(1) PERMANENT ORDERS PROHIBITING PUBLICATION OF NAME, ADDRESS AND IDENTIFYING PARTICULARS OF THE AGGRIEVED INDIVIDUALS AND EVIDENCE GIVEN BY MR COCKER AT PARAGRAPH 7 OF HIS WITNESS STATEMENT DATED 18 JUNE 2019

(2) PERMANENT ORDER PREVENTING SEARCH OF THE TRIBUNAL FILE WITHOUT LEAVE OF THE TRIBUNAL OR OF THE CHAIRPERSON

IN THE HUMAN RIGHTS REVIEW TRIBUNAL **[2022] NZHRRT 15**

I TE TARAIPIUNARA MANA TANGATA

Reference No. HRRT 040/2018

UNDER	**THE PRIVACY ACT 2020**
BETWEEN	**DIRECTOR OF HUMAN RIGHTS PROCEEDINGS**
	PLAINTIFF
AND	**NETSAFE INCORPORATED**
	DEFENDANT

AT WELLINGTON

BEFORE:
Mr RPG Haines ONZM QC, Chairperson
Ms K Anderson, Deputy Chairperson
Ms WV Gilchrist, Member
Ms ST Scott QSM, Member

REPRESENTATION:
Mr SRG Judd and Mr G Robins for plaintiff
Ms SC Carter for defendant

DATE OF HEARING: **15 to 25 July 2019**

DATE OF DECISION: **22 March 2022**

(REDACTED) DECISION OF TRIBUNAL[1]

---

[1] [This decision is to be cited as *Director of Human Rights Proceedings v Netsafe Inc* [2022] NZHRRT 15. Note publication restrictions.]

INTRODUCTION

[1] The Director of Human Rights Proceedings (Director) alleges interferences with the privacy interests of three aggrieved persons, [redacted] (Ms A), [redacted] (Ms B) and [redacted] (Ms C).

[2] In April 2017 these women each requested their personal information from Netsafe Incorporated (Netsafe). Netsafe refused their requests, but in January 2018 released some information to each of them. Netsafe has conceded that there was no basis to have withheld the information that was subsequently released to the three women in January 2018. That is an appropriate concession.

[3] Netsafe considers its refusal of each of the three Information Privacy Principle (IPP) 6 requests was justified under s 27(1)(c) and s 29(1)(a) of the Privacy Act 1993 (PA 1993). Those provisions respectively enable requests to be refused to avoid prejudice to the maintenance of the law or if doing so would result in the unwarranted disclosure of the affairs of another. The effect of s 88 is that Netsafe bears the onus of proving that either or both exceptions apply.

[4] The Director's statement of claim contains two causes of action. The first is that the IPP 6 requests were incorrectly refused in that there was no proper justification under PA 1993, ss 27(1)(c) and 29(1)(a). The second is that when Netsafe did hand over some documents (in January 2018, post refusal of the IPP 6 requests) this was out of time and a deemed refusal followed. As there is no separate and distinct interference with privacy by virtue of the undue delay in releasing the information, this second cause of action does not need to be considered (*Turner v The University of Otago* [2021] NZHRRT 18 at [39]).

[5] Accordingly, the liability issue is whether Netsafe has proved, on the balance of probabilities, that refusals of the three April 2017 IPP 6 requests were justified under s 27(1)(c) and/or s 29(1)(a).

[6] If that onus is not discharged by Netsafe, an interference with the privacy of the three aggrieved individuals will have occurred (s 66(2)). Issues of some complexity in relation to the question of remedies under ss 85 and 88 of the Privacy Act would then arise.

[7] The Director's claim was both filed and heard under the Privacy Act 1993. On 1 December 2020 the Privacy Act 1993 was repealed and replaced by the Privacy Act 2020. The transitional provisions in Privacy Act 2020 Schedule 1, Part 1 cl 9(1) provide that the present proceedings must be continued and completed under the 2020 Act, but the relevant legal rights and obligations in force at the time the actions subject to this claim were taken are not altered. Accordingly, all references in this decision are to the 1993 Act.

EVIDENCE: LIABILITY

[8] Evidence relevant to liability is discussed in the following section. Evidence relevant to remedies issues is set out later in this decision.

Context

[9] Netsafe is the Approved Agency under the Harmful Digital Communications Act (HDCA). The HDCA is intended (among other things) to prevent and mitigate harm

caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress. This Act was fully in force as from 21 November 2016.

[10] As the Approved Agency, Netsafe's functions include receiving and assessing complaints about harm caused to individuals by digital communications. It is also (among other things) required to investigate complaints and to use advice, negotiation, mediation and persuasion (as appropriate) to resolve complaints (HDCA, s 8). It does not itself have coercive powers or the power to institute proceedings in the District Court under the HDCA.

[11] The making of a complaint to the HDCA is the initial step a person must take before being able to initiate civil proceedings under the HDCA in the District Court. The District Court can order an individual to take down material, cease or refrain from certain conduct, or publish a correction and/or an apology (among other possible orders) (HDCA, s 19). Interim orders to the same effect can be made by the Court (HDCA, s 18).

[12] Two months after the HDCA came into effect, in January 2017, Mr Z made a complaint to the HDCA about certain digital communications by Ms A. Under HDCA s 12(1) Mr Z could apply to the District Court for orders against named producers, provided that Netsafe had first received a complaint about a digital communication, and had had a reasonable opportunity to assess the complaint and decide what action (if any) to take. Evidence of the steps taken by Netsafe is provided in the form of a Case Summary prepared by Netsafe.

[13] Three days after making a complaint to Netsafe, Mr Z received a Case Summary from Netsafe. Mr Z was then able to, and did, issue proceedings against the three aggrieved persons in the District Court. Mr Z also applied for interim orders against the three defendants. His application for interim orders was on a without notice basis, meaning the three aggrieved persons had no knowledge of the application and were not heard by the Court before the application was determined. After initially referring the matter back to Netsafe, the Court granted the interim orders Mr Z had sought.

[14] Between 7 and 11 April 2017 each of the aggrieved persons was served with copies of the interim orders affecting them. On 7, 11 and 18 April they separately applied to Netsafe for access to their personal information. Their requests were initially refused in their entirety. Some nine months later, Netsafe released a limited amount of information to them.

[15] The documents which Netsafe has continued to withhold have been made available to the Tribunal (Closed Bundle). These documents relate to dealings between Netsafe and Mr Z about his complaint, his application to the District Court, dealings between Netsafe and the District Court, and include information recorded by Netsafe staff in Netsafe's Zendesk system (its customer information system).

[16] The evidence contained in the Closed Bundle has been addressed in closed hearings from which the aggrieved persons and the public were, of necessity, excluded. Due to the Director's unique role, Netsafe had however also made the Closed Bundle available to the Director. The Tribunal has therefore had the benefit of submissions by the Director in relation to whether there were lawful grounds to withhold the documents in the Closed Bundle.

[17] At the time of the hearing of this proceeding, Mr Z's HDCA proceedings were part heard only. Following the conclusion of the Tribunal's hearing, the Director advised the Tribunal that Mr Z and the three women had settled the HDCA proceeding. The District Court issued orders cancelling or otherwise discharging the interim orders (and certain costs orders). In addition, permanent suppression orders were made in respect of the names of all parties and the evidence given in the HDCA Court proceeding (both by way of affidavit and viva voce).

[18] The effect of those orders is to limit evidence that can be referred to in the public version of this decision, given the overlap between certain evidence before this Tribunal and that which was in evidence before the District Court. Permanent non-publication orders, discussed later in this decision, are made by the Tribunal in these circumstances.

Evidence for the Director

[19] Each of the three aggrieved persons gave evidence. They explained the pre-existing history between Mr Z and them. Ms A and Ms B had previously each been in relationships with Mr Z. After each of those respective relationships had ended, they were subjected to online and other harassment by Mr Z. This occurred in the period before the HDCA came into effect, hence the remedies under the HDCA were not available to the aggrieved persons at the relevant time.

[20] In the Family Court both Ms A and Ms B had been granted temporary and then final protection orders against Mr Z. Ms C had supported Ms A and Ms B through the civil court processes in relation to the temporary and permanent protection orders against Mr Z, and then in criminal processes relating to Mr Z's breaches of those orders, for which Mr Z was convicted.

[21] The women made it clear to the Tribunal that collectively they consider Mr Z's use of the HDCA processes was another form of harassment of them by Mr Z.

[22] They also stated that their own social media postings identified in the District Court civil claim are largely private Facebook postings. They expressed concern that, despite their attempts to block Mr Z from their online communications, he appeared to have been able to access their private communications. They consider this is a continuation of cyber stalking activity that resulted in the previous protection orders against him.

[23] Against that background, we address the evidence of each of the aggrieved persons.

Ms A's evidence

[24] Ms A's evidence explained the context in which she had obtained a protection order against Mr Z in 2015 and the prosecution of him for breaching orders against her and Ms B.

[25] Ms A was served with District Court *ex parte* interim orders made under the HDCA in late March 2017 at her place of work. This was the first time she had any awareness of Mr Z's complaint to Netsafe about digital communications produced by her and the orders made by the Court under the HDCA.

[26] Due to technical defects with the formal service documents, and after Ms A had been in communication with the Court, amended interim orders were served on her on 7 April 2017 (being the formal date of service).

[27] These interim orders required that Ms A (and the two other women):

> **[27.1]** Cease or refrain from posting any communications in respect of Mr Z on any form of social or public media.
>
> **[27.2]** Refrain from inciting others to communicate like material in relation to the plaintiff on any form of social or public media.

[28] One of the documents served on Ms A was page 1 of Netsafe's Case Summary dated 18 January 2017. This document identified Ms A as the 'Alleged Producer' of the digital communication complained about by Mr Z. The other two women (Ms B and Ms C) were not identified as producers on the Case Summary or otherwise referred to in this Summary. The Case Summary identified the following Communication Principal Breaches:

A digital communication should not be threatening, intimidating or menacing	Serious Breach
A digital communication should not be used to harass an individual	Serious Breach
A digital communication should not make a false allegation	Serious Breach, multiple
A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual	Breach

[29] Under the heading "Assessment of Harm" the words "Serious Emotional Distress" were recorded. There was a further statement "Likely to cause harm: Yes."

[30] Ms A's evidence includes:

> The material provided that day [7 April 2017] made it clear that Netsafe had determined I had breached, in multiple and serious ways, the communication principles in the HDCA and the Court had made similar findings. What was not clear was what Mr [Z] had said about me to Netsafe. Nor was it clear what activity had been "determined" to breach the communication principles, and exactly what I needed to cease or refrain from doing. Given the care I had taken, and the experience I was trying to share, I was confused as to how my 14 January 2017 post could have been determined to be a clear breach of the HDCA communication principles (as I was led to believe by the papers served on me). I thought there must have been a mistake, or that Mr [Z] had convincingly spun an alternative reality or had either generated fabricated material that he was claiming to be from me or had wrongly attributed material generated by others to me.

[31] Ms A immediately contacted Netsafe, sending an email just after 5 pm on 7 April 2017, to queries@Netsafe.org.nz. In this email Ms A advised she had just been served with an interim order made under the HDCA and requested, as a matter of urgency, that she be provided with copies of Mr Z's complaint about her to Netsafe, the complete Case Summary (noting she had been served with a one-page document only), and any notes, materials, documents or other information in relation to the assessment and investigation into the claim and details of all correspondence and/or communications with the Court in relation to the matter. She asked that the request be dealt with urgently, noting that

matters were before the Court. Ms A also identified that Exhibit B to Mr Z's affidavit was a one-page document purporting to be a Netsafe Case Summary.

[32] Netsafe responded on 10 April 2017 acknowledging receipt of Ms A's information request and asking for reasons why the request should be treated as urgent. On 11 April 2017 Ms A replied to Netsafe advising that interim orders have been made against her without notice. She advised:

> [G]iven Mr Z's history, it is important that this matter is resolved as quickly as possible. In order for that to occur, we need to understand what exactly has occurred to date. I would rather not be forced to raise the processing of this matter with the Ombudsman at this date, so look forward to receiving the information as quickly as possible.

Later that same day Netsafe responded to Ms A, confirming that it accepted that there was a genuine and legitimate need for urgency.

[33] On 20 April 2017, Netsafe provided its substantive response to Ms A and refused to release any information to her. Netsafe relied upon ss 27(1)(c) (release would be likely to prejudice the maintenance of the law) and 29(1)(a) (to prevent the unwarranted disclosure of the affairs of another) when refusing the personal information requests (and other grounds for refusing Official Information Act requests, which are not part of this proceeding).

