ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

New Zealand

Status of Consent for Processing Personal Data

JUNE 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Daimhin Warner

Principal & Director, Simply Privacy

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Elizabeth Santhosh.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in New Zealand's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

The Privacy Act 2020[1] (the "**Act**") provides the default rules relating to the processing of personal information ("**PI**") under New Zealand law. These are articulated within and throughout the 13 Information Privacy Principles ("**IPPs**") contained in Section 22 of the Act. Note that any other laws which provide for the collection, use or disclosure of PI override the IPPs.[2]

The IPPs are summarized below. IPPs with direct relevance to consent are shown in bold:

- IPP 1 permits an agency to collect PI only to the extent necessary for a lawful purpose. There are no exceptions to this rule.
- **IPP 2** requires an agency to collect PI directly from the individual who is the subject of that PI. However, this rule is subject to an exhaustive list of exceptions, including consent (not that the Act uses the term "**authorization**"),[3] which an agency may rely on to collect PI from a third party. Thus, an agency may collect PI from a third party if the agency believes on reasonable grounds that the individual authorizes the collection of his/her PI from someone else.
- IPP 3 requires an agency to provide individuals with certain information when collecting PI directly from them. This rule is also subject to exceptions.
- IPP 4 permits an agency to collect PI only in ways that are lawful, fair, and not unreasonably intrusive. There are no exceptions to this rule. Notably, the fairness element has been interpreted as including consideration of imbalances of power, which might, for example, call into question the appropriateness of relying on authorization in certain circumstances.
- IPP 5 relates to storage and security of PI.
- IPPs 6 and 7 relate to individuals' rights to access and correct their PI.
- IPP 8 requires an agency to take reasonable steps to ensure that PI is accurate, complete, and up to date before using or disclosing it. There are no exceptions to this rule.
- IPP 9 permits an agency to retain PI only for as long as it is needed for a lawful purpose. There are no exceptions to this rule.
- **IPP 10** permits an agency to use PI only for the purpose(s) for which it was collected ("**primary purpose(s)**"). However, an agency may rely on an exhaustive list of exceptions, including authorization,[4] to use PI for a purpose other than the primary purpose ("**secondary purpose**"). Thus, an agency may use PI for a secondary purpose if it believes on reasonable grounds that the use of the information for that other purpose is authorized by the individual concerned.
- **IPP 11** states that an agency must not disclose PI to any other agency or person. However, this rule is subject to an exhaustive list of exceptions which entities may rely on to disclose PI. The primary exception is that the disclosure is either one of the purposes for which the information was collected or is directly related to those purposes.[5] Authorization is another exception[6] but is used less in practice. Thus, an agency may disclose PI if it believes on reasonable grounds that the disclosure is authorized by the individual concerned.
- **IPP 12** is New Zealand's cross-border information sharing provision and sets out an exhaustive list of legal bases to disclose PI to a foreign person or entity, including authorization (which must be accompanied by certain other information).[7]

---

[1] Available at https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
[2] Privacy Act 2020, Article 24.
[3] IPP 2(2)(a).
[4] IPP 10(1)(c).
[5] IPP 11(1)(a).
[6] IPP 11(1)(c).
[7] IPP 12(1)(a).

- IPP 13 relates to the assigning or use of unique identifiers.

2. ROLE OF THE PRIVACY COMMISSIONER

The Act establishes the Office of the Privacy Commissioner as an independent entity which administers and enforces the Act.[8]

The Privacy Commissioner has not issued specific guidance on consent requirements but has considered the scope of authorization in the context of specific sets of facts through Case Notes. For instance, the Commissioner considered and rejected an argument from a bank that a customer could be deemed to have consented to the disclosure of PI to the Police.[9] This reflects the fact that consent is not a significant feature of the Act.

The Act also empowers the Privacy Commissioner to issue codes of practice in relation to the IPPs to regulate specific classes of agency (such as health agencies), classes of PI (such as credit information), classes of activity (such as responding to a civil emergency), or classes of industry (such as telecommunications).[10] These codes can modify the IPPs to prescribe more stringent or less stringent standards[11] or exempt certain actions from the IPPs entirely.[12] However, a code cannot limit or restrict the application of IPPs 6 or 7, which provide for individuals' rights to access and correct their PI.[13]

2.1. Health Information Privacy Code 2020 ("HIPC")

The HIPC[14] specifically regulates the collection and use of health information by public and private sector health agencies. This code modifies several of the IPPs (termed "**Rules**" in the HIPC) in ways that place greater emphasis on consent, or authorization, recognizing the inherent sensitivity of health information and reflecting the more general concept of "informed consent" in the health sector.

It is worth noting the introduction of "representatives" in the health context. Clause 3(1) of the HIPC defines a "representative" as a personal representative of a deceased individual, a parent or guardian of an individual, or a person lawfully acting on behalf of someone who is unable to give their consent (e.g., under a power of attorney). In most cases where authorization is a legal basis to process health information, the representative can provide authorization if the individual is not able to do so personally.

Rule 2 (like IPP 2) permits a health agency to collect health information from a third party on the basis of authorization, among other legal bases. However, Rule 2(2)(a) goes further than the requirements of the Act by requiring a health agency to make the individual aware of the matters set out in Rule 3(1), which relates to transparency of purpose etc. By contrast, IPP 3 applies only where PI is collected from the person concerned. This additional requirement more clearly mandates a type of *informed* consent.

Rule 10 (like IPP 10) requires a health agency to use health information only for the purposes for which it was collected. However, a health agency may rely on an exhaustive list of exceptions, including authorization, to use PI for a secondary purpose. Thus, a health agency may use health information for a secondary purpose if it believes on reasonable grounds that the use of the information for that other purpose is authorized by the individual concerned or the individual's representative.

