Sensitive personal information and the Privacy Act 2020

This note provides guidance on how the Privacy Act applies to sensitive personal information.

Personal information

The starting point is that the Privacy Act 2020 applies broadly to all "personal information". Personal information is any information that tells us something about a specific individual. It is not limited to "private" or "secret" or "sensitive" information.

Personal information is any piece of information that relates to a living, identifiable human being.[1] People's names, contact details, financial health, purchase records can all be personal information.

The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address or another identifier, or if their identity could be pieced together.

The question is whether there's a reasonable chance that someone could be identified from the information. Any information that you can look at and say "this is about X" may be considered personal information, if X is an identifiable person.

This term covers a wide range of information *"from the very sensitive to the seemingly banal".*[2] At one end of the spectrum, some personal information is particularly sensitive, while at the other end is routine information about an individual that is not very sensitive at all.

What is sensitive personal information?

Sensitive personal information is information about the individual that has some real significance to them, is revealing of them, or generally relates to matters that an individual might wish to keep private. This can be contrasted with routine or mundane information that is about a person but is either not particularly revealing or does not reveal information that is very intimate or "private".

Certain types of personal information can generally be regarded as sensitive if the inferences that can be drawn about the individual from that information are potentially sensitive. For example, information about a person's race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural or political beliefs can reveal details that are very

---

[1] There is no general protection for the privacy of the deceased under the Privacy Act, however the privacy of the deceased is recognised in certain contexts: Office of the Privacy Commissioner, "Does the Privacy Act apply to information about dead people?"; "Privacy beyond the grave" (24 July 2018).
[2] See *R v Alsford* [2017] NZSC 42, [30]].

personal and that could result in the individual being treated in a certain way if used or revealed in a particular context.[3]

Information about a person's activities or memberships can be sensitive if this reveals insights into an individual's personal opinions and personal choices from which inferences can be drawn. For example, a person's membership of an advocacy group, trade union or political party is generally sensitive personal information and should be treated with confidentiality.

The Privacy Act does not prescribe fixed categories of "sensitive" personal information. Rather, any personal information can be sensitive, even highly sensitive, depending on the particular context and surrounding circumstances, including cultural perspectives.

Certain types of personal information are inherently sensitive however, including health,[4] genetic,[5] biometric,[6] and financial information.

The personal information of children and young people is also sensitive, given their inherent vulnerability and more limited agency than adults.[7]

How does the Privacy Act apply to sensitive personal information?

The Privacy Commissioner has emphasised that agencies who handle sensitive data need to take extra care to ensure the information is handled properly.[8]

Agencies have a higher standard of care when they collect or hold sensitive information. While the Privacy Act doesn't specify special procedures for information that is sensitive, the obligations on agencies are stronger with respect to sensitive information and they will be held to a higher standard of accountability.

The privacy principles

The privacy principles create a higher standard of protection for sensitive personal information. As the privacy principles depend on the particular context, the more sensitive the personal

---

[3] Similarly, under European privacy law (the General Data Protection Regulation) special categories of personal data are recognised as sensitive:
- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

[4] Privacy Commissioner *Case Notes* 298757 [2019] NZPriv Cmr 9; 297084 [2019] NZPriv Cmr 11.

[5] Office of the Privacy Commissioner "Your DNA is only a click away: Home DNA tests and privacy", blog, 6 August 2019; Law Commission *The Use of DNA in Criminal Investigations | Te Whakamahi I te Ira Tangata i ngā Mātai Taihara* (NZLC R144, 2020).

[6] Office of the Privacy Commissioner: Biometrics and Privacy, position paper, 7 October 2021.

[7] See Privacy Act 2020, IPP 4(1)(b).

[8] Privacy Commissioner *Case Note* 270745 [2016] NZPriv Cmr 10.

information, the greater the obligation on the agency to ensure compliance. For example, several privacy principles require agencies to take steps that are reasonable "in the circumstances".

Sensitive personal information should not be collected unless it is necessary for an agency's lawful purpose (IPP 1). The collection of personal information from an individual will require the agency to take steps that are reasonable in light of the sensitivity of the information to ensure that the individual is aware of the collection of that information and the purpose for which it is being collected, as well as other relevant information under IPP 3.

In particular, the sensitivity of the information is relevant when considering whether the means used to collect personal information are fair and not unreasonably intrusive on the personal affairs of the individual (IPP 4). The sensitivity of personal information about children and young people is reflected in IPP 4 as a relevant consideration in assessing whether personal information is being collected by means that are fair and not unreasonable intrusive.