[34] Netsafe's explanation of the applicability of the maintenance of the law ground was as follows:

> In performing its statutory alternative dispute investigation/resolution functions Netsafe relies on the free and unsolicited flow of information, which is in the public interest and crucial to Netsafe's law maintenance function.
>
> Netsafe has no power to compel parties to disclose information. As such, it is vitally important that Netsafe safeguards its ability to persuade the parties involved to volunteer full, frank and untainted factual responses. Such responses help Netsafe decide what its involvement should be in each case and are essential to derive consensual outcomes.
>
> If information gathered during the investigation or resolution process could be obtained by a counterparty or third-party (by way of requests under the Privacy Act or OIA) the parties involved would likely tailor their responses accordingly or refuse to provide Netsafe with information. This would have a significant adverse impact on the exercise of Netsafe's statutory alternative dispute investigation/resolution functions as provided for under the HDCA.

[35] Netsafe's explanation of the applicability of s 29(1)(a) (avoiding the unwarranted disclosure of the affairs of another), was as follows:

> The requester's rights of access to the information is outweighed by the other person's privacy rights. The information requested was generated and/or obtained in confidence and "without prejudice".
>
> There are exceptions to confidentiality and the "without prejudice" privilege, however, no exception appears to apply in this case. As such, it is not appropriate for the information to be released, either in part or in full.

[36] These explanations of the withholding grounds are replicated in Netsafe's letters to Ms B and Ms C refusing their information requests. In other words, Netsafe's responses to each of the women were identical.

[37] Ms A says that a consequence of Netsafe's refusal was that she was not able to ascertain what Mr Z had said about her, what activity or actions formed the basis of his

complaint, and she did not have a full copy of the Case Summary or any information on Netsafe's assessment or investigation.

[38] Ms A explained in her evidence that she had been seeking, consistently, to understand what she had done that Netsafe considered was in breach of the communication principles under the HDCA, but that she remained in the dark.

[39] Following Netsafe's refusal, and encouraged by the Court to do so, the three women applied to the District Court for orders requiring Netsafe to release Mr Z's complaint information to them. In response to the non-party discovery application, Netsafe identified the lack of jurisdiction for the District Court to order discovery in HDCA proceedings, due to r 49 of the HDC Rules. The unavailability of the discovery mechanism under relevant Rules was accepted by the women, and their discovery application was withdrawn.

[40] It does not appear that the three women considered applying to the Court under PA, s 11(1) to enforce their IPP 6(1) right. That is a right that is enforceable in a court of law, and is a right distinct from a right to discovery under relevant Court Rules.

[41] Following the Privacy Commissioner's intervention, there was a release of certain documents by Netsafe to Ms A (and the two other women) on 15 January 2018.

[42] The January 2018 release was limited to copies of:

> **[42.1]** Documents the women had already received via the service of the District Court documents (Mr Z's February 2017 application to the District Court and his affidavit in support).
>
> **[42.2]** The women's own correspondence with Netsafe.
>
> **[42.3]** A complete copy of the Case Summary (i.e. including the previously missing page 2).
>
> **[42.4]** A heavily redacted copy of Mr Z's complaint to Netsafe.
>
> **[42.5]** A few emails between Mr Z and Netsafe.

[43] The second page of the Case Summary released at this time contained the following information:

> Should you decide to make an application to the District Court for an order/s under the Harmful Digital Communications Act 2015, you must attach this case summary to the application.
>
> The purpose of this case summary is to provide the District Court with information to help the court determine whether Netsafe has:
>
> - received a complaint;
> - had a reasonable opportunity to assess the complaint and decide what action to take (if any);
> - made an attempt to resolve the complaint.
>
> This case summary is not to be used for any purpose other than the purpose stated above. It is not to be construed as legal advice or a decision in favour of any party.

For more information please call Netsafe 0508 638723 (NETSAFE). Our contact centre is open from 8 am – 8 pm Monday to Friday, and 9 am – 5 pm Saturday and Sunday.

[44] As detailed below, Netsafe relies on page 2 of the Case Summary for its submission that it had not determined that Ms A had breached the specified communication principles.

[45] The day after receiving the January 2018 tranche of documents (16 January 2018) Ms A emailed Netsafe noting that the information provided did not respond to the full scope of information she had requested. Specifically, she identified that she did not have Netsafe's correspondence or communication with the Court about her and did not have any clarification of what aspects of her activity were breaches of the communication principles under the HDCA. She asked for prompt resolution of her outstanding requests, but did not receive such resolution.

Ms B's evidence

[46] Ms B's evidence outlined the harassment she experienced from Mr Z when their relationship had ended in 2014, the temporary protection order she obtained, and Mr Z's conviction for breaching the temporary protection order, on the basis of his psychological violence.

[47] Her temporary protection order against Mr Z was made final in April 2016.

[48] Ms B had been diagnosed with PTSD, as a result of Mr Z's actions. She was in therapy until April 2017.

[49] Ms B was the first of the three women to be served with the District Court interim orders. She says she was not surprised given the history of Mr Z making a police complaint about her and a complaint to the Broadcasting Standards Association against a journalist who had interviewed Ms B about protection orders (neither complaints being upheld).

[50] She assumed that Mr Z had fabricated digital material to get Netsafe to make its findings and then presented other material to the Court. The reason for her assumption was that most, if not all, of the documents relating to her referred to in the documents served on her did not exist digitally (because she had taken postings down some time ago). In addition, there was material that had no relevance to Mr Z and material that no reasonable person could have inferred referred to him.

[51] Ms B could see that she (like Ms C) was not named on the Case Summary. She refers to trying to figure out how the three of them were defendants in the District Court when only Ms A was named in the Case Summary.

[52] On 11 April 2017 Ms B asked Netsafe for information on her rights with respect to disclosure of information relating to the complaint, the assessment process by which allegations are determined to be false, the process for assessing harm and by whom and who had made the decision in relation to the assessment of harm. She asked what checks Netsafe does to determine the veracity and online content of screenshots (among other policy and process queries).

[53] The following day (12 April 2017) Netsafe acknowledged receipt of Ms B's information request and advised that the questions would be answered in accordance with the Official Information Act.

[54] On 13 April 2017 Ms B wrote to Netsafe stating that the timeframe proposed was not appropriate in the circumstances and advised of Mr Z's previous convictions for psychological violence against her. She emphasised her distress and asked for an urgent response.

[55] Following a further exchange with Netsafe, on 18 April 2017 Ms B wrote to Netsafe:

> I therefore wish to request, under the Privacy Act and the OIA, information you hold on the case quoted previously. Given this matter is before the court and for the personal situation also outlined previously I ask that this be dealt with urgently.

[56] The following day Netsafe confirmed that it would treat this further request with urgency.

[57] On 20 April 2017 Netsafe refused Ms B's request. The reasons for refusing her Privacy Act request are identical to those provided to Ms A and Ms C (refer paragraphs [34] to [35] above).

[58] Netsafe released a limited amount of information to Ms B in January 2018.

Ms C's evidence

[59] Ms C was the last of the three women to be served with the District Court orders.

[60] On 11 April 2017 Ms C emailed Netsafe seeking information. She noted that she was named as a defendant in court proceedings but was not named in the documents provided to the court.

[61] An aspect unique to Ms C was that the Facebook posts provided by Mr Z to Netsafe referred to her under her maiden name. That position was the same in relation to the copies of posts Mr Z attached to his affidavit filed in the District Court. The name she was identified by in the civil proceedings against her therefore differed from the name in the social media extracts Mr Z had included in the affidavit he filed in the District Court.

[62] Ms C requested all information about the case and any communications or cases pending relating to her. She also sought all notes in relation to the investigation, details of all related communications with the Court, and details of any communication and all cases received about her. Ms C advised that she had been served the interim court order based on a very biased submission from a vexatious litigant and therefore requested that her request was treated urgently. She said the entire process was causing her anxiety and emotional harm.

[63] As in the case of Ms A and Ms B, the reasons for Netsafe's refusal were those set out in the withholding grounds of PA 1993, ss 27(1)(c) and 29(1)(a), and with the same explanations as set out in paragraphs [34] to [35] above.

[64] Ms C sent an email to Netsafe on 21 April 2017 advising she was surprised that Netsafe would not even confirm whether a complaint had been made against her (as she was not named in the Netsafe report provided to the Court). She noted:

> I fail to see how releasing this, whether there was a finding by Netsafe relating to me or indeed to what constituted the relevant "harmful" material which I have allegedly produced, meets any of your reasoning.

[65] She also stated:

> I am completely disinterested in Mr Z's or any other such personal material; I ask for facts and Netsafe's findings only.

[66] Netsafe's response on 27 April 2017 was to advise Ms C of her right to take matters to the Ombudsman and/or the Privacy Commissioner. Ms C never got an answer to her question about whether there was a complaint about her. As discussed below, Netsafe says that the answer was inherently 'no', on the basis that this was the inference to be drawn when Netsafe wrote to Ms C saying the matter was before the Court.

Complaints are made to the Privacy Commissioner

[67] On 3 July 2017 Ms A made a complaint to the Privacy Commissioner. She identified herself as a victim of domestic violence and that her abuser had made a complaint to Netsafe about her. She considered that there had been a breach of:

> **[67.1]** IPP 5, on the basis Netsafe did not ensure there were reasonable safeguards in place to prevent misuse of her personal information.
>
> **[67.2]** IPP 6, on the basis Netsafe has refused to disclose any information about the complaint.
>
> **[67.3]** IPP 7, on the basis Netsafe has not provided an opportunity to correct information it has about her.
>
> **[67.4]** IPP 8, on the basis Netsafe did not take all reasonable steps to check information before releasing its assessment Case Summary to Mr Z (noting he is a convicted criminal and information on this is available online).

[68] Ms B and Ms C made similar complaints.

[69] The Privacy Commissioner's provisional opinion was that all the material should be released. Netsafe then proceeded to re-assess what it considered should be released. A date of release was agreed between Netsafe and the Privacy Commissioner.

[70] On 21 December 2017, the Office of the Privacy Commissioner advised the three women that Netsafe was not meeting the agreed release date of 22 December 2017 (previously extended from 15 December) as:

> Unfortunately other parties have raised objections to the disclosure, and Netsafe is considering whether to extend the disclosure date to respond to them.

[71] In the circumstances the Office of the Privacy Commissioner advised it was closing its file with a finding Netsafe had breached IPP 6 of the Privacy Act and had interfered with the women's privacy.

[72] The delay arose because Netsafe had been checking that Mr Z consented to releasing information to the three women. On 3 January 2018, Mr Z's lawyer advised Netsafe that his client would not seek to prevent the release of the relevant information.

[73] On 16 January 2018 Netsafe released certain information to the three women.

Evidence for Netsafe

[74] Both Netsafe's Director of Operations, Ms Helen O'Toole, and its Chief Executive, Mr Martin Cocker gave evidence on behalf of Netsafe.

[75] No evidence was provided by the Case Manager who had dealt with Mr Z's complaint and who prepared the Case Summary provided to Mr Z.

[76] However, Netsafe's documentary record relating to Mr Z's complaint and interactions between Netsafe and Mr Z are before the Tribunal, save for the record of one phone call between Mr Z and Netsafe that was not available due to technical reasons at the time of that call. No substantive issue is likely to have turned on that missing documentation.

[77] Ms O'Toole had had some interactions relating to Mr Z's complaint to Netsafe. This occurred after Mr Z had initiated proceedings in the District Court and the Court had referred the matter back to Netsafe. She provided direct evidence relating to this development. In addition, Ms O'Toole provided evidence on Netsafe's processes when it receives a complaint, Netsafe's involvement after it has closed its file, and what happened in relation to Mr Z's complaint to Netsafe. This latter aspect included the documentary record of Netsafe's assessment of the complaint and issue of the Case Summary, and interactions with Mr Z before and after he filed his application in the District Court.

[78] Mr Cocker confirmed that, while not the author of relevant correspondence, ultimately he was responsible for the April 2017 responses to the three personal information requests and the January 2018 release of certain information to the three women. He provided direct evidence of the considerations that underpinned these decisions. Mr Cocker also gave evidence about (among other things) the intent of the HDCA, the establishment of Netsafe, Netsafe's role on receipt of a complaint, Netsafe's reliance on confidentiality, and its role in proceedings under the HDCA (including Netsafe's processes being the gateway to District Court proceedings).