Rule 11 (like IPP 11) states that a health agency may not disclose health information to any other agency or person. However, Rule 11 differs from IPP 11 in a few material ways which appear to prioritize authorization for disclosure of health information

Firstly, while the first exception to IPP 11 is that the disclosure is one of the purposes for which the information was collected, the first exception to Rule 11 of the HIPC is authorization, followed by

---

[8] See Privacy Act 2020, Part 2.

[9] Sam Grover, "Hager and Westpac - A bit more context, information and clarification" *Privacy Commissioner website* (March 22, 2017), available at https://www.privacy.org.nz/blog/hager-and-westpac/

[10] Privacy Act 2020, ss 32(1) and 32(3).

[11] Privacy Act 2020, s 32(2)(a).

[12] Privacy Act 2020, s 32(2)(b).

[13] Privacy Act 2020, s 32(5).

[14] Available at https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/

purpose. This encourages health agencies to obtain the authorization of an individual or their representative to disclose health information.

Secondly, before a health agency can rely on the other equivalent exceptions to disclose health information (such as directly related purpose, research, public health or safety or maintenance of the law), a health agency must attempt to obtain individual authorization, and may only rely on the exceptions if authorization is "either not desirable or not practicable."

Rule 12 follows the same approach as IPP 12.

2.2. Credit Reporting Privacy Code 2020 ("CRPC")

The CRPC[15] specifically regulates the activities of credit reporters. While most CRPC rules mirror the IPPs, IPP 11 requires that disclosures of credit information to "subscribers" (e.g., credit providers, landlords, employers, or insurers) may only be made with the authorization of the individual concerned. As these disclosures form the bulk of a credit reporter's business, this is a significant regulatory departure from the IPPs.

The CRPC also specifically prohibits the use of bundled consent by credit reporters (discussed further below).

3. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PRIVACY ACT 2020

Consent is not the primary or default basis for collecting, using, and disclosing PI under the IPPs.

Rather, the default basis for collecting PI under the IPPs is that collection of PI must be necessary for a lawful purpose connected with a function or an activity of the agency ("**legitimate business purpose**").[16] Subject to exceptions,[17] the IPPs require that agencies collect PI directly from the individuals concerned[18] and notify individuals of, among others, the legitimate business purpose for collection.[19] By default, PI may only be used or disclosed for the lawful business purpose for which it was collected, or a purpose directly related thereto.[20]

"Authorization" (i.e., consent) functions as an exception to certain requirements under the IPPs. Specifically, where the agency believes, on reasonable grounds, that the individual has given authorization, the IPPs permit agencies to:

- collect PI from third parties other than the individual;[21]
- use PI for a legitimate business purpose other than the purpose of collection or a purpose related thereto;[22] and
- disclose PI for a legitimate business purpose other than the purpose of collection or a purpose related thereto. [23]

Additionally, authorization functions as one of several legal bases under the IPPs for cross-border transfer of PI, provided that the agency has expressly informed the foreign recipient may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Act.[24]

---

[15] Available at https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/crpc2020/
[16] IPP 1(1).
[17] IPP 2(2).
[18] IPP 2(1).
[19] IPP 3(1)(b)
[20] IPPs 10(1)(a) and 11(1)(a).
[21] IPP 2(2)(c)
[22] IPP 10(2)(c).
[23] IPP 11(2)(c).
[24] IPP 12(1)(a).

There is no specifically stated position from regulator, the government, or any other organization which provides the rationale for consent-based provisions in the law. However, the Privacy Commissioner has been vocally concerned about the limitations of consent as a lawful basis to collect, use, or disclose PI. In a much-cited blog post, the Commissioner expressed the view that consent without clarity is not enough and that there are other, more appropriate lawful bases to rely on in the Act.[25]

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

The Act uses the term "authorization" rather than "consent" but does not define this term. "Authorization" is generally understood to be something slightly more than consent, as it implies a level of informed decision making (i.e., a positive and conscious act) by the individual, whereas consent tends to convey a more passive position on the part of the individual.

The Act does not define the scope of authorization or refer to different forms of it. However, IPP 12, which relates to disclosures to foreign entities, requires a stronger form of authorization than appears to be required in other parts of the Act. Thus, IPP 12(1)(a) requires that an individual must have been "expressly informed" of the risks before authorizing an overseas transfer.

Note that the Unsolicited Electronic Messages Act 2007[26] ("**UEMA**"), which regulates the sending of direct marketing messages in New Zealand, uses the term "consent" and provides several definitions. Section 4(1) of the UEMA includes the following definition. The UEMA also recognizes:

- express consent;[27]
- consent that can reasonably be inferred,[28] including from the conduct and the business and other relationships of the persons concerned;[29] and
- deemed consent where:
  - an electronic address has been conspicuously published by a person in a business or official capacity;[30] and
  - publication of the address is not accompanied by a statement to the effect that the relevant electronic address-holder does not want to receive unsolicited electronic messages at that electronic address;[31] and
  - the message sent to that address is relevant to the business, role, functions, or duties of the person in a business or official capacity. [32]

4.2. Withdrawal of consent

The Act does not expressly provide for withdrawal of consent.

4.1. Bundled consent

The Act does not expressly refer to bundled consent or whether provision of goods and services may be made conditional on consent. However, depending on the circumstances, such practices may be

[25] John Edwards, "Click to consent? Not good enough anymore" *Privacy Commissioner website* (2 September 2019), available at https://www.privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/
[26] Available at https://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html
[27] Unsolicited Electronic Messages Act 2007 ("**UEMA**"), s 4(1)(a)(i).
[28] UEMA, s 4(1)(a)(ii).
[29] UEMA, s 4(1)(a)(ii)(A).
[30] UEMA, s 4(1)(a)(iii)(A).
[31] UEMA, s 4(1)(a)(iii)(B).
[32] UEMA, s 4(1)(a)(iii)(C).

inconsistent with the requirement that collection of PI must be by means that are fair in the circumstances of the case.[33]

The CRPC specifically prohibits the use of "bundled consent" in the context of credit reporting. Specifically, a credit reporter "must not bundle a request for authorization of an additional unrelated use or disclosure of credit information into application processes for access to credit information under Rule 6 of the CRPC, correction to credit information under Rule 7 of the CRPC, or suppression of credit information under Rule 11 CRPC.[34] This prohibition was intended to prevent concerning practices by credit reporters of making individual access and correction rights contingent on consent to use or disclose credit information in some way.