The sensitivity of the information is also relevant to what security safeguards are reasonable in the circumstances (IPP 5),[9] and whether steps to check accuracy of the information are reasonable (IPP 8).[10]

On review, the Privacy Commissioner and the Human Rights Review Tribunal expect agencies to meet a higher standard of transparency, security and protection when the personal information is sensitive.[11]

Exemptions

The Privacy Act provides additional flexibility through specified exemptions. However, in some cases these exemptions are not available where information is highly sensitive. For example, the personal and domestic affairs exemption (section 27) does not apply if the collection, use or disclosure of the personal information at issue would be highly offensive to a reasonable person.

For example, disclosing the mental health details or past sexual abuse history of another individual without a legal basis for the disclosure is unlikely to be justified under the Privacy Act, regardless of a personal relationship between the individuals or a personal reason for the disclosure. The disclosure of such sensitive personal information could meet the "highly offensive" threshold that disqualifies the disclosure from being exempt from scrutiny under the Privacy Act.

---

[9] See Privacy Commissioner *Case Note* 83994 [2008] NZPrivCmr 6.
[10] See *Taylor v Orcon* [2015] NZHRRT 15 [46]-[47].
[11] See further, interference with privacy and damages, discussed below.

Codes of Practice

For particular types of sensitive information, such as health information or credit information, Codes of Practice have been developed which place additional obligations on certain agencies who deal with particular kinds of information.

The Credit Information Privacy Code 2020 sets out special rules for the handling of credit information by credit reporters.

The handling of health information by health agencies is also subject to special rules in the Health Information Privacy Code 2020.

While all health information is sensitive, some categories of information are particularly so. For example, particularly sensitive information could include information relating to sexual life;[12] ethnicity; HIV status; diseases or conditions carrying social stigma; mental health history; life expectancy; or addiction.[13]

Oversight, compliance and enforcement

The broader Privacy Act framework takes account of the relative sensitivity of personal information. The following are some examples.

Notifiable privacy breaches

The sensitivity of the information is a factor to be taken into account in assessing whether a privacy breach is notifiable to the Privacy Commissioner and to affected individuals (section 113(b)).

Compliance notices

When considering whether to issue a compliance notice, the Privacy Commissioner must consider a number of factors including the seriousness of the breach (section 124(1)(b)), which will depend in part on the sensitivity of the relevant personal information.

Approved Information Sharing Agreements

Information sharing agreements under Part 9A of the Privacy Act must specify the safeguards that will apply to protect the privacy of individuals and ensure that any interference with their privacy is minimised (section 144(2)(d)). The more sensitive the information, the more robust

[12] For example, sexual orientation, sexual practice, fertility, past pregnancies, miscarriages or terminations, sterilisation, contraception, STDs, and sexual dysfunction.
[13] From the commentary to the Health Information Privacy Code 1994, rule 4; also reproduced in Paul Roth and Blair Stewart, Privacy Law and Practice (LexisNexis) HIC4.2, rule 4.

the safeguards will need to be to protect it under an information sharing arrangement and to minimise adverse effects on the privacy of individuals.

Te Ao Māori and cultural perspectives

Under the Privacy Act, the Commissioner must take account of cultural perspectives on privacy[14] including tikanga Māori.[15] The Commissioner's obligation will have an influence upon whether personal information is regarded as sensitive, depending on the particular circumstances and the cultural perspective of the individual. [16]

Sensitive personal information may be of particular importance for Māori. For example, biometric information is particularly sensitive information and some biometric information (such as the results of DNA analysis) is directly connected to whakapapa (genealogy) which links an individual to their ancestors and to whānau, hapū and iwi.[17]

Although the definition of personal information is broad, one of the current features of the Privacy Act that may be relevant from a te ao Māori perspective is that the Act only applies to personal information about deceased individuals in certain circumstances, such as under the Health Information Privacy Code.[18] From different cultural perspectives (particularly Māori) the Act's primary focus on the privacy interests of living people may affect the ability to protect the deceased's identity and personal information by living descendants.

As indicated in OPC's position paper on Biometrics and Privacy,[19] personal information raises distinct issues and concerns from Te Ao Māori perspectives, including the relationship between individual and collective privacy. These are both profound and practical issues that require agencies working alongside Māori to understand those perspectives and how, practically, the Privacy Act's framework can support the Crown's Tiriti obligations and tikanga Māori through appropriate treatment and protection of sensitive personal information.