Evidence of Ms O'Toole

[79] Key aspects of Ms O'Toole's evidence included:

> **[79.1]** Netsafe always treats reports of harmful digital communications as being confidential, with assurances being provided by Case Managers to complainants that their report will be treated as confidential, subject to the need to tell someone else if Netsafe considers the person or another could be seriously harmed.
>
> **[79.2]** In the context of Netsafe's role concerning resolution of complaints, a Case Manager may offer to get in touch with the producer of the communication. However any such action would only be taken with the complainant's consent, save if there was a serious and imminent risk of suicide, in which case Police would be asked to do a welfare check.
>
> **[79.3]** For the purposes of verification of information provided to Netsafe, Netsafe seeks screen shots or links (URLs) to relevant communications. This is so that Netsafe can ensure the communications are real. However other than these verification checks, Case Managers do not take any steps to establish who produced the communication or what the background is. A Case Manager would

only contact the alleged producer to get more background information with the complainant's consent.

[79.4] A complaint is closed when the Case Manager is satisfied that there are no further steps that Netsafe can take to provide advice or to resolve the dispute. When the complaint is closed, the Case Manager will provide a link to the Ministry of Justice web page relating to making an application to the District Court under the HDCA and provide them with a Case Summary, as it is a document required for any such application.

[79.5] Mr Z provided Netsafe with a copy of his application to the District Court and affidavit in support, although not being required to do so. As a consequence, Netsafe knew that Mr Z had stated in his affidavit provided to the Court that Netsafe had determined that the relevant communication principles had been breached and had omitted to include page 2 of the Case Summary. However Netsafe did not consider it was its role to advise the Court that Netsafe's position is that it does not make any such determinations, and did not attempt to correct information Mr Z had put before the Court.

[79.6] That Netsafe has treated the complaint by Mr Z as relating to Ms A only. The Case Summary was therefore prepared in relation to Ms A only.

[79.7] Mr Z applied to the Court in relation to the three women. Netsafe's view was that at the point the Court referred the matter back to Netsafe, this became a complaint about three people.

Evidence of Mr Cocker

[80] Mr Cocker addressed Netsafe's statutory functions under the HDCA. These (relevantly) include:

[80.1] Receiving and assessing complaints about harm caused to individuals by digital communications.

[80.2] Investigating complaints.

[80.3] Using advice, negotiation, mediation and persuasion (as appropriate) to resolve complaints (HDCA, s 8(1)(a) to (c)).

[81] Mr Cocker stated that Netsafe is not an enforcement agency or a regulator and has no investigative powers.

[82] Like Ms O'Toole, he stated that Netsafe does not determine whether a digital communication is in breach of the HDCA's communication principles.

[83] In terms of the process followed after receiving a complaint, Mr Cocker confirmed that Netsafe must first assess whether the complaint falls within its scope. This requires an assessment of whether the report indicates the potential for personal harm. Verification of information may be attempted, but only via publicly available information.

[84] He outlined that Netsafe responds to a complaint in one of four possible ways:

[84.1] Advising a complainant of options they can use to help themselves.

[84.2] Contacting the on-line host to request the digital communication is removed.

[84.3] Referring the complaint to another organisation, service or agency.

[84.4] Contacting the alleged producer so that Netsafe can provide them with advice, mediate or negotiate an outcome, or persuade them to take an action in their interest.

[85] Mr Cocker emphasised the consent-led approach Netsafe adopts. He said that the consent of the complainant is sought to any of the resolution options, including what exactly can be shared with the host or producer.

[86] Mr Cocker explained Netsafe's role in the HDCA court processes in the following way:

> The Approved Agency process is therefore the gateway to the District Court proceedings under the HDCA. A complaint must first be made to Netsafe, and Netsafe be given a reasonable opportunity to assess the complaint. I am aware that the Ministry of Justice form for making an application for an order under the HDCA requires the applicant to attach a Case Summary prepared by Netsafe.

[87] Mr Cocker said that other than through its gateway function and the possibility of referral back by the Court for further attempts at mediation, Netsafe has no role in relation to the District Court HDCA proceedings.

[88] Mr Cocker explained why strict confidentiality over information received by Netsafe is seen as a fundamental component of its service. The reasons include Netsafe's reliance on the free and voluntary flow of information. He identified this as 'crucial' to the functioning of the HDCA, given Netsafe is the gateway to the District Court proceedings. His view was that disclosing information provided to Netsafe as part of a complaint may seriously inhibit other persons coming forward and using Netsafe's services. He put this point in the following way:

> Netsafe therefore considers that the contents of a complaint and any subsequent conversations with parties attract a very strong privacy interest that is unlikely to be outweighed by other interests. This must be considered in the context of the ability of the HDCA to function as intended.

Netsafe's response to the aggrieved persons

[89] As noted above, Mr Cocker confirmed that while he is not the named author on the letters Netsafe wrote to each of the aggrieved individuals, ultimately it was his decision about what was and was not provided to them. He said that while he had more involvement after the Privacy Commissioner's involvement, the April 2017 responses to the three women would not have gone out without his authorisation.

[90] Mr Cocker outlined that at the time of the Privacy Commissioner's involvement (late 2017), Netsafe contemplated release of certain information, but only if:

[90.1] The women had already been provided with it, as defendants in the HDCA process, as the risk of unwarranted disclosure of Mr Z's affairs would be reduced.

[90.2] Any concerns that people would lose confidence in the role of Netsafe as a confidential place to seek help could be abated.

[91] To manage the risk of loss of confidence in Netsafe, Netsafe sought Mr Z's consent to Netsafe's proposed release of information.

[92] Netsafe wrote to Mr Z on 18 December 2017. Mr Z was not expressly asked to consent to the proposed disclosure. Rather the letter stated Netsafe was informing him as a matter of courtesy and that the information would be disclosed on 22 December, being a timeframe that would enable Mr Z to seek legal advice before Netsafe took the step of releasing information. An electronic link to the bundle of material for release to the women was provided. Mr Cocker said the purpose of taking this step was so that Mr Z could confirm to Netsafe that what it was intending to release was material that had already been provided to the women.

[93] Following extensions sought and granted to Mr Z and then his lawyer, and confirmation on 3 January 2018 that Mr Z was not seeking to prevent the release of the information, Netsafe released a tranche of material to the three women on 15 January 2018.

[94] In closing submissions Netsafe accepted, in hindsight, that the released material could not fall within the maintenance of the law or the unwarranted disclosure of another's affairs. This was because no harm could be caused, because the women already had that documentation. In relation to liability issues, this is in effect a concession that IPP 6 was breached in relation to the tranche of material released in January 2018.

[95] Other evidence that was provided by Mr Cocker included:

> **[95.1]** An acceptance that Netsafe is subject to the Privacy Act. However he considered that the HDCA and the Privacy Act were at loggerheads with each other.
>
> **[95.2]** An emphasis on Netsafe's belief that the confidentiality settings continue after Netsafe's investigation has concluded.
>
> **[95.3]** Confirmation that Netsafe did not ask Mr Z in April 2017 whether he consented (or not) to the release of information to the three women. Rather it determined its response on the basis of Netsafe's perception of the significance of confidentiality to its organisation.
>
> **[95.4]** When Netsafe received Mr Z's complaint, it was aware that although Mr Z referenced other people, his issue was with Ms A. Netsafe processed the case and gave him the Case Summary naming Ms A only on that basis. Later in evidence Mr Cocker confirmed that Netsafe did not receive a complaint about Ms B and Ms C, but then qualified this with the explanation Netsafe does not receive complaints about people, it receives complaints about 'blocks of content.' In the relevant circumstances, it was enough for Netsafe that there was reference to the three women in the blocks of content provided by Mr Z. Therefore, by the time the Court referred matters back to Netsafe, Netsafe understood the action was between Mr Z and the three women. In this context, the responses to questions by Ms B and Ms C about whether there was a complaint against them, was implicitly on the basis:
>
> > If you had a Court ruling against you, the complaint must have come through Netsafe.

[96] In addition Mr Cocker said advice to Netsafe had been that at the point someone engages with Netsafe (by making a complaint), they have entered a mediation process and the without prejudice rules begin to apply. He considered the position was unchanged even where the complainant gives strict instructions that the making of the complaint and their identity is not to be disclosed to the author of the digital communication.

[97] He accepted that if the aggrieved individuals had access to the information Netsafe held about them, they could have had a basis to question certain facts referred to in Judge Doherty's decision. He also confirmed:

> **[97.1]** There was no evidence Netsafe's 'confidentiality script' was read to Mr Z.
>
> **[97.2]** If the women had had access to Mr Z's complaint and Netsafe's information about how it processed that complaint, they could argue with Netsafe's processes and the findings of breach set out in the Case Summary.
>
> **[97.3]** Netsafe had an unwritten policy of not telling people whether there is a complaint against them.
>
> **[97.4]** Netsafe's view was that a Judge in the District Court considering a Case Summary issued by Netsafe would not put weight on that document.
>
> **[97.5]** The fact that the District Court Judge had declined Mr Z's request for anonymity and considered that there was no evidence of any specific threat of immediate or future physical harm to Mr Z, was given no weight by Netsafe when deciding whether to release information to the three women. Mr Cocker accepted that this information was relevant to consideration of the personal information requests.

[98] On 18 April 2018 the Privacy Commissioner referred the three complaints to the Director of Human Rights Proceedings, who provided Netsafe with an opportunity to be heard before the Director made a decision on whether to institute proceedings against Netsafe. Netsafe was invited to raise any issues it considered relevant.

[99] Netsafe's explanation to the Director of Human Rights Proceedings on why proceedings should not be issued included the following:

> Consequently, in considering all requests under the Privacy Act Netsafe performs the task of assessing the privacy interests of the requestor, the HDC Act complainant, in the public interest in Netsafe maintaining confidentiality in respect of its mediation process. Netsafe considers each request on a case-by-case basis against this background.
>
> …
>
> In the present case, the Privacy Commissioner has given significant weight to the fact that the requestors have protection orders in place against Mr [Z], who made the complaint to Netsafe. In Netsafe's view, this factor should not carry significant weight in Netsafe's information access decisions. Netsafe cannot predetermine or make judgements about the merits of a HDC Act complaint, other than as provided in s8(3) of the HDC Act. The relevant information was given to Netsafe by Mr [Z] in the context of an expectation of confidentiality.
>
> …
>
> In the present case, the material that was disclosed on 16 January 2018 was that which had previously been provided to the requestors in [another] context. Netsafe accepts the privacy interests Mr Z had in the information already disclosed was reduced, so that disclosure of that

> information did not amount to the unwarranted disclosure of his affairs. However, in Netsafe's view, disclosure of information that was not previously provided would amount to the unwarranted disclosure of Mr [Z's] affairs, because the information was given to Netsafe in reliance on the confidential nature of its processes and for the purpose of resolving a HDC Act complaint.
>
> …
>
> This Rule [49 (1)(f)] therefore prohibits a District Court from ordering disclosure of information by Netsafe if civil proceedings are brought. This prima facie indicates that Parliament did not intend information held by Netsafe to be provided to other parties to civil proceedings or constitute any evidence in the proceedings.

Whether Netsafe contacted Facebook

[100] A factual issue that arose in the hearing was whether Netsafe had ever contacted the host (Facebook) to seek removal of any posts specified in Mr Z's complaint. This is relevant to the question of whether Netsafe took steps to resolve Mr Z's complaint, including how perceived confidentiality obligations were managed when doing so.

[101] There is no evidence that Netsafe contacted Facebook. Nor is there any evidence that Netsafe sought Mr Z's consent to sharing any specific information with Facebook. Any such exchanges would have been recorded in the Zendesk system. The transcript of a phone call between Netsafe and Mr Z on 16 January 2017 records that Netsafe referred Mr Z to Facebook's reporting tool, so that Mr Z could ask the platform's team to see if the postings were in breach of their terms of use and to have it/them removed. Mr Z is recorded as advising he has asked them "a million times" and "because it's so cryptic they don't see it as anything harmful."

[102] Netsafe's Zendesk system records that the Case Manager, in an email to Mr Z on 18 January 2017 on his options following its assessment of his complaint, reflected Mr Z's advice to Netsafe back to him when stating "*It appears the Facebook posts are not a breach of their Community Terms of Service and therefore Facebook will not remove the posts*."

[103] We conclude that it is very unlikely that Netsafe contacted Facebook.