5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The Act does not recognize or make specific provisions for special categories or uses of PI.

However, note that the HIPC adopts a different approach to consent in the context of health information (see above).

5.1. Children

IPP 4 permits collection of PI only by means that are lawful[35] and fair in the circumstances of the case (particularly in circumstances where PI is being collected from children or young persons)[36] and do not intrude to an unreasonable extent upon the personal affairs of the individual concerned.[37]

This provision appears to hold collection of PI from children or young persons to higher standards of fairness and reasonableness. This may impact the appropriateness of relying on consent as a legal basis to process children's data.

6. CONSENT FOR CROSS-BORDER DATA TRANSFERS

IPP 12 sets out an exhaustive list of legal bases for disclosure of PI to a foreign person or entity. One such basis is where the individual authorizes the disclosure, after having been expressly informed that the information may not be protected by comparable safeguards to those required by the Act.[38]

It should be noted that unlike other privacy laws, including the GDPR, "disclosure" for the purposes of IPP 12 does not include sharing PI with a service provider.

7. TRANSPARENCY AND NOTICE

The Act does not define authorization and generally does not require provision of specific information before authorization can be established, except in the context of cross-border data transfers (see above).

However, IPP 3 sets out the requirements for a privacy notice when PI is collected from an individual. Specifically, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

- the fact that the information is being collected;[39]

[33] IPP 4(b)(i).
[34] CRPC, Rule 4(2).
[35] IPP 4(a).
[36] IPP 4(b)(i).
[37] IPP 4(b)(ii).
[38] IPP 12(1)(a).
[39] IPP 3(1)(a).

- the purpose for which the information is being collected;[40] and
- the intended recipients of the information;[41] and
- the name and address of the agency that is collecting the information;[42] and the agency that will hold the information;[43] and
- if the collection of the information is authorized or required by or under law:
  - the particular law by or under which the collection of the information is authorized or required;[44] and
  - whether the supply of the information by that individual is voluntary or mandatory; [45]
- the consequences (if any) for that individual if all or any part of the requested information is not provided;[46] and
- the rights of access to, and correction of, information provided by the IPPs.[47]

However, this notice requirement is subject to exceptions, and an agency is not required to provide the above information if the agency believes, on reasonable grounds that:

- non-compliance would not prejudice the interests of the individual concerned;[48] or
- non-compliance is necessary:
  - to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses;[49]
  - for the enforcement of a law that imposes a pecuniary penalty;[50]
  - for the protection of public revenue;[51] or
  - for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);[52] or
- compliance would prejudice the purposes of the collection;[53] or
- compliance is not reasonably practicable in the circumstances of the particular case;[54] or
- the information:
  - will not be used in a form in which the individual concerned is identified;[55] or
  - will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.[56]

---

40 IPP 3(1)(b).
41 IPP 3(1)(c).
42 IPP 3(1)(d)(i).
43 IPP 3(1)(d)(ii).
44 IPP 3(1)(e)(i).
45 IPP 3(1)(e)(ii).
46 IPP 3(1)(f).
47 IPP 3(1)(g).
48 IPP 3(4)(a).
49 IPP(4)(b)(i).
50 IPP(4)(b)(ii).
51 IPP(4)(b)(iii).
52 IPP(4)(b)(iv).
53 IPP(4)(c).
54 IPP(4)(d).
55 IPP(4)(e)(i).
56 IPP(4)(e)(ii).

8. SANCTIONS AND ENFORCEMENT

The Act does not provide specific sanctions for breach of the IPPs. Rather, the Act operates an enforcement and complaints regimes for general breaches of the IPPs that cause an "interference with the privacy of an individual."[57] This refers to any breach of the IPPs that:

- has caused, or may cause, loss, detriment, damage, or injury to the individual;[58]
- has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of the individual;[59] or
- has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of the individual.[60]

It may be an interference with the privacy of an individual if an agency seeks to rely on authorization to collect, use, or disclose PI, but no such authorization exists.

The Privacy Commissioner has a role in investigating and resolving privacy complaints[61] and can issue binding compliance notices in respect of breaches.[62] The Commissioner can also initiate, on its own motion, investigations into practices that, in the Commissioner's view, may breach the Act.[63]

It should be noted that the Act does not provide for the imposition of a punitive fine for an interference with the privacy of an individual. Rather, the Act empowers the Human Rights Review Tribunal to order agencies which have committed such interferences to pay compensation to affected individuals.[64] The individual in question would need to establish harm to qualify for an award of damages.

The Act also provides criminal offenses, punishable with monetary fines of up to NZD$10,000, including interfering with actions by the Privacy Commissioner.[65] Several of these offenses touch on the issue of consent, including:

- representing that a person holds any authority under the Act when the person does not;[66] and
- misleading an agency by impersonating an individual or pretending to be acting under the authority of an individual, in order to have information used.[67]

Active enforcement is occasional. For example, where an agency seeks to argue that an individual authorized the collection of his/her PI from a third party or authorized a particular use or disclosure of his/her PI (see case note references below for examples), such matters would be investigated and enforced under the Act's complaints and enforcement regime. For the most part, because the Act's enforcement regime is primarily complaint-based, it largely relies on individuals being aware of a breach and making a complaint to the Commissioner.