Tikanga and te Tiriti o Waitangi will be relevant considerations to the handling of sensitive personal information under the information privacy principles.[20] State sector agencies will need to assess the sensitivity of personal information in terms of both obligations and rights under te Tiriti o Waitangi and with regard to tikanga Māori, and take appropriate steps, including through consultation, to ensure that the collection and handling of this personal

---

[14] Privacy Act, s 21(c).
[15] As the Law Commission notes tikanga provides a "koru…of ethics" and a shared basis for "doing things right doing things the right way, and doing things for the right reasons" Law Commission *The Use of DNA in Criminal Investigations | Te Whakamahi I te Ira Tangata I ngā Mātai Taihara* (NZLC R144, 2020) at 63.
[16] The Office of the Privacy Commissioner "Compliance and Regulatory Action Framework" (November 2020) sets out the guiding principles the OPC will follow in our approach to compliance and regulatory action. OPC's guiding principles includes kōtuitui which is expressed in the guidance as seeking opportunities to partner with Māori wherever possible and striving to interweave mātauranga Māori for positive intercultural outcomes.
[17] See, for example, the position taken by Te Mana Raraunga | Māori Data Sovereignty Network on NZ Police's use of facial recognition technology and Law Commission *The Use of DNA in Criminal Investigations | Te Whakamahi I te Ira Tangata I ngā Mātai Taihara* (NZLC R144, 2020) at 62-69.
[18] Office of the Privacy Commissioner, above n 1.
[19] Office of the Privacy Commissioner: "Biometrics and Privacy", position paper, 7 October 2021.
[20] See *Te Pou Matakana Limited v Attorney-General* [2021] NZHC 3319 (No.1); *Te Pou Matakana Limited v Attorney-General* [2021] NZHC 3319 (No. 2).

information is subject to relevant processes, protocols and safeguards, as for other types of sensitive personal information. Private sector agencies should also be mindful of tikanga Māori and the potential sensitivity of personal information in this context.

Interference with privacy and damages

The sensitivity of personal information is taken into account in the enforcement of the IPPs and providing redress to individuals. A breach of the IPPs involving sensitive personal information is more likely to negatively impact on the individual concerned and result in a finding of an "interference with privacy" (section 69).

Where damages are awarded by the Human Rights Review Tribunal, the more sensitive the personal information at issue, the greater the impact on the individual and the higher the damages award may be (section 103).

Is personal information sensitive? – taking a case by case approach

Deciding whether any particular personal information is sensitive requires a case by case approach. What is sensitive for one individual in one context may not be sensitive for another individual in a different context. For example, the contact details for one individual may be highly sensitive if they have a protection order in place due to family violence.

A privacy impact assessment can help an agency to identify the range of scenarios that result from the agency's handling of personal information that may have an effect on individuals and mean the information should be treated with particular care.

Reasonable expectation of privacy

A useful approach is to assess if the individual has a "reasonable expectation of privacy" in the information. This is not a threshold used in the Privacy Act, but is a legal test used in other areas of privacy law to assess the sensitivity of information and the level of protection it requires under the law.[21] If personal information comprises of details in which the individual would have a reasonable expectation of privacy, this is a strong indicator that the information is sensitive and should be treated accordingly under the Privacy Act.

A reasonable expectation of privacy is directed at protecting "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state" and includes information "which tends to reveal intimate details of the lifestyle and personal choices of the individual."[22]

There is generally a reasonable expectation of privacy in an individual's banking information, and telecommunications, for example.

However, other more routine data will not raise a reasonable expectation of privacy. For example, basic electricity data does not tend to reveal intimate details of the individual's

[21] For example, a reasonable expectation of privacy is a threshold under the torts of privacy and for purposes of section 21 of the New Zealand Bill of Rights Act 1990 (freedom from unreasonable search and seizure).
[22] *R v Alsford* [2017] NZSC 17 [56], [63], citing *R v Plant* [1993] 3 SCR 281.

lifestyle and personal choices. However, if the electricity data could reveal intimate details about an individual (such as from smart meters) this might raise a reasonable expectation of privacy.[23]

Prohibited grounds of discrimination

Another tool to assess the sensitivity of personal information is the list of grounds of prohibited discrimination in section 21 of the Human Rights Act 1993. The prohibited grounds of discrimination include sex (including pregnancy and childbirth, and gender identity), religious belief, ethical belief, colour, race, ethic or national origin, disability (including physical or psychiatric illness), age, political opinion, employment and family status and sexual orientation.

Political opinion can be revealed by information about a person's affiliations with political parties, with non-governmental organisations, or with organisations such as trade unions. This personal information is usually treated as sensitive information, as it is revealing of an individual's views and personal choices from which inferences can be drawn.[24]

The potential for discriminatory impacts from the collection use and disclosure of personal information relating to these grounds can have a bearing on whether the information should be treated as sensitive and require particular care. In particular, information about a person's physical or psychiatric illness is generally treated as highly sensitive information.

If information falls in a protected category under the Human Rights Act, that could require the agency to take additional "reasonable steps" for example, to keep that information secure (as discussed above).

[23] *R v Alsford*, above, fn96.
[24] See also the Te Kawa Mataaho | Public Service Commission July 2019 findings cautioning government agencies against collecting information on the political leanings or party affiliations of citizens.