FINDINGS OF FACT: LIABILITY

[104] Netsafe did not attempt to resolve Mr Z's complaint. There was no negotiation, mediation or persuasion by Netsafe in relation to this complaint. This outcome was a consequence of Mr Z not consenting to the producer being contacted and Netsafe's policy. Nor did Netsafe contact Facebook to persuade it that relevant posts should be removed.

[105] There is no evidence of a confidentiality 'script' having been read to Mr Z or available to him on Netsafe's website at the relevant time. Nor do the transcripts of telephone conversations between Netsafe and Mr Z contain any express reference to confidentiality of the complaint process.

[106] Netsafe held personal information about each of the three aggrieved individuals, but refused to release it to them. It considered releasing the information would prejudice the maintenance of the law or involve the unwarranted disclosure of the affairs of another.

[107] Netsafe did not ask Mr Z if he would consent to Netsafe releasing the information sought by the three aggrieved individuals in April 2017. It assumed he would not consent. When reconsidering matters after the Privacy Commissioner's intervention in late 2017,

Netsafe sought Mr Z's consent to the proposed release. Only after Mr Z's lawyer advised Mr Z did not oppose the release, did Netsafe release certain information to the women.

[108] Netsafe held copies of the documents Mr Z had filed in the District Court. It therefore had the ability to confirm:

> **[108.1]** What information had already been released to the women through the Court proceeding.
>
> **[108.2]** That Mr Z had provided the Court with digital communications that had not been provided to Netsafe as part of his complaint.
>
> **[108.3]** That Mr Z's affidavit contained a statement that Netsafe had determined that serious and multiple breaches under the HDCA had occurred.

[109] In making its April 2017 decision to refuse the requests, Netsafe did not appear to consider relevant factors including:

> **[109.1]** Netsafe's resolution function had not been triggered and/or was spent in relation to Mr Z's complaint.
>
> **[109.2]** Mr Z had put a dispute into the hands of the District Court, which had refused anonymity for Mr Z.
>
> **[109.3]** The women wished to access the information to enable them to respond to urgent matters before the District Court. Accordingly, right to justice considerations under the New Zealand Bill of Rights Act 1990 (NZBORA) applied in relation to the information requests by the aggrieved persons.

[110] The driving rationale for refusing to release information to the three women was a concern that doing so would undermine the confidentiality of Netsafe's processes. Netsafe considered that confidentiality considerations did not change after Netsafe had concluded its processes and a complainant elects to file proceedings in the District Court, and serves interim orders on a defendant or defendants. In addition it did not consider that where the parties were well known to each other, with a history of rancour and litigation, confidentiality considerations may change.

THE ISSUES

[111] In relation to liability, the issue is whether at the time Netsafe refused to release information (in April 2017) it had a lawful basis for doing so.

[112] The only grounds on which Netsafe could refuse access are those set out in ss 27, 28 and 29 of the Privacy Act 1993. To avoid liability, Netsafe must establish on the balance of probabilities that it had a proper basis to refuse to release the information (s 87).

THE LAW

Privacy Act 1993

[113] Principle 6 of the Privacy Act concerns access to personal information. It provides:

Principle 6

Access to Personal Information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled –

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b), an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

…

[114] The legal right of access to personal information conferred by IPP 6 is a strong right. This right is a necessary precondition to the exercise of the entitlement in IPP 7 to request the correction of personal information. In the absence of Netsafe complying with IPP 6, the women have no opportunity to apply to have their personal information corrected.

Interference with privacy

[115] Section 66 provides:

66 Interference with privacy

(1) For the purposes of this Part, an action is an interference with the privacy of an individual if, and only if,—

(a) in relation to that individual,—

(i) the action breaches an information privacy principle; or

(ii) the action breaches a code of practice issued under section 63 (which relates to public registers); or

(iia) the action breaches an information privacy principle or a code of practice as modified by an Order in Council made under section 96J; or

(iib) the provisions of an information sharing agreement approved by an Order in Council made under section 96J have not been complied with; or

(iii) the provisions of Part 10 (which relates to information matching) have not been complied with; and

(b) in the opinion of the Commissioner or, as the case may be, the Tribunal, the action—

(i) has caused, or may cause, loss, detriment, damage, or injury to that individual; or

(ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or

(iii) has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.

(2) Without limiting subsection (1), an action is an interference with the privacy of an individual if, in relation to an information privacy request made by the individual,—

(a) the action consists of a decision made under Part 4 or Part 5 in relation to the request, including—

(i) a refusal to make information available in response to the request; or

(ii) a decision by which an agency decides, in accordance with section 42 or section 43, in what manner or, in accordance with section 40, for what charge the request is to be granted; or

(iii) a decision by which an agency imposes conditions on the use, communication, or publication of information made available pursuant to the request; or

(iv) a decision by which an agency gives a notice under section 32; or

(v) a decision by which an agency extends any time limit under section 41; or

(vi) a refusal to correct personal information; and

(b) the Commissioner or, as the case may be, the Tribunal is of the opinion that there is no proper basis for that decision.

(3) If, in relation to any information privacy request, any agency fails within the time limit fixed by section 40(1) (or, where that time limit has been extended under this Act, within that time limit as so extended) to comply with paragraph (a) or paragraph (b) of section 40(1), that failure shall be deemed, for the purposes of subsection (2)(a)(i) of this section, to be a refusal to make available the information to which the request relates.

(4) Undue delay in making information available in response to an information privacy request for that information shall be deemed, for the purposes of subsection (2)(a)(i), to be a refusal to make that information available.

[116] Accordingly, in accordance with s 66(2) of the Privacy Act, an action is an interference with privacy where there is a refusal to make personal information available in response to a request and the Tribunal is satisfied that there was no proper basis for the refusal. Under this limb of s 66, it is not necessary to prove harm caused by the refusal for the purpose of establishing liability (causation remaining relevant to remedies however).

[117] Thus, the issue of whether Netsafe had interfered with the privacy interests of the three aggrieved women turns on whether it had a basis to refuse to release information. As above, in relation to the material released in January 2018, Netsafe has conceded no such basis existed. In effect liability is admitted in relation to that tranche of documents. However the further issue for the Tribunal is whether there were lawful grounds for Netsafe to withhold the additional material, namely that which is contained in the Closed Bundle provided to the Tribunal.

MAINTENANCE OF THE LAW

[118] We now address, in turn, the first of the provisions relied on by Netsafe, namely s 27(1)(c) – likely to prejudice the maintenance of the law. The relevant part of the section is:

27 Security, defence, international relations, etc

(1) An agency may refuse to disclose any information requested pursuant to principle 6 if the disclosure of the information would be likely—

…

> (c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; or
>
> …

[119] The term "likely" is to be understood as requiring the agency to show there is a real and substantial risk to the interest being protected*: Commissioner of Police v Ombudsman* [1988] 1 NZLR 385 (CA) at [391], [404] and [411] and *Nicholl v Chief Executive of the Department of Work and Income* [2003] 3 NZLR 426 at [13]. See also *Rafiq v Civil Aviation Authority of New Zealand* [2013] NZHRRT 10 (8 April 2013) at [31]. To similar effect (but in a different context) see *St Peter's College v The Crown* [2016] NZHC 925, [2016] NZAR 788 at [10].

[120] The High Court has confirmed that the maintenance of the law exception is not confined to criminal law enforcement: However the limits of this exception have not been exhaustively defined: *Geary v NZ Psychologists Board* [2012] 2 NZLR 414 at [62].

[121] This provision has been used to protect the identity of confidential informants. As stated by Rodney Hansen J in *Nicholl* v *Chief Executive of the Department of Work and Income* [2003] 3 NZLR 426 at [16]:

> The decisions are firmly grounded in the words of the statute and in the pragmatic concerns which, since *R v Hardy* (1794) 24 St Tr 199, have conferred public interest immunity on police informants. For more than two centuries it has been accepted that the public interest favours preserving the anonymity of police informers by keeping open avenues of information which will assist in the detection and investigation of crime.

[122] In the present case, the women knew who had complained against them, as this was set out in the Court documents served on them. Accordingly, the issue of release (or withholding) of an informer's name is not relevant in the present circumstances.

Submissions for Netsafe: s 27(1)(c)

[123] Netsafe relies on the *Geary* decision to support its proposition that the scope of maintenance of the law exception extends to the law in general, including the HDCA.

[124] Netsafe says that in performing its statutory alternative dispute resolution function, it relies on the free and unsolicited flow of information. It says that this free flow of information is fundamental to its maintenance of the law function. Netsafe says that releasing information gathered during an investigation or resolution process would have a significant adverse impact on Netsafe's ability to carry out its statutory functions. It says its statutory function is not frustrated where release of information occurs only where confidentiality has been waived or there is specific agreement of the complainant to the release. It denied its approach amounted to a blanket rule applied to all IPP 6 requests.

[125] Netsafe submits that the Director's proposition, that there may be a maintenance of the law argument up to the point of proceedings having been issued, fails to give any consideration to the fact that r 49 of the HDC Rules means that no party can apply for discovery in the civil proceedings from each other or from Netsafe. Netsafe says that r 49 clearly underpins the continuing expectation that the existing confidential source of the information is retained, even once the matter is before the District Court.

[126] In addition, Netsafe says s 57 of the Evidence Act 2006 supports its view of the importance of confidentiality in its complaints processes.

Submissions for the Director: s 27(1)(c)

[127] The Director submits that s 27(1)(c) does not apply where the requests for information were made after Mr Z had issued HDCA proceedings and obtained *ex parte* interim orders against the three women. He submits that their right to a fair trial was prejudiced by Netsafe refusing to release their personal information to them.

[128] The Director says that Netsafe's role probably ended after it issued the Case Summary and certainly ended once proceedings in the District Court had been filed. From this point in time the Director submits there was no ongoing need to protect any confidentiality in the HDCA complaints process. He maintains that any potential impact on prospective complainants is speculative.

[129] In relation to Netsafe's proposition that s 57 of the Evidence Act 2006 supports the withholding of information requested, the Director says there is no express carve out in PA 1993 for information within the scope of s 57 (unlike the position relating to legal professional privilege). In addition, he says that any s 57 privilege is Mr Z's, not Netsafe's. More fundamentally, the Director says there was no mediation, so therefore s 57 has no application on the facts. He does not see support in the HDC Rules relating to discovery for the approach Netsafe took in response to the three IPP 6 requests.

[130] In order to assess whether the maintenance of the law exception applies in the circumstances, it is necessary to outline relevant provisions of the HDCA and the HDC Rules.

Harmful Digital Communications Act 2015

[131] The HDCA as enacted contained many (but not all) of the policy settings proposed by the Law Commission in its 2012 Ministerial Briefing Paper *Harmful Digital Communications: The adequacy of the current sanctions and remedies*. One of the features proposed by the Law Commission and carried over into the HDCA is the informal resolution of complaints, with judicially imposed sanctions as a last resort. Another is that complaints must pass through an agency before they advance to another forum (a Tribunal under the Law Commission's proposal, the District Court as the HDCA was enacted).

[132] The purpose of the HDCA is to:

> **[132.1]** Deter, prevent and mitigate harm caused to individuals by digital communications.
>
> **[132.2]** Provide victims of harmful digital communications with a quick and efficient means of redress.

[133] The HDCA establishes ten communication principles, including those referred to in the Netsafe Case Summary set out at paragraph [28] above.

[134] As an Approved Agency, Netsafe is required to take into account the communication principles and to act consistently with the rights and freedoms contained in NZBORA (HDCA, s 6(2)). That includes the right to justice, including the observance of the principles of natural justice and right to seek judicial review (NZBORA, s 27).

[135] Section 8 of the Act sets out the Approved Agency's functions. For completeness we set this out in full:

> **Functions and powers of Approved Agency**
>
> (1) The functions of the Approved Agency are—
>
> (a) to receive and assess complaints about harm caused to individuals by digital communications:
>
> (b) to investigate complaints:
>
> (c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
>
> (d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act:
>
> (e) to provide education and advice on policies for online safety and conduct on the Internet:
>
> (f) to perform the other functions conferred on it by or under this Act, including functions prescribed by Order in Council made under section 7.
>
> (2) The Agency may, subject to any other enactment, seek and receive any information that the Agency considers will assist it in the performance of its functions.
>
> (3) The Agency may refuse to investigate, or cease investigating, any complaint if the Agency considers that—
>
> (a) the complaint is trivial, frivolous, or vexatious; or
>
> (b) the subject matter or nature of the complaint is unlikely to cause harm to any individual; or
>
> (c) the subject matter or nature of the complaint does not contravene the communication principles.
>
> (4) The Agency may decide not to take any further action on a complaint if, in the course of assessing or investigating the complaint, it appears to the Agency that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.
>
> (5) If the Agency decides not to take any further action on a complaint, it must notify the complainant of the right to apply to the District Court for an order under this Act.