That said, the Commissioner has the power to inquire generally into any matter if it appears that the privacy of individuals is being, or may be, infringed.[68] The Commissioner has publicly stated that these powers will be used strategically to inquire into general agency practices. In view of the Commissioner's public concerns about consent, it is very possible that consent will be a future topic of inquiry.

The issue of authorization under the Act has received relatively little consideration in New Zealand. Neither the Commissioner nor the courts have generally scrutinized broad industry approaches to the use of consent (other than icy prohibiting bundled consent in the credit reporting sector through the

[57] Privacy Act 2020, s 69.
[58] Privacy Act 2020, s 69(2)(b)(i).
[59] Privacy Act 2020, s 69(2)(b)(ii).
[60] Privacy Act 2020, s 69(2)(b)(iii).
[61] See, generally, Privacy Act 2020, Part 5, Subparts 1 and 2.
[62] Privacy Act 2020, ss 102(2)(b) and 102(2)(d).
[63] Privacy Act 2020, s 79(b).
[64] Privacy Act 2020, s 103.
[65] Privacy Act 2020, s 212.
[66] Privacy Act 2020, s 212(2)(b).
[67] Privacy Act 2020, s 212(2)(c).
[68] Privacy Act 2020, s 17(1)(i).

CRPC). For the most part, questions of authorization have arisen in relation to specific acts by agencies, such as collection of PI from third parties, or *ad hoc* disclosures of PI.

8.1. Case Note 2976 [1996] NZ PrivCmr 1

On the facts of this case,[69] a married couple complained to the Privacy Commissioner on the ground that a bank had failed to obtain the couple's authorization to conduct a credit check on them when they opened a joint savings account with the bank.

The bank seemingly did not inform the couple that it would conduct a credit check on them and instead simply stated that it would get their application form checked. However, the bank proceeded to disclose the couple's names, address, dates of birth, occupations, and places of employment to a credit reference agency. After their visit to the bank, the husband and wife were both contacted at their workplaces by a debt collection agency regarding a dispute they were having about an account.

The Commissioner determined that the couple had not provided authorization for collection of their PI from a third party under IPP 2(2)(b). The Commissioner further considered that authorization for this purpose would require a "positive act" – failure to object would not amount to authorization.

8.2. Case Note 19740 [2002] NZ PrivCmr 5

On the facts of this case,[70] a woman applied for employment in a government department by completing the department's application form and providing her curriculum vitae and a written reference from her former employer. The application form required the woman to nominate a referee. The woman understood from this that the department would only contact the referee nominated in the form, and that if such a referee nominated another person to provide the reference, then the department would contact the woman.

The woman's application was unsuccessful, and the department returned her application documents to her. From the documents, the woman learned that the department had contacted her former employer, who had provided the written reference but was not nominated in the application form.

The Commissioner determined that the department had breached IPP 3 as it had failed to notify applicants that it had an internal policy of following up on all references, regardless of whether the applicant had nominated the referee in the application form. The Commissioner also took the view that the department was obligated to inform applicants of how the department would handle all information included in their application, not merely how it would handle nominated referees and people that they nominated.

Notably, the Commissioner rejected the department's argument that the woman, by providing a reference from her former employer, gave implied authorization for the department to contact her former employer as the department had given no indication of how such a reference, if provided, would be used.

8.3. *L v J* [1999] NZCRT 9

On the facts of this case,[71] the plaintiff was a patient of the defendant, a general medical practitioner. The plaintiff's cousin informed the defendant by telephone call that the plaintiff's family had a history of psychiatric problems. The defendant included this information in a referral relating to the plaintiff. A psychiatrist later diagnosed the plaintiff with a psychiatric condition, informed the defendant of this, and requested the plaintiff's medical notes. The defendant provided the psychiatrist with access to the defendant's medical files on numerous occasions.

---

[69] Available at https://www.privacy.org.nz/publications/case-notes-and-court-decisions/case-note-2976-1996-nzprivcmr-1-couple-complain-bank-conducted-unauthorised-credit-check-and-disclosed-employment-details/

[70] Available at https://www.privacy.org.nz/publications/case-notes-and-court-decisions/case-note-19740-2002-nzprivcmr-5-job-applicant-alleges-that-department-contacted-former-employer/

[71] Available at http://www.nzlii.org/nz/cases/NZCRT/1999/9.html

The Complaints Review Tribunal took the view that the defendant had breached, among others, Rule 2 of the version of the HIPC then in force by receiving PI about the plaintiff from the psychiatrist and by collecting PI about the plaintiff from the plaintiff's cousin.

However, the Tribunal did not find that the defendant had breached the version of the HIPC then in force by disclosing the plaintiff's medical records to the psychiatrist without the plaintiff's consent. The Tribunal took the view that the disclosure had been for one of the purposes for which the health information had originally been collected (i.e., providing treatment to the plaintiff) and that the psychiatrist would have been unable to fulfill this purpose without the information.

Notably, the Tribunal also appeared to recognize a form of implied authorization by acknowledging that the plaintiff had informed the psychiatrist that the defendant was her general medical practitioner and that there "must have been the clear implication that by asking for this information the psychiatrist would access her medical file, or those parts of it which were relevant to his treatment of her."[72]

8.4. *L v L* [2001] NZCRT 15

On the facts of this case,[73] the plaintiff complained that the defendant (a specialist obstetrician and gynecologist) had breached the version of the version of the HIPC then in force by disclosing the fact that the plaintiff had undergone a hysterectomy to the plaintiff's husband without the plaintiff's consent.

Before going into hospital for surgery, the plaintiff had named her husband as her next-of-kin in an admission form but did not complete the section of the form which requested the details of a person to be contacted after the operation. The plaintiff argued that she had intentionally left this section of the form blank.

