (refer to pages 7-9).

6. **Do you have reasonable grounds to believe that releasing the information is necessary to avoid prejudice to the maintenance of the law by a New Zealand public sector agency (principle 11(1)(e)(i))?**

   Yes → go to question 8

   No → go to question 7

   If you are not sure, read the guidance to see if you have the necessary grounds (refer to pages 10-13).

7. **Do you have grounds to believe that another principle 11 exception applies in the circumstances?**

   Yes → go to question 8

   No → decline the request, OR ask the law enforcement agency to narrow the scope of the request to the personal information that is necessary OR go to question 9.

8. **Does the exception to privacy principle 11 apply to the request in full or in part?**

   In full → go to question 10

   In part → consider asking the law enforcement agency to narrow the scope of the request OR go to question 9.

9. Does another Act enable the disclosure of personal information on request?

Yes → go to question 10

No → decline the request if there is no apparent lawful basis for the disclosure. If there is a partial basis for disclosure under the Privacy Act, go to question 10.

10. How sensitive is the personal information?

If the information requested is sensitive, confidential or privileged, you should take extra care when exercising your discretion to disclose personal information. You may want to ask for further clarification from the requester. It may be that because of the nature of the information requested, a legal demand should be used to obtain some or all of it.

For more on requests for privileged, sensitive, or confidential personal information, read the guidance on pages 4 and 12.

11. Have you recorded your decision and reasons?

Once you have made a decision, and informed the law enforcement agency, keep a record of your decision and the reasons for it. If you have decided to release the information, keep a record of what information was released and the basis for releasing it.