[136] In broad terms, the HDCA enables informal resolution. It is Netsafe's function to facilitate such resolution. There are two further options for action under the HDCA. The first is civil action, such as that taken by Mr Z. Netsafe has no role as a party to any such civil proceeding. The second is criminal enforcement under the HDCA. This could arise via a direct complaint to Police, or a complaint to Netsafe that it would refer to Police. Other than through a referral, Netsafe also has no formal role in relation to criminal proceedings under the HDCA.

[137] Netsafe as the approved agency was required to consider requests for the personal information about complainants and authors in the ordinary way in accordance with the Privacy Act 1993. Netsafe's counsel did not argue otherwise.

[138] No person can issue proceedings in the District Court unless Netsafe has first received a complaint about the communication and had a reasonable opportunity to

assess it and decide what action to take (s 12). The Court must be satisfied of specified matters before it can grant the orders sought (s 12(2)). All parties accepted, as does the Tribunal, that s 12(2) requires that the Court must form its own view on whether the s 12 HDCA criteria are satisfied (relevantly, that there has been a breach, that the breach has caused or is likely to cause harm, the application is/is not frivolous or vexatious).

[139] There is a power under HDCA, s 14 for the Court to seek further information from Netsafe. This power can be exercised for the purpose of the Court satisfying itself that the relevant criteria specified in s 12 are met or whether to refer the matter back to Netsafe under HDCA, s 13. Netsafe must provide the requested information.

The Harmful Digital Communication Rules 2016

[140] The HDC Rules provide that as soon as possible after an application on notice is made, it must be referred to a Judge (r 16). A date and time to hear the application must be fixed, which must be as soon as possible (r 17). A defendant intending to oppose an application must file a notice of opposition (r 18). That opposition must set out the grounds of opposition and enough information to advise the Court of the facts the defendant relies upon (r 18(2)). No affidavit is required, however. This differs from the rule relating to an application by a defendant under s 20 of the HDCA to discharge an interim order. This is made by way of an interlocutory application and an affidavit in support is required (r 26).

[141] The Court can elect to determine an application on the papers (HDCA, s 16(1)), although there may also be an oral hearing. Given the purpose of mitigating harm, it is not unexpected that a prompt on the papers process is provided for under the legislation.

[142] Rule 49 lists District Court Rules that do not apply in HDCA proceedings in the District Court. One of the rules that does not apply is the rule relating to discovery in a civil proceeding.

Section 57 of the Evidence Act 2006

[143] Section 57 of the Evidence Act 2006 provides that privilege can be claimed in respect of settlement negotiations, mediation or plea discussions. Netsafe has relied on this ground to support both its s 27(1)(c) and s 29(1)(a) submissions. Section 57 relevantly provides:

> **57 Privilege for settlement negotiations, mediation, or plea discussions**
>
> (1) A person who is a party to, or a mediator in, a dispute of a kind for which relief may be given in a civil proceeding has a privilege in respect of any communication between that person and any other person who is a party to the dispute if the communication—
>
> (a) was intended to be confidential; and
>
> (b) was made in connection with an attempt to settle or mediate the dispute between the persons.
>
> (2) A person who is a party to a dispute of a kind for which relief may be given in a civil proceeding has a privilege in respect of a confidential document that the person has prepared, or caused to be prepared, in connection with an attempt to mediate the dispute or to negotiate a settlement of the dispute.
>
> …
>
> (3) This section does not apply to—
>
> …
>
> (d) the use in a proceeding of a communication or document made or prepared in connection with any settlement negotiations or mediation if the court considers that,

> in the interests of justice, the need for the communication or document to be disclosed in the proceeding outweighs the need for the privilege, taking into account the particular nature and benefit of the settlement negotiations or mediation.

[144] Netsafe submits that this section is relevant, as it is the mediator in a dispute between Mr Z and the producer/s of the digital communications provided by Mr Z. It says its mediation role is relevant to its withholding of information.

[145] However Netsafe was not involved in attempting to settle or mediate a dispute between Mr Z and the authors of the relevant social media posts. This was because Mr Z would not give permission for Netsafe to contact the women.

[146] Nor does s 57(1)(a) assist Netsafe, as it is doubtful the protection provided by this provision in the Evidence Act applies where a person has waived confidentiality, by initiating proceedings in the District Court and serving them on a respondent.

[147] For these reasons, s 57 of the Evidence Act is not a basis for refusing a personal information request in the circumstances.

Discussion: s 27(1)(c)

[148] The meaning of the phrase "to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences and the right to a fair trial" was considered in *Beattie v Official Assignee* [2021] NZHRRT 21 at [79]. For the reasons set out in that decision s 27(1)(c) is not limited in its application to criminal proceedings nor to criminal law enforcement. It applies also (as in the present case) to a statutory agency with public responsibilities.

[149] The issue is whether the maintenance of the law exception was available to Netsafe at the relevant point in time, namely after:

> **[149.1]** It had concluded its functions under the HDCA in relation to Mr Z's complaint.
>
> **[149.2]** Mr Z had issued civil proceedings in the District Court.
>
> **[149.3]** The three women had been served with interim orders issued by the District Court which named Mr Z as the person who had made a complaint to Netsafe.

[150] Netsafe says that r 49 of the HDC Rules supports its view on the maintenance of the law exception because:

> **[150.1]** The rule underpins a clear expectation of confidentiality, even once the matter is before the District Court.
>
> **[150.2]** It was clearly not intended for any material held by Netsafe to be part of the Court process.

[151] Factors the Tribunal considers weigh against Netsafe's interpretation include:

> **[151.1]** The civil procedure under the HDCA is modelled on the process for interlocutory applications and is intended to proceed at pace. The pace aspect is consistent with the purpose of the HDCA, including mitigating harm.

[151.2] There must be a real possibility that the absence of usual discovery processes is due to the model being an interlocutory application model directed at speedy decision making, rather than an indication that certain material must not be available to the Court.

[151.3] The absence of civil discovery processes supports the view that the appropriate course is to apply under the Privacy Act: *Dotcom v United States of America* [2014] NZHC 2550, at [61].

[152] In the Tribunal's view, the fact that discovery was not available in HDCA civil proceedings does not support Netsafe's view that personal information could only be released by Netsafe after Court proceedings had been issued where the complainant consented/waived confidentiality.

[153] As above, the Tribunal does not accept that the privilege articulated in s 57 of the Evidence Act is relevant. The evidence is clear that there was no attempt at a mediation between Mr Z and the alleged producer, because Mr Z prohibited any such contact. The fact that Netsafe, as an institution, considers its primary role is as mediator is not sufficient to be able to invoke this privilege in support of the proposition that the maintenance of law exception applied in the circumstances.

[154] The Tribunal considers that the proposition that Netsafe's role under the HDCA would be undermined if it released personal information without the agreement of the complainant is untenable. Such an approach undermines the case-by-case assessment of individual circumstances required under the Privacy Act 1993. Relevantly in this case, Netsafe's role under the HDCA had concluded in relation to Mr Z's complaint and two of the women had protection orders against Mr Z and all three had been served with the papers filed by Mr Z in the District Court.

[155] There is no evidence that Netsafe had delivered its confidentiality script to Mr Z, thereby creating an initial expectation of confidentiality. Mr Z had initiated District Court proceedings and had them served on the three women. Any expectation of confidentiality that Mr Z may have had prior to filing and serving his HDCA proceeding was temporary only.

[156] In the Tribunal's view, it is speculative to suggest that complainants will not avail themselves of Netsafe's services if personal information is released to requestors who are facing HDCA civil proceedings.

[157] For these reasons, the Tribunal finds that Netsafe has not established a real and substantial risk to the maintenance of the law if the requested information was released to each of the aggrieved persons in the circumstances they found themselves in.

UNWARRANTED DISCLOSURE OF THE AFFAIRS OF ANOTHER

[158] Section 29(1)(a) relevantly provides:

> **29 Other reasons for refusal of requests**
>
> (1) An agency may refuse to disclose any information requested pursuant to principle 6 if—
>
> (a) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual.

[159] This provision has two requirements. First, that the disclosure of the information would disclose the affairs of another person and second, that such disclosure would be unwarranted: *Watson v Capital and Coast District Health Board* [2015] NZHRRT 27 at [68]. As set out at paragraph [93] of the Watson decision:

> [93] As to the second requirement, it has been correctly said that particular weight needs to be given to the word "unwarranted". This, together with the use of the phrase "the affairs of another individual" rather than "privacy" appears to narrow the scope of the provision. See Taylor and Roth Access to Information (LexisNexis, Wellington, 2011) at [3.5.4]. In our view the term "unwarranted" requires the Principle 6 right of access held by the requester to be weighed against the competing interest recognised in s 29(1)(a). In that exercise consideration must be given to the context in which the information was collected and to the purpose for which the information was collected, held and used. How the balance is to be struck in a particular case and a determination made whether disclosure of the information would involve the "unwarranted disclosure" of the affairs of another individual will depend on the circumstances. See *Director of Human Rights Proceedings v Commissioner of Police* [2007] NZHRRT 22 at [63]. In that decision the Tribunal at [64] made reference to some of the considerations which may be relevant when weighing the competing interests. See also *Geary v Accident Compensation Corporation* at [78] to [88].

[160] Netsafe's letters to each of the three women in April 2017 advised that documents were being withheld under this section of the Privacy Act because, firstly, Mr Z's privacy rights outweighed their rights of access to the information and, secondly because the information requested was generated and/or obtained in confidence and "without prejudice". While recognising that exceptions to confidentiality and the without prejudice privilege exist, Netsafe concluded that "no exception appears to apply in this case. As such, it is not appropriate for the information to be released, either in part or in full."

Submissions for the Director: s 29(1)(a)

[161] The Director emphasised the importance of the legal right of access to personal information. Mr Judd submitted that none of the considerations set out in *Director of Human Rights Proceeding v Commissioner of Police* (2007) 8 HRNZ 428 applied. This was because:

[161.1] No issue of anonymity of an informer arose as Mr Z's request for anonymity had been declined by the District Court and he had willingly made his identity and fact of his complaint known to the aggrieved individuals.

[161.2] Evidence of Mr Z's discussions with Netsafe about content created by one or more of the three women would assist them in the District Court proceedings.

[161.3] The parties were all well-known to each other.

[161.4] The women had a strong interest in receiving the information, including wishing to know whether a complaint had been made against them (Ms B or Ms C) or upheld (Ms A).

Submissions for Netsafe: s 29(1)(a)

[162] Netsafe emphasises that the information it had received from Mr Z contained highly personal and highly sensitive information in which he held a strong privacy interest and which had been given to an agency that was acting as a mediator. In addition Ms Carter submitted that:

[162.1] The privilege under s 57 of the Evidence Act was an additional factor supporting Netsafe's conclusion that disclosure would amount to the unwarranted disclosure of Mr Z's affairs.

[162.2] Although Mr Z had to some extent detailed his personal information previously provided to Netsafe in his affidavit to the Court, he had not provided all such information. On this basis Netsafe submitted that Mr Z had not waived confidentiality over all information provided to Netsafe.

[162.3] Netsafe had been concerned that it would be breaching a mediation privilege.

[162.4] Natural justice considerations did not support disclosure in the circumstances, as Netsafe's processes have no bearing on the District Court proceeding under the HDCA, as the District Court looks at matters afresh. In addition, if natural justice required that Netsafe's information be provided to a defendant in HDCA proceedings, then r 49 of the HDC Rules would not have precluded discovery.

[162.5] All that the women needed in order to respond to the HDCA application was contained in the affidavit that Mr Z had filed with the Court. Specifically, both the Court and the parties should have been aware that the Case Summary had no evidential weight.

[162.6] The withheld material could not establish that the s 12 HDCA criteria were not met, and this could be the only useful purpose that the withheld material could be applied to.

Discussion

[163] It is clear from the Tribunal's inspection of the withheld documents (being the Closed Bundle documents) that the withheld information contains information about Mr Z's affairs, together with information about Ms A, Ms B and Ms C (save that Ms C is identified by her maiden name). Thus, the first criteria is satisfied.

[164] The real issue is whether or not the disclosure would be unwarranted. This turns on whether the women's IPP 6 rights of access were outweighed by Mr Z's privacy interest.