However, following the surgery, the defendant called the home telephone number of the plaintiff and her husband and left message on an answering machine that the surgery had been completed. Later the same day, the plaintiff experienced complications and had to undergo an emergency surgery. The defendant called the plaintiff's husband to inform him of the emergency before the operation and called him again following the operation to advise that it had been completed.

The plaintiff argued that the three telephone calls made by the defendant were in breach of the plaintiff's express request that the defendant should not inform the husband of the plaintiff's surgery.

The Complaints Review Tribunal determined that the defendant had not breached the HIPC by making the telephone calls to the plaintiff's husband and disclosing the fact that the plaintiff had undergone the surgery. This was mainly based on the Tribunal's finding that the plaintiff had not established that she had expressly requested that the defendant should not contact the husband. However, the Tribunal also considered – notably – that the plaintiff had impliedly authorized the disclosure by providing the hospital with her husband's contact details.

8.5. *Lehmann v CanWest Radioworks Ltd* [2006] NZHRRT 35

On the facts of this case,[74] the defendant (a radio station operator) wanted to contact the plaintiff to discuss payment of a debt which the plaintiff owed to the defendant. To that end, the defendant arranged for a message inquiring about the plaintiff's whereabouts to be broadcast by its radio stations across New Zealand. The messages were broadcasted 73 times across four days in November 2001.

The plaintiff complained that the defendant's attempts to contact him contravened IPPs 1, 2, and/or 4.

The Human Rights Review Tribunal (successor to the Complaints Review Tribunal) dismissed the plaintiff's complaint and notably, held that the authorization exception to IPP 2 applied because the Tribunal found that the only PI about the plaintiff that was collected was his mobile telephone number, and that the defendant reasonably believed that the plaintiff authorized the defendant's collection of this information from the plaintiff's solicitor.

---

[72] *L v J* [1999] NZCRT 9, at page 7.
[73] Available at http://www.nzlii.org/nz/cases/NZCRT/2001/15.html
[74] Available at http://www.nzlii.org/nz/cases/NZHRRT/2006/35.html

8.6. *Powell v Accident Compensation Corporation* [2014] NZACC 89

In this case,[75] the Accident Compensation Corporation ("**ACC**") – the sole and compulsory provider of accident insurance in New Zealand for all work and non-work-related injuries – was challenged in relation to its use of broad and long-lasting authorization to collect, use, and share health information about claimants.

The case turned on form ACC167 ("**Form 167**") which required claimants to give consent for ACCC to collect, use, and disclose claimants' PI to assess their entitlement to compensation, rehabilitation, and medical treatment, and to help with evaluation of ACC's services and performance and research into injury prevention and effective rehabilitation.[76]

Form 167 also provided that the consent would apply to all aspects of claimants' claims, including agencies and services providers from whom ACC asks for information, or the whole period during which ACC provided assistance with the claim (subject to alternative arrangements negotiated with ACCC).[77]

The appellant had been injured in a 1989 and had received compensation payments on a weekly basis since then.[78] However, in 2007, ACC asked the appellant to sign an ACC 2 consent form (the precursor to Form 167)[79] and later, Form 167.[80] The appellant refused to sign the form, and ACCC therefore stopped compensation payments to her.[81]

The appellant challenged this decision on the basis that that the type and scope of information collected under Form 167, the sources of information authorized by Form 167, and the duration of the authority granted by Form 167 were broader than that permitted under Section 72(1)(c) of the Accident Compensation Act 2001 ("**ACA**").[82]

On appeal, the Dunedin District Court found that the authority sought by Form 167 was far greater than required and that the appellant had been given no ability to give a more limited authority which would nevertheless be compliant with Section 72(1)(c) of the ACA.[83]

On that basis, the Court found that a claimant's refusal to consent to the wide-ranging authority in Form 167 would not be unreasonable,[84] and ACC's decision to stop the plaintiff's entitlements on the basis that she had refused to sign Form 167 was unlawful.[85] The Court recommended that ACC adopt a new consent form as soon as possible.[86]

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

New Zealand law does not provide for as comprehensive a balancing test as that anticipated by Article 6(1)(f) of the European Union's General Data Protection Regulation ("**GDPR**"), or similar provisions of other laws.

However, the default approach to collection of PI under the IPPs shares many elements with balancing test under other laws like the GDPR. Specifically, both Article 6(1)(f) and the IPPs recognize that

---

[75] *Powell v Accident Compensation Corporation* [2014] NZACC 89 ("***Powell v ACC***"), available at http://www.nzlii.org/nz/cases/NZACC/2014/89.html
[76] *Powell v ACC*, at [44].
[77] *Powell v ACC*, at [44].
[78] *Powell v ACC*, at [3].
[79] *Powell v ACC*, at [5].
[80] *Powell v ACC*, at [11].
[81] *Powell v ACC*, at [12]-[22].
[82] *Powell v ACC*, at [33].
[83] *Powell v ACC*, at [45]-[46].
[84] *Powell v ACC*, at [47].
[85] *Powell v ACC*, at [48].
[86] *Powell v ACC*, at [49].

collection of PI is permitted where necessary for a lawful purpose that is connected with the functions or activities of the agency.

However, while the Act requires the agency to consider the possible impact of collection on the individuals concerned through the requirements of fairness and reasonableness of intrusion into the individual's personal affairs in IPP 4, the Act does not go as far as the GDPR, which expressly requires that the agency weigh its interest against the interests, rights, and freedoms the individual. That said, a situation in which the individual's interests, rights, and freedoms clearly overrode the agency's purpose for collecting the individual's PI likely would not meet the Act's fairness and reasonableness requirements.

Element	General Data Protection Regulation (European Union), Article 6(1)(f)	Privacy Act 2020 (New Zealand), Section 22
Necessity for a lawful purpose	Processing of personal data must be necessary for the purpose of a legitimate interest pursued by the controller or a third party.	Collection of PI must be where necessary for a lawful purpose connected with a function or an activity of the agency (**IPP 1(1)**).
Balance of interests	Processing is not permitted if the legitimate interest is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.	Collection of PI is permitted only by means that are lawful (**IPP 4(a)**) and fair (**IPP 4(b)(i)**) and do not intrude to an unreasonable extent upon the personal affairs of the individual concerned (**IPP 4(b)(ii)**).

9.1. Impact assessments

Part 7 of the Act relates to public sector information sharing and provides for the establishment by government agencies of Approved Information Sharing Agreements ("**AISAs**"). Section 150 of the Act requires the parties to an AISA to consult with the Privacy Commissioner. The AISA process established by the Commissioner includes a requirement for the parties to submit a Privacy Impact Assessment ("**PIA**") relating to the information sharing sought.

The Privacy Commissioner has published a Privacy Impact Assessment Toolkit,[87] and also provides full learning modules on completing PIAs and on the AISA process, including the PIA requirement.

Outside of the public sector, PIAs are considered to be good practice but are not mandated by law in New Zealand. The Commissioner recommends that agencies document their decision-making processes for using or disclosing PI under relevant legal bases and encourages agencies to publish their PIAs; however, this is not mandated by the law.

There is also no proactive statutory requirement to share PIAs with the Commissioner. However, note that the Privacy Commissioner has the power to request an agency to provide it with any information relevant to the exercise of powers under the Act.[88]

[87] Available at https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/
[88] Privacy Act 2020, s 202.

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

As discussed above, the Act does not require consent to collect PI from the individual concerned, provided that such collection is necessary for a lawful purpose connected with a function or activity of the agency.[89] The Act also permits the agency to use PI collected on this basis for the same purpose as that of collection.[90]

Apart from the above, IPPs 2, 10, and 11 each provide an exhaustive list of legal bases for, respectively, collecting PI from a third party, using PI for a secondary purpose, or disclosing PI without consent.

10.1. Collecting PI from a third party

IPP 2 permits collection of PI from persons other than the individual concerned without consent where the agency believes on reasonable grounds, that:

- collection from a third party would not prejudice the interests of the individual concerned;[91]
- collection from the individual concerned would prejudice the purposes of collection;[92]
- the information is publicly available;[93]
- collection from a third party is necessary:
  - to avoid prejudice to the maintenance of the law;[94]
  - for the enforcement of a law that imposes a pecuniary penalty;[95]
  - for the protection of public revenue;[96]
  - for the conduct of proceedings before a court or tribunal that have been commenced or are reasonably in contemplation;[97] or
  - to prevent or lessen a serious threat to the life or health of any individual;[98]
- collection from the individual concerned is not reasonably practicable in the circumstances[99] –note that this basis is interpreted extremely narrowly;
- the information:
  - will not be used in a form in which the individual concerned is identified;[100] or
  - will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.[101]

10.2. Using PI for a secondary purpose

IPP 10 permits use of PI for a secondary purpose without consent where the agency believes, on reasonable grounds that:

---

89 IPPs 1(1) and 2(1).
90 IPP 10(1).
91 IPP 2(2)(a).
92 IPP 2(2)(b).
93 IPP 2(2)(d).
94 IPP 2(2)(e)(i).
95 IPP 2(2)(e)(ii).
96 IPP 2(2)(e)(iii).
97 IPP 2(2)(e)(iv).
98 IPP 2(2)(e)(v).
99 IPP 2(2)(f).
100 IPP 2(2)(g)(i).
101 IPP 2(2)(g)(ii).

- the secondary purpose is directly related to the primary purpose;[102]
- the information is to be used:
  - in a form in which the individual concerned is not identified;[103]
  - for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;[104]
- the source of the information is a publicly available publication, and, in the circumstances of the case, it would not be unfair or unreasonable to use the information;[105]
- use of PI for a secondary purpose is necessary:
  - to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses;[106]
  - for the enforcement of a law that imposes a pecuniary penalty;[107]
  - for the protection of public revenue;[108]
  - for the conduct of proceedings before a court or tribunal that have been commenced or are reasonably in contemplation;[109] or
- the use of the information for that other purpose is necessary to prevent or lessen a serious threat to:
  - public health or public safety;[110] or
  - the life or health of any individual.[111]

Additionally, an intelligence and security agency that holds PI that was obtained in connection with a primary purpose may use the information for a secondary purpose if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.[112]

10.3. Disclosing PI

IPP 11 permits disclosure of PI where the agency believes, on reasonable grounds that:

- the disclosure is one of the purposes in connection with which the information was obtained or is directly related to such a purpose;[113]
- the disclosure is to the individual concerned;[114]
- the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information;[115]
- the disclosure is necessary—

[102] IPP 10(1)(a).
[103] IPP 10(1)(b)(i).
[104] IPP 10(1)(b)(ii).
[105] IPP 10(1)(d).
[106] IPP 10(1)(e)(i).
[107] IPP 10(1)(e)(ii).
[108] IPP 10(1)(e)(iii).
[109] IPP 10(1)(e)(iv).
[110] IPP 10(1)(f)(i).
[111] IPP 10(1)(f)(ii).
[112] IPP 10(2).
[113] IPP 11(1)(a).
[114] IPP 11(1)(b).
[115] IPP 11(1)(d).