[165] Netsafe did not adduce evidence from Mr Z as to the importance to him of having his privacy protected in the circumstances. As a consequence, Netsafe is asserting Mr Z's privacy interest on his behalf without the Tribunal having the benefit of direct evidence from Mr Z of the impact of any disclosure on him. This is not a criticism of Netsafe, but is illustrative of the difficulties for an agency in effect asserting another's interest as the reason for a refusal to disclose.

[166] In assessing whether release of the information sought would be unwarranted, the Tribunal notes the following:

[166.1] Netsafe collected and held the information provided by Mr Z pursuant to its statutory function of receiving complaints about harmful digital communications. It used the information provided to prepare a Case Summary, which enabled Mr Z to apply to the District Court.

[166.2] Netsafe was not acting as a mediator, whether between Mr Z and the aggrieved persons or between Mr Z and Facebook.

[166.3] Mr Z was identified on the Court documents served on the women. There is no suggestion (nor could there be) that Mr Z was an anonymous informer.

[166.4] Mr Z's privacy interest was strongest at the point in time before Netsafe issued its Case Summary. At the point at which Mr Z initiated civil proceedings in the District Court and served the three women with the Court documents, his privacy interest was reduced by a substantial degree.

[167] In relation to the women's interest in receiving the information requested:

[167.1] Netsafe was aware that its Case Summary named one producer only, but that Mr Z had named the three women as defendants to the civil proceeding. It knew that Ms B and Ms C wanted to know whether the s 12 HDCA threshold criteria was satisfied in relation to each of them. Their only means of establishing this was by obtaining access to information Netsafe held about them.

[167.2] Netsafe knew what communications Mr Z had submitted to it and had a copy of the documents he filed in Court. Mr Z's Court documents referred to communications Mr Z had not provided to Netsafe and which had not been assessed by it. Netsafe should therefore have known that there was the potential for the Court to proceed on the basis of incorrect information. Releasing information to the women was a means by which they would be able to ensure that the Court was proceeding on the basis of accurate information.

[167.3] Mr Cocker accepted that if the women had had access to Mr Z's complaint and Netsafe's information about how it processed that complaint, they could argue with the processes Netsafe had taken and the findings relating to breach that Netsafe had made.

[167.4] The fact that discovery in the context of the civil proceeding was not an available option meant that the Privacy Act process was an appropriate process in the circumstances. Therefore the absence of a discovery regime did not mean that Netsafe's information should not be before the Court.

[168] The foundation for Netsafe's refusal was that the information was generated and/or obtained in confidence and "without prejudice".

[169] We do not consider that Netsafe has established on the evidence that it expressly conveyed to Mr Z that his complaint would be treated as confidential. Even had there been such representation, we agree with the Director's submission that by putting matters into the hands of the Court, Mr Z's expectation of confidentiality must be diminished. Persons having their rights adjudicated on by the Court cannot expect to have relevant or potentially relevant evidence kept secret from other parties to a proceeding (although in certain circumstances a court may have a discretion to make orders having such effect).

[170] For reasons explained above, the Tribunal does not accept that the without prejudice protection under s 57 of the Evidence Act is relevant, whether between Mr Z and the defendants to his civil claim or between Netsafe and those defendants.

[171] The Tribunal finds that on the facts the women's interests in receiving the information clearly outweighed the interests of Mr Z who was, in effect, wanting to maintain confidentiality over information he had himself served on the aggrieved individuals.

Conclusion on liability

[172] Netsafe has conceded that there was no basis to withhold the information ultimately provided to the women in January 2018.

[173] In relation to the information which Netsafe continues to withhold, Netsafe has not discharged its burden of proving the information withheld from the three women falls within the exceptions in ss 27(1)(c) and 29(1)(a) of PA 1993.

[174] As there has been a breach of IPP 6, there has consequently been an interference with their privacy as that term is defined in s 66(2) of the Act.

REMEDY

[175] As an interference with the privacy interests of each of the three aggrieved women has been established, the Tribunal may grant one or more of the remedies allowed by s 85 of the Privacy Act. Such remedies are discretionary.

[176] Relevantly, remedies sought by the Director are:

> **[176.1]** Declarations that Netsafe interfered with the aggrieved persons' privacy (s 85(1)(a)).
>
> **[176.2]** Damages:
>
> > **[176.2.1]** For humiliation, loss of dignity and injury to feelings, in an amount to be assessed by the Tribunal (ss 85(1)(c) and 88(1)(c)).
> >
> > **[176.2.2]** For loss of a benefit of having the information to assist with the District Court proceedings, in an amount to be assessed by the Tribunal (ss 85(1)(c) and 88(1)(b))
> >
> > **[176.2.3]** Damages for pecuniary loss, including legal costs incurred in the District Court proceedings and loss of professional and business opportunities (ss 85(1)(c) and 88(1)(a)).
>
> **[176.3]** An order directing Netsafe to make the personal information available to each of the three women.
>
> **[176.4]** Costs.

Evidence relevant to remedies

[177] In this section of our decision we set out evidence that is relevant to the remedies claimed. In light of the claim for damages for the loss of a benefit, this evidence is, of necessity, detailed.

What happened in the HDCA proceeding

[178] On 28 April 2017 the three women filed a memorandum in the District Court proceeding. In that memorandum they drew the Court's attention to the fact that only Ms A was named in Netsafe's Case Summary and that Netsafe had refused their personal information requests. As defendants they asked the Court to exercise its powers to direct Netsafe to confirm whether the complaint related only to Ms A as the producer of the communications, to provide a full copy of Netsafe's Case Summary and the reasons for concluding communications breached relevant principles (among other things).

[179] The Civil Case Manager in the District Court advised Ms A by email on 15 May 2017 that her memorandum had been considered by the Judge and advised:

> A formal application for discovery (against the plaintiff) and for non-party discovery (against Netsafe) needs to be filed with us, we endorse it and send it back to you for service.
>
> The two applications (party and non-party) can be filed as one document if you so wish.
>
> We will arrange for service on the plaintiff due to confidentiality.

Unsuccessful discovery application

[180] The three women filed an application in the District Court for party and non-party discovery on 22 May 2017. Netsafe opposed that application on the basis that the usual discovery procedures were not available in HDCA proceedings, by virtue of the HDCA Rule 49. Ms A later withdrew the formal discovery application, as she accepted the legal position as set out in Netsafe's opposition.

[181] After discussing the process of seeking discovery through the civil court process, and many other communications with Netsafe seeking to obtain further information, Ms A's evidence is:

> At no point did [legal advisor] of Netsafe or their legal Counsel Sally Carter explain that Netsafe had not in fact made findings or determinations or reach conclusions in relation to my activity, as they now claim in the Statement of Defence. It is clear from all of my communications with Netsafe referred to above that I understood they had determined and concluded that I had breached the communication principles of the HDCA and was desperate to understand what I had done wrong. They ignored my requests, and never explained or mentioned in any way what the Statement of Defence now claims: that Netsafe had not determined I had breached the HDCA.

Application to strike out Mr Z's claim

[182] On 7 August 2017 the three women applied to the District Court to strike out Mr Z's civil claim in its entirety. They say they did so without the benefit of having any of the information about the complaints made about them held by Netsafe, except for the information relating to those complaints included in Mr Z's affidavit served on them.

[183] The grounds for the strike-out of the proceeding included that the Netsafe investigation had been materially flawed, the alleged communications were not in breach of the communication principles and Mr Z's application was vexatious given that he had been refused a protection order by the District Court against Ms B and almost immediately pursued the application under the HDCA.

[184] In September 2017 their legal counsel advised the Court that the strike-out application should be determined as part of any future substantive hearing. An

interlocutory application to dismiss Mr Z's claim against Ms B and Ms C was made, on the basis of want of jurisdiction, due to the lack of evidence Netsafe had investigated them.

[185] In determining whether the claim against Ms B and Ms C should be dismissed for want of jurisdiction, the Court noted:

> **[185.1]** Mr Z's affidavit referred to his complaint to Netsafe and identified the three women as respondents.
>
> **[185.2]** The Netsafe Case Summary identified Ms A as the producer and Ms B and Ms C were not named in that document.
>
> **[185.3]** Netsafe's response to the Court, after the matter had initially been referred back to Netsafe. That response referenced a quoted comment from Mr Z that he had evidence that any contact or persuasion towards the defendants would likely cause further postings and harm.
>
> **[185.4]** The Court when issuing the interim orders found that the communications by each of the defendants constituted repeated breaches of communication principles (HDCA s 12(2)(a)).

[186] The Court concluded that against the background it appeared that Netsafe did indeed consider the complaints against Ms B and Ms C. Therefore they remained as defendants in the proceeding.

[187] Ms O'Toole accepted that Netsafe had treated the complaint as only being in relation to Ms A's communications. Ms B's and Ms C's lack of access to their personal information held by Netsafe meant they could not use any such information to support a submission to the District Court that Netsafe's file disclosed they had not been the subject of a complaint.

[188] There was information contained in the Closed Bundle which showed that:

> **[188.1]** Mr Z had clarified to Netsafe that the producer he was complaining about was Ms A.
>
> **[188.2]** There had been no 'assessment' of posts by them (because there was no evidence of any assessments, only the conclusions stated on the Case Summary).

Mr Z's lawyer's approach Ms A's place of work

[189] The substantive hearing of Mr Z's HDCA civil claim was set down for three days beginning on 29 May 2018. Settlement was being explored. An offer made was rejected by the women.

[190] Mr Z's lawyer then contacted senior personnel at Ms A's place of work and requested a meeting. That meeting occurred. After Ms A learned of this, she informed counsel acting for her (Mr Marchant) who expressed concern at this development. Mr Marchant was asked by Ms A's workplace to attend a meeting with senior staff. He did so. His strong impression of the two-hour meeting was that the workplace was putting pressure on Ms A to settle. Ms A was required to update her workplace daily on progress with settlement.

[191] Ms A was provided with a record prepared by her workplace outlining what Mr Z's lawyers had told senior members at her workplace. This included that Netsafe had determined she had breached the HDCA and that she had breached the order (among other things). When reading the note of that meeting Ms A felt she could not dispute that Netsafe had determined that she was in breach of the HDCA.

HDCA substantive proceeding is adjourned part heard

[192] The HDCA substantive hearing went ahead in May 2018 but was adjourned part heard, to a seven-day fixture in December 2018. Suppression orders were made by the Court at that time.

[193] Ms A felt her position at her place of work was impossible, and did not want to put herself or her workplace back in the same position in advance of the December 2018 hearing in the District Court. Ms A handed in her resignation. Her financial claim includes a claim for reduced income as a result of lower income in her changed employment circumstances.

Evidence relating to hurt and humiliation and injury to feelings

Impact on Ms A

[194] Ms A said that the HDCA interim orders were served on her by the Court bailiff at her place of work. She kept her place of work informed about the civil claim against her. Ms A was distressed not knowing what Mr Z had told Netsafe about her, particularly in light of past history. She said that meetings with key persons at her place of work were made more difficult because she understood that Netsafe had found against her (based on page 1 of the Case Summary) and she had no way of challenging Netsafe's findings.

[195] Ms A outlined the therapy she has undertaken as a consequence of events.

[196] Ms A also said how upsetting it was to receive the Netsafe letters and emails, in light of their tone and refusal to understand how vulnerable she was as a victim of Mr Z. She says she was stressed and anxious about Netsafe's processes and procedures which she considers allow psychological abuse to continue unabated.

[197] Mr Marchant provided evidence of the distress Ms A suffered. Mr Marchant acted for the three women in the civil proceeding issued by Mr Z. He referred to Ms A's distress at Netsafe's conclusion that she had breached the communication principles of the HDCA and the refusal to provide the information requested. His evidence included that it was traumatic for Ms A not having a way of showing key individuals at her place of work that Netsafe's assessment was flawed.

Impact on Ms B

[198] Ms B says that Netsafe's point blank refusal to provide her personal information to her made her concerned about what Mr Z told Netsafe about her. She considered Netsafe was judging her and that this was distressing.

[199] Ms B gave evidence of the distress she experienced in not being able to counter the basis of the findings set out in the Case Summary, because she did not know what the basis was. She said she felt Netsafe had no regard for the expenses of litigation on an individual.

[200] Ms B confirmed that the strain has meant that she has worked part-time only since April 2017 with a loss in income as a consequence. She has declined to be interviewed by media in relation to domestic violence issues because of being the subject of an interim order. Ms B referred to the exacerbated sense of powerlessness in the circumstances.

[201] Ms Tollemache gave evidence in respect of how Ms B has been affected by Netsafe's refusal to release information. She had no direct involvement with Netsafe, however she was Ms B's confidant during the HDCA/Netsafe processes. Ms Tollemache's evidence emphasised that:

> **[201.1]** Ms B had been starting to recover from the impact of Mr Z's actions, which had previously caused Ms B to be fearful for her life and for periods of time to be unable to work due to stress caused by Mr Z's actions.
>
> **[201.2]** Ms B was retraumatised by Netsafe's conduct.

[202] In response to questions from the Tribunal relating to the impact on Ms B of the refusal to release information, Ms Tollemache said that the lack of transparency and inability to understand what was happening and why the proceedings had been brought were "horrifying" and "devastating", while acknowledging that this impact was on top of everything else.

[203] Mr Marchant considered that Ms B was gobsmacked that the legal system would allow the information requests to be refused because doing so might be damaging to Mr Z.

Impact on Ms C

[204] Ms C's evidence was that it was difficult to explain the magnitude of emotional distress Netsafe's breach of her privacy rights has caused her. She outlined the impact of not knowing what was held on the file and the impact on her job hunting, which she put on hold. In relation to an advisory contract role, Ms C said that she suffers serious emotional and reputational damage through having to declare a conflict in relation to any HDC and/or Netsafe matters.

[205] In relation to Ms C, Mr Marchant said that at a deep visceral level she has been caused an enormous amount of stress, including because she was seeing two victims of harassment by Mr Z having to go through the process. In addition she was usually in the role of supporting victims, and was then in the position of being in breach of the law.

[206] Mr Perkins QC also gave evidence relating to the impact of Netsafe's actions on Ms C, a person he had known for some 15 years. Mr Perkins QC said it was clear to him that Ms C was upset and at times even distressed at a Court order against her based on Netsafe's Case Summary. He says it runs contrary to Ms C's understanding of and commitment to the concept of fairness that Netsafe could compile such a Case Summary without providing her any opportunity to comment on or counter what was being alleged against her. He describes the situation being seriously compounded by the refusal to provide certain information to Ms C, which left her in the dark, not knowing if there was a complaint against her or not.

Netsafe's conduct

[207] Pursuant to s 85(4), the Tribunal must take the conduct of the defendant into account when deciding what, if any, remedy to grant.

[208] The Director submits that the proceeding has highlighted Netsafe's gross misunderstanding of its duties under the Privacy Act. He says that Netsafe appeared to be in breach of other obligations under the Privacy Act (although accepting that in the circumstances those other alleged breaches are outside this Tribunal's jurisdiction). Overall, the Director submits that the defendant's conduct is not a reason to reduce damages.

[209] Counsel for Netsafe submits that Netsafe at all times acted in good faith and was attempting to execute its statutory function to the best of its abilities in an uncertain area of law.

[210] We have been satisfied by the evidence of Ms O'Toole and Mr Cocker that Netsafe withheld the relevant information out of a genuine, but misguided, concern over the performance of its statutory functions as an approved agency.

[211] The Tribunal finds nothing in Netsafe's conduct which would mitigate the impact of its interference with the privacy of the three women.

DECLARATION

[212] While the grant of a declaration under s 85(1)(a) is discretionary, the grant of such declaratory relief should not ordinarily be denied and there is a "very high threshold for exception": *Geary v New Zealand Psychologists Board* [2012] NZHC 384, [2012] 2 NZLR 414 (Kós J, Ms SL Ineson and Ms PJ Davies) at [107] and [108].

[213] On the facts we see nothing that could possibly justify the withholding of a formal declaration that Netsafe interfered with the privacy of Ms A, Ms B and Ms C.

ORDER FOR COMPLETE DISCLOSURE

[214] Next we address the need for the three women to be provided with the withheld information.

[215] Section 85(1)(d) provides that the Tribunal may order that the defendant perform any acts specified in the order with a view to remedying the interference, or redressing any loss or damage suffered by the aggrieved individual as a result of the interference, or both.

[216] In our view it is necessary and appropriate to order that Ms A, Ms B and Ms C be given access to their respective personal information held by Netsafe at the date of their information requests, excepting those documents already provided to them in January 2018. The formal orders below provide the production order is to come into effect only after the appeal period has expired.

DAMAGES

[217] In respect of all damages claimed, there must be a causal connection between the interference and the form of loss or harm claimed. In appropriate circumstances causation may be assumed or inferred: see *Winter v Jans* HC Hamilton CIV-2003-419- 854, 6 April 2004 at [33] and [34].

Humiliation and injury to feelings

[218] We turn now to the request for an award of damages under s 88(1)(c) for humiliation, loss of dignity and injury to feelings caused by the interference with the aggrieved individuals' privacy.

[219] The award of damages of this type is intended to be an appropriate response to compensate for the humiliation, loss of dignity or injury to feelings: *Hammond v Credit Union Baywide* [2015] NZHRRT 2 at [170] (*Hammond*). Its purpose is not to punish the defendant. Under the approach in *Hammond* three bands are recognised. At the less serious end of the scale awards have ranged up to $10,000. For more serious cases, awards have ranged from $10,000 to about $50,000. For the most serious category of cases, awards may be in excess of $50,000. As the Tribunal emphasised in *Hammond*, the bands are not prescriptive.

[220] The Director submits that the emotional harm suffered is significant and in the 'most serious' band in *Hammond v Credit Union Baywide* [2015] NZHRRT 6, (2015) HRNZ 66.

[221] Netsafe submits that the harm the women say that they have experienced cannot be separated from the independent finding of the District Court that there were prima facie breaches of the HDCA and the ongoing impact of the HDCA proceeding. It submits that:

> **[221.1]** The hurt and humiliation is in reality from having been found to breach the HDCA, rather than not having information to understand the finding.
>
> **[221.2]** Any re-traumatisation by Mr Z arises from the HDCA proceeding and not from the withholding of the information.

[222] In the alternative, Netsafe says any damages award would be at the lower end of the spectrum.

[223] The Tribunal accepts the evidence from the three aggrieved women that they experienced humiliation and injury to feelings caused by Netsafe's refusal to release information to them. There was a high level of anxiety and stress arising out of not knowing what Mr Z had said about them and how Netsafe had reached the conclusions set out in the Case Summary. In relation to Ms B and Ms C, Netsafe's refusal to clarify whether complaints had been made about them or to provide them with information from which they could assess that for themselves was clearly a specific cause of frustration and dismay.

[224] The evidence of the three women was supported by direct evidence of Mr Marchant, Ms Tollemache and Mr Perkins QC. No substantive challenge was made by counsel for Netsafe to their evidence about the impact on each of the three women of Netsafe's refusal to release information to them when they requested it in April 2017.

[225] It is however also clear from the evidence before the Tribunal that the injury to feelings and humiliation that the three women described to the Tribunal has mixed causes. One of those other causes is the fact that they had HDCA legal proceedings issued against them and they were subject to interim orders obtained by Mr Z before they made their IPP 6 requests. Ms A and Ms B said they experienced the HDCA civil proceeding issued by Mr Z as a new form of harassment by Mr Z.

[226] It is not possible to specify with precision the extent to which the different factors contributed respectively to the overall humiliation and injury to feelings experienced by each of the women separately. However, the Tribunal accepts there is strong evidence before it that for each of Ms A, Ms B and Ms C, Netsafe's interference with their privacy did, of itself, cause humiliation and injury to feelings to each of them. It was not the sole factor contributing to the hurt and humiliation and injury to feelings they felt, but it was a factor, which compounded distress caused by other factors. They are entitled to damages for this harm.

[227] While each of the women's expression of and reasons for their feelings differs, the Tribunal is satisfied that each of them experienced humiliation and injury to feelings to the same degree and extent. In other words, the Tribunal does not consider the impact on any one of them is higher or lower than the impact on the other/s.

[228] The Tribunal does not consider that this is a Band One matter. The impact on each of the women as a result of Netsafe's refusal to release information was clearly significant. Nor is this a Band Three matter, as there is no element of calculated attack (as in *Director of Human Rights Proceedings v Slater* [2019] NZHRRT 13) or sustained campaign to inflict harm (as in *Hammond*).

[229] The Tribunal considers that the appropriate award is in the amount of $30,000 to each of the aggrieved women.

Loss of a benefit

[230] Relevant legal principles to claims for loss of a benefit are not in dispute. These include:

> **[230.1]** The benefit claimed may be monetary, but it is not required to be so.
>
> **[230.2]** There must be a causal connection between the interference in privacy and the loss of the benefit claimed.
>
> **[230.3]** The act or omission must be a material cause to the loss or harm: *Naidu v Royal Australasian College of Surgeons* [2018] NZHRRT 23 and *Taylor v Orcan* [2015] NZHRRT 15 at [61].
>
> **[230.4]** Causation can be inferred from the nature of the breach: *Winter v Jans* HC, CIV 2003-419-854, 6 April 2004 at [33].
>
> **[230.5]** In a litigation benefit context, it is necessary for the plaintiff to establish the claimed benefit was one which they might reasonably have been expected to obtain but for the interference: s 88 PA 1993.

Loss of benefit of use in Court proceedings

[231] The Tribunal has previously accepted that a delay or a failure to provide documents intended for use in court or other legal processes, constitutes the loss of a benefit. See *Watson v Capital and Coast District Health Board* [2015] NZHRRT 27 (7 July 2015) (*Watson*) at [127] and *Director of Human Rights Proceedings v Schubach* [2015] NZHRRT 4 (19 February 2015) (*Schubach*) at [97].

[232] The Director submits that if the women had been provided their personal information, they would have been entitled to ask Netsafe to correct the information and, if such correction had been made, Netsafe would have had to change its assessment of Mr Z's complaint and the Case Summary, to record that there were no breaches of communication principles and no harm to Mr Z. In other words, the threshold for the Court's intervention would not be satisfied.

[233] The Director says that the Case Summary is the most important document in this proceeding. He put it this way:

> The reason that these aggrieved individuals have suffered all of the harm that they have suffered is that they never had a chance to fight this document. They never had a chance to get the information that sits behind this document that would have enabled them to go to the District Court and say 'Your Honour, this document is not to be relied upon'.

[234] The Director says further that if the Court had the withheld information it would have discharged the interim orders and dismissed the claim. In the alternative, the Director submits that there was a percentage chance of this occurring, such percentage possibility being sufficient to enable this Tribunal to grant a remedy.

[235] Netsafe's submission is that there is no evidential basis to support a conclusion that the information would have affected the outcome of the HDCA litigation. Ms Carter submitted:

> **[235.1]** There is no ground for strike-out of the HDCA claim against them in the withheld material, and if anything, that material put Ms B and Ms C in a worse position than having a Case Summary that does not name them.
>
> **[235.2]** It is the Court that must be satisfied that Netsafe had considered the digital communication that is before the Court and that at least two of the communications before the Court had been considered by Netsafe.
>
> **[235.3]** It is sufficient for s 12 HDCA purposes that a single communication has been considered by Netsafe.
>
> **[235.4]** The Court is the decision maker on whether the threshold under the HDCA is satisfied.
>
> **[235.5]** It is speculative and there is no evidential basis to conclude that having page 2 of the Case Summary may have influenced the Court's decision, noting that page 2 was released in January 2018 but that the proceeding was still on foot in 2019.
>
> **[235.6]** Whilst there may potentially have been the opportunity for Ms B and Ms C to use the withheld documents, it is too remote and too speculative to say it would have made a difference in relation to the actual District Court proceeding.
>
> **[235.7]** Netsafe cannot be held responsible if the District Court has made an error of law.

[236] In relation to the Director's submission that there was no basis for the findings of breach in the Case Summary, Ms Carter submits that there is no information that indicates those findings were baseless. She also submits that it is the Court that must be satisfied

of a relevant breach, and that on the available evidence the District Court carried out this assessment and reached the conclusion there was jurisdiction to issue the interim orders.

Discussion

[237] The three aggrieved persons have undeniably lost the opportunity to ask to have information Netsafe held about them corrected. However that is true of every person making an IPP 6 request and from whom information is withheld.

[238] The Tribunal considers that it is speculative and too remote to be able to conclude that Netsafe would have amended its Case Summary. Even if it had done so, there is a substantial degree of speculation about whether the interim order would have been set aside on the basis of an amended Case Summary.

[239] Even if the interim order were to be set aside, the substantive claim would remain live.

[240] Although the period in which Netsafe assessed the complaint was undeniably short, the brevity of this time period was obvious on the face of the Case Summary before the Court. The prospect of successfully arguing lack of threshold on the basis of there not having been a reasonable opportunity to assess the complaint appears remote. The other relevant criteria appear to have been satisfied (a complaint was received and Netsafe decided it could take no action).

[241] On this basis, the Tribunal considers that it is too speculative to be able to conclude that release of the withheld material would have made a difference to whether the substantive action remained on foot against Ms A.

[242] We consider the position is however different in relation to Ms B and Ms C, whose names did not appear in the Case Summary.

[243] We consider there is a credible basis to conclude that if Ms B and Ms C had access to the withheld information and been able to put that before the Court in support of their interlocutory application, the Court may have accepted that Mr Z was not complaining about content they had produced. The Court would then be likely to conclude that they were not the appropriate individuals or other persons who should be subject to an order, being a requirement of HDCA, s 19(5)(k). We say this because:

> **[243.1]** Netsafe's position at the hearing was that it had in fact treated Mr Z's complaint as confined to Ms A (which is why only Ms A was listed on the Case Summary) and it had not proceeded on the basis there were complaints against communications produced by Ms B and Ms C.
>
> **[243.2]** Netsafe's position at the hearing is consistent with the documentary record. While there is evidence in the documents that Mr Z identified all three women in his complaint, when required to specify the relevant producer/s, he expressly confined this to Ms A. It is difficult to conclude that this information could not have materially influenced the outcome of Ms B's and C's strike-out application.

[244] Finally, we note Ms A's evidence that she lost the benefit of having page 2 of the Case Summary when interacting with both the Court and senior personnel at her place of work. We do not consider that the delay in releasing the full copy of the Case Summary has materially caused the loss of a benefit as:

[244.1] The language of identified breaches on page 1 is unequivocal and forceful. The Tribunal agrees that the language used in the Case Summary indicates that Netsafe has in fact concluded that there were breaches of the communication principles under the HDCA and that harm had resulted. In this context, the language on page 2 could not reasonably be interpreted as contradicting the express language of breach on page 1 of the document.

[244.2] In any event, the May 2018 meetings Mr Marchant and Ms A referred to occurred four months after Netsafe released the full copy of the Case Summary to Ms A. Information on page 2 of this document was therefore available to Ms A from that date and able to be deployed by her in discussions with those senior persons at her place of work.

[244.3] We accept Netsafe's submission that the fact the full copy of the Case Summary was released in January 2018 but the HDCA proceedings remained on foot in January 2019 indicates that page 2 of the document was not a magic bullet in being able to dispose of Mr Z's HDCA claim.

[245] On the facts we are satisfied that Ms B and Ms C have lost the benefit of use of documents in the HDCA proceedings, namely in support of their interlocutory application to have Mr Z's proceeding against them dismissed on the basis there had not been a complaint to Netsafe about their digital communications. However those same documents would not assist Ms A in the same way, because Mr Z was clearly complaining about her communications.

[246] Netsafe's interference with Ms B's and Ms C's privacy is a contributing and material factor to the loss of their respective benefit of using information in their strike-out application in the District Court proceedings. They are entitled to compensation for their loss.

[247] Damages for loss of a benefit cannot be an exact calculation, but they are intended to be a meaningful recognition of the benefit that has been lost. In both *Watson* and *Schubach*, awards of $5,000 for the loss of benefit were awarded. The Tribunal accepts that in this claim the interference with Ms B and Ms C's privacy was material in their loss of benefit. The Tribunal considers an award of $5,000 is appropriate.

Damages for pecuniary loss and expenses incurred

[248] The financial claims for pecuniary loss and expenses are in the following terms:

[248.1] Ms A: Share of costs of defending the District Court claim in the amount of $30,205.25 (excluding pre-judgment interest) and cost to her of lost professional opportunities. The basis of this latter financial claim is her resignation from her then (2018) professional role and reduced earnings in her subsequent role.

[248.2] Ms B: Share of costs of defending the District Court claim in the amount of $28,370.25 (excluding pre-judgment interest).

[248.3] Ms C: Share of costs of defending the District Court claim in the amount of $28,370.25 (excluding pre-judgment interest).

Costs of defending the HDCA proceeding

[249] There is no dispute as to the quantum of the legal costs incurred by the three women in defending Mr Z's HDCA civil proceeding.

[250] The Tribunal accepts Netsafe's submission that at least part of these costs would have been incurred irrespective of Netsafe's response to the three personal information requests. This is due to Mr Z having received the Case Summary and being entitled to issue proceedings in the District Court. Legal costs would inevitably arise in relation to defending the substantive claim.

[251] No evidence was before the Tribunal as to how legal costs incurred might be attributed to either defending the substantive claim, on one hand, or costs that might have been able to be avoided by each of the women if Netsafe had released all information to the women, on the other. It is therefore difficult to agree that the Director has discharged the onus of proving financial loss caused by the interferences with privacy for this head of claim.

[252] There is a further complication. This arises because of the settlement of the civil proceedings initiated by Mr Z. As noted above, Mr Z's HDCA proceeding was discontinued in early 2020, after the parties had reached agreement on settlement terms. The memorandum filed in the District Court, provided to the Tribunal by the Director, records that there was no issue as to costs in relation to the discontinuance of the District Court proceeding.

[253] Counsel for Netsafe submits that settlement of the HDCA claim on the basis costs lie where they fall in the District Court suggests that it would be inappropriate for the Director to seek recovery of those costs as a damages claim in this proceeding. Ms Carter submits that because the aggrieved women had the opportunity to seek costs from Mr Z but did not do so as part of a negotiated outcome, these costs cannot be claimed in this forum.

[254] In response the Director agrees that these legal costs could not be claimed in this proceeding if the negotiated settlement of the civil claim included that Mr Z had agreed to pay costs to the defendants. However he submits that the fact that costs lie where they fall in the civil claim does not preclude recovery in this forum.

[255] Mr Judd submits that the costs of defending the District Court proceedings would not have been incurred, or incurred to the same extent, had there been no interference with privacy.

[256] As the Tribunal has noted above, there is no evidence on what proportion of the costs would not have been incurred to the same extent. In this context, the Tribunal does not need to decide the issue of whether costs can be claimed in this proceeding in relation to legal costs arising from proceedings ultimately settled on the basis costs lie where they fall.

[257] Due to the absence of relevant evidence before the Tribunal, we decline to make an award of damages for compensation for legal costs incurred.

Damages for loss of professional and business opportunities

[258] This head of claim is relevant to Ms A and Ms B. The claim in relation to Ms A relates to the difference in income projections based on the role she was in before resigning in 2019 and for the three years after she become self-employed.

[259] The claim in relation to Ms B is for $40,000 loss of income due to the public and professional limbo she finds herself in. This claim was not strongly pursued by the Director. However for completeness we determine this claim.

[260] These claims are in substance loss of a chance claims.

Ms A's money claim

[261] The evidence includes Ms A's anticipated annual income for three years (2020-2023) at her former place of work, estimates of future income in her self-employed role following her resignation, and the difference between them.

[262] The Director accepts that this claim is a loss of a chance claim, with suggested outcomes being uncertain. Mr Judd says that this loss of a chance claim is then to be reduced to whatever is available after the Tribunal's calculation of other damages and further reduction to the Tribunal's financial limit.

[263] Ms A's evidence relating to the circumstances in which she felt resignation was her best option means that there is difficulty in establishing the requisite causation link between the interference in privacy and this head of claim.

[264] Ms A's decision to resign is clearly linked by her to the fact of Mr Z's lawyers seeking and obtaining a private audience with senior personnel at her (then) place of work in May 2018, and subsequent pressure by her employer to settle the HDCA claim. The three-day 29 May 2018 substantive hearing had been adjourned part heard to December 2018. Ms A was concerned that pressure would continue in that context. The Tribunal finds these were substantive and material considerations in Ms A's resignation decision.

[265] Counsel for Netsafe points to Ms A's evidence where she says that she would not have left her place of work at that time "*were it not for the HDCA proceeding*" and the fact that Mr Z's proceeding would have occurred regardless of any interference with her privacy.

[266] We agree with Ms Carter's submission that, due to these factors, the Tribunal cannot be satisfied that Netsafe's actions were the cause of loss of future income, relative to income from Ms A's new role. Rather this was a consequence of Mr Z's actions, the actions of lawyers acting on his behalf and pressure put on Ms A by those at her place of work.

Ms B's money claim

[267] The Director refers to Ms B's unchallenged evidence that she has suffered financial loss of at least $40,000 in the financial year to April 2019, and feeling unable to undertake domestic violence awareness work that she would otherwise have undertaken.

[268] Netsafe argues that the outcomes Ms B refers to are a result of the HDCA proceeding itself, rather than Netsafe's actions.

[269] The Tribunal agrees that there is insufficient evidence to establish that Netsafe's actions are the material causes of the damages claimed.

Interest claimed

[270] Finally the Tribunal notes that the Director sought interest on the awards of damages. However the Tribunal has no jurisdiction to award interest.

Continued suppression

[271] As noted above, permanent suppression orders relating to the identity of the aggrieved persons are required so as to comply with orders made by the District Court. Personal details of the aggrieved persons have in fact been anonymised in this decision.

[272] However, the unredacted decision of the Tribunal does contain some (albeit minimal) reference to evidence received in the course of the closed hearing from which the three aggrieved individuals and the public were excluded. These references are highlighted in yellow as is evidence which might otherwise justify withholding. The Director and Netsafe need to be heard on the question whether those references should be removed from the redacted version of the Tribunal's decision. To that end:

> **[272.1]** The day prior to the unredacted decision being released to counsel notice is to be given to counsel that the decision is to be so released.
>
> **[272.2]** The release will be to counsel only. The submissions regarding any redaction sought are to be filed and served by 4pm on the third day following release of the unredacted decision to counsel. Counsel are to confer in the hope a joint memorandum can be filed. Otherwise separate memoranda are to be filed and exchanged.
>
> **[272.3]** The Tribunal will thereafter publish a redacted decision. Only that decision can be released to the aggrieved individuals and the public at large and published on the Tribunal's web page and on NZLii.

FORMAL ORDERS

[273] The Tribunal is satisfied on the balance of probabilities that the actions of Netsafe were interferences with the privacy of [redacted] (Ms A), [redacted] (Ms B) and [redacted] (Ms C) and makes the following orders:

> **[273.1]** A declaration is made under s 85(1)(a) of the Privacy Act 1993 that Netsafe interfered with [redacted] (Ms A's), [redacted] (Ms B's) and [redacted] (Ms C's) privacy by failing to provide information held by Netsafe as required.
>
> **[273.2]** An order is made under s 85(1)(d) of the Privacy Act 1993 that Netsafe provide each of [redacted] (Ms A), [redacted] (Ms B) and [redacted] (Ms C) with a full and complete copy of all the documents contained in the Closed Bundle of documents in this hearing within 20 working days of the expiration of the appeal period.

[273.3] Netsafe is to pay each of [redacted] (Ms B) and [redacted] (Ms C) damages of $5,000 for the loss of a benefit under s 85(1)(b) of the Privacy Act 1993.

[273.4] Netsafe is to pay each of [redacted] (Ms A), [redacted] (Ms B) and [redacted] (Ms C) damages of $30,000 for humiliation and injury to feelings under s 85(1)(c) of the Privacy Act 1993.

[273.5] Pursuant to s 107(3)(b) of the Human Rights Act 1993 the Tribunal makes permanent orders:

[273.5.1] Publication of the names, address, occupation and any other details which might lead to the identification of [redacted] is prohibited.

[273.5.2] There is to be no search of the Tribunal file without leave of the Tribunal or of the Chairperson.

[274] The Director has sought costs, and suggested this issue be determined on the papers if the parties are not able to reach agreement. The Tribunal reserves the question of costs for separate consideration.

[275] If the parties cannot reach agreement on the question of costs, the following procedure is to apply:

[275.1] The Director is to file submissions within 14 days after the date of the decision.

[275.2] The submissions for Netsafe are to be filed within 14 days with a right of reply to the Director within seven days after that.

[276] The Tribunal will then determine the issue of costs based on the written submissions without any further oral hearing.

[277] In case it should prove necessary, we leave it to the Chairperson or the Deputy Chairperson to vary the foregoing timetable.

.....	.....	.....	.....
Mr RPG Haines ONZM QC **Chairperson**	**Ms K Anderson** **Deputy Chairperson**	**Ms WV Gilchrist** **Member**	**Ms ST Scott QSM** **Member**