  - to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses;[116]
  - for the enforcement of a law that imposes a pecuniary penalty;[117]
  - for the protection of public revenue;[118]
  - for the conduct of proceedings before a court or tribunal that have been commenced or are reasonably in contemplation;[119] or
- the disclosure is necessary to prevent or lessen a serious threat to:
  - public health or public safety;[120] or
  - the life or health of the individual concerned or another individual;[121] or
- the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;[122] or
- the information is to be used:
  - in a form in which the individual concerned is not identified;[123] or
  - for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;[124] or
- the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern.[125]

10.4. Exemptions to the Act

The Act excludes from its scope only:

- the Sovereign;[126]
- the Governor-General;[127]
- the House of Representatives;[128]
- a member of Parliament in their official capacity;[129]
- the Parliamentary Service Commission; [130]
- the Parliamentary Service; [131]
- an Ombudsman;[132]
- an inquiry or board of inquiry;[133] or

---

116 IPP 1(1)(e)(i).
117 IPP 1(1)(e)(ii).
118 IPP 1(1)(e)(iii).
119 IPP 1(1)(e)(iii).
120 IPP 1(1)(f)(i).
121 IPP 1(1)(f)(ii).
122 IPP 1(1)(g).
123 IPP 1(1)(h)(i).
124 IPP 1(1)(h)(ii).
125 IPP 1(1)(i).
126 Privacy Act 2020, s 8(b)(i).
127 Privacy Act 2020, s 8(b)(ii).
128 Privacy Act 2020, s 8(b)(iii).
129 Privacy Act 2020, s 8(b)(iv).
130 Privacy Act 2020, s 8(b)(v).
131 Privacy Act 2020, s 8(b)(vi).
132 Privacy Act 2020, s 8(b)(vii).
133 Privacy Act 2020, s 8(b)(viii) and 8(b)(ix).

- a news entity to the extent it is carrying out news activities.[134]

Further, the Act does not apply to the actions of an individual solely for the purposes of, or in connection with, the individual's personal or domestic affairs,[135] unless the collection, use, or disclosure of the PI would be highly offensive to a reasonable person.[136]

10.5. Collecting, using, or disclosing PI where obtaining consent is impractical, impossible, inappropriate, and/or would require disproportionate effort

The Act expressly permits an agency to collect PI from a source other than the individual concerned without the individual's consent where the agency believes, on reasonable grounds, that it would not be reasonably practicable in the circumstance of the case to collect the PI directly from the individual concerned.[137]

10.6. Necessity for performance of a contract between the individual and controller

The Act does not expressly provide that an agency may collect, use, or disclose PI for performance of a contract between the agency and the individual.

However, it is likely that the Act would permit such collection, use, or disclosure without consent under the default rule that PI may be collected where necessary for a lawful purpose connected with a function or an activity of the agency[138] and used[139] or disclosed[140] for a purpose directly related to the purpose of collection.

Alternatively, an agency would likely have reasonable grounds for believing that the individual has authorized collection of the individual's PI from a third party,[141] use of such information for a secondary purpose,[142] and/or disclosure of such information[143] if a valid and enforceable contract between the agency and the individual provides for any of these.

10.7. Necessity for a research purpose

The Act expressly permits an agency to collect PI from a third party,[144] use PI for a secondary purpose,[145] or disclose PI[146] without the individual's consent where the agency believes, on reasonable grounds, that the information will be used for a statistical or research and will not be published in a form that could reasonably be expected to identify the individual concerned.

10.8. Necessity for carrying out a task in the public interest

The Act does not provide a general legal basis for collecting, using, or disclosing PI without consent to carry out a task in the public interest.

---

134 Privacy Act 2020, s 8(b)(x).
135 Privacy Act 2020, ss 27(1) and 27(2).
136 Privacy Act 2020, ss 27(3).
137 IPP 2(2)(f).
138 IPP 1(1).
139 IPP 10(1)(a).
140 IPP 11(1)(a).
141 IPP 2(2)(c).
142 IPP 10(1)(c).
143 IPP 11(1)(c).
144 IPP 2(2)(g).
145 IPP 10(1)(b)(ii).
146 IPP 11(1)(h)(ii).

The default rule may permit certain government agencies to collect, use, and disclose PI to fulfill specific tasks in the public interest, but only insofar as these tasks are connected with the usual functions or activities of the agency in question.[147]

However, the Act does provide legal bases for collection of PI from a third party, use of PI for a secondary purpose, or disclosure of PI where necessary for certain specific tasks in the public interest, including:

- avoiding prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses;[148]
- enforcement of a law that imposes a pecuniary penalty;[149]
- protection of public revenue;[150]
- conduct of proceedings before any court or tribunal which have been commenced or are reasonably in contemplation;[151] and
- preventing or lessening a serious threat to:
  - the life or health of any individual[152] or
  - for use and disclosure of PI, public health, or public safety.[153]

10.9. Necessity for law enforcement, defense, or national security

The Act does not provide a general legal basis for collecting, using, or disclosing PI without consent for purposes of law enforcement, defense, or national security.

The default rule may permit certain government agencies to collect, use, and disclose PI for specific purposes in collection with law enforcement, defense, or national security, but only insofar as these purposes are connected with the usual functions or activities of the agency in question.[154]

However, the Act does provide legal bases for collection of PI from a third party, use of PI for a secondary purpose, or disclosure of PI where necessary for certain specific tasks related to these purposes, including:

- avoiding prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses;[155]
- enforcement of a law that imposes a pecuniary penalty;[156]
- protection of public revenue;[157] and
- conduct of proceedings before any court or tribunal which have been commenced or are reasonably in contemplation.[158]

Additionally, the Act permits use of PI for a secondary purpose, or disclosure of PI where necessary:

- to prevent or lessen a serious threat to public health or public safety;[159] or
- for an intelligence and security agency to perform any of its functions.[160]

---

147 IPP 1(1)(a).
148 IPP 2(2)(e)(i); IPP 10(1)(e)(i); IPP 11(1)(e)(i).
149 IPP 2(2)(e)(ii); IPP 10(1)(e)(ii); IPP 11(1)(e)(ii).
150 IPP 2(2)(e)(iii); IPP 10(1)(e)(iii); IPP 11(1)(e)(iii).
151 IPP 2(2)(e)(iv); IPP 10(1)(e)(iv); IPP 11(1)(e)(iv).
152 IPP 2(2)(e)(v); IPP 10(1)(f)(ii); IPP 11(1)(f)(ii).
153 IPP 10(1)(f)(i); IPP 11(1)(f)(i).
154 IPP 1(1)(a).
155 IPP 2(2)(e)(i); IPP 10(1)(e)(i); IPP 11(1)(e)(i).
156 IPP 2(2)(e)(ii); IPP 10(1)(e)(ii); IPP 11(1)(e)(ii).
157 IPP 2(2)(e)(iii); IPP 10(1)(e)(iii); IPP 11(1)(e)(iii).
158 IPP 2(2)(e)(iv); IPP 10(1)(e)(iv); IPP 11(1)(e)(iv).
159 IPP 10(1)(f)(i); IPP 11(1)(f)(i).
160 IPP 10(2); IPP 11(1)(g).

10.10. Necessity for vital interests of the individual, a health emergency, etc.

The Act does not provide a general legal basis for collecting, using, or disclosing PI without consent to protect the vital interests of individuals.

The default rule may permit certain agencies to collect, use, and disclose PI to protect vital interests of individuals, but only insofar as this purpose is connected with the usual functions or activities of the agency in question.[161]

However, the Act permits use of PI for a secondary purpose,[162] or disclosure of PI[163] where necessary to prevent or lessen a serious threat to the life or health of the individual concerned or another individual.

10.11. Necessity for compliance with a legal obligation

The Act does not provide a general legal basis for collecting, using, or disclosing PI without consent to comply with a legal obligation.

However, it is likely that the Act would permit such collection, use, or disclosure without consent under the default rule that PI may be collected where necessary for a lawful purpose connected with a function or an activity of the agency[164] and used[165] or disclosed[166] for a purpose directly related to the purpose of collection.

10.12. Necessity for prevention, detection, mitigation, and investigation of fraud, security breach, or other prohibited/illegal activities in high-risk scenarios

The Act does not provide a general legal basis for collecting, using, or disclosing PI without consent to prevent, detect, mitigate, or investigate prohibited or illegal activities.

However, it is likely that the Act would permit such collection, use, or disclosure without consent under the default rule that PI may be collected where necessary for a lawful purpose connected with a function or an activity of the agency[167] and used[168] or disclosed[169] for a purpose directly related to the purpose of collection.

10.13. Rule of interpretation

The Act anticipates a pragmatic interpretation of the IPPs. Section 21 of the Act requires the Privacy Commissioner when performing his/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 efficiently.

The exceptions to the IPPs generally incorporate an element of *reasonableness*. They require only that an agency believes "on reasonable grounds," but not that the agency is absolutely certain, that a legal basis applies. This incorporates subjective (belief) and objective (reasonable grounds) elements. An agency must show that it has applied its mind to this assessment at the time of the decision to apply the exception. Reasonable belief has been held to mean "an actual belief based on a proper

[161] IPP 1(1)(a).
[162] IPP 10(1)(f)(ii).
[163] IPP 11(1)(f)(ii).
[164] IPP 1(1).
[165] IPP 10(1)(a).
[166] IPP 11(1)(a).
[167] IPP 1(1).
[168] IPP 10(1)(a).
[169] IPP 11(1)(a).

consideration of the relevant circumstances,"[170] and the Supreme Court has held that it is a relatively low test.[171]

The burden of establishing that an exception applies rests with the agency seeking to rely on it. For example, an agency being asked to provide PI for the purpose of a law enforcement investigation must be able to satisfy itself that reasonable grounds exist to believe that the exception applies.[172]

Some exceptions (including maintenance of the law) also require the agency to satisfy a *necessity* element, which includes consideration of data minimization and proportionality. Necessity has been held to have a higher threshold than reasonableness. The Human Rights Review Tribunal – considering the application of the maintenance of the law exception – held that something was "necessary" when it was "required for a given situation, rather than that it was indispensable or essential."[173]

10.14.COVID-19

During the COVID-19 pandemic, the Privacy Commissioner issued a report on the sharing of health information between government health agencies and the Police under Rule 11 of the HIPC.[174] The report considered, among other things, the interpretation of a "serious threat" to public health or safety or to the life and health of individuals under Rule 11(2)(d) of the HPIC and clarified that:

- in determining whether a threat is serious, an agency should have regard to the likelihood of a threat being realized, the severity of the consequences if the threat is realized, and the time at which the threat may be realized;[175]
- a key consideration for ongoing disclosures is that the nature of the serious threat must be kept under regular review to make sure that the use and disclosure of PI remains necessary to respond to the nature of the serious threat presenting at the relevant point in time;[176] and
- the public health and safety exception does not offer a wholesale license to depart from the privacy principles for general operational purposes – rather, it is targeted to the particular threat and the necessity of using or disclosing PI to prevent or lessen that threat.[177]

---

[170] *Geary v Accident Compensation Corporation* [2013] NZHRRT 34.
[171] *R v Alsford* [2017] NZSC 42 at [34].
[172] *R v Alsford* [2017] NZSC 42 at [33], in which the Supreme Court stated that a requesting agency must provide a holding agency with sufficient information to enable it to reach a reason-based view about whether or not requested information is required for an authorized purpose.
[173] *Tan v New Zealand Police* [2016] NZHRRT 32 at [78].
[174] Privacy Commissioner, "Inquiry into Ministry of Health disclosure of Covid-19 Patient Information" ("**COVID-19 Report**") (September 2020), archived version available at https://web.archive.org/web/20210212101100/https://www.privacy.org.nz/assets/DOCUMENTS/Inquiry-into-Ministry-of-Health-Disclosure-of-Covid-19-Patient-Information.pdf
[175] COVID-19 Report, at [49].
[176] COVID-19 Report, at [50].
[177] COVID-19 Report, at [51].

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG