IN THE HUMAN RIGHTS REVIEW TRIBUNAL **[2014] NZHRRT 48**

	Reference No. HRRT 020/2012
UNDER	**THE PRIVACY ACT 1993**
BETWEEN	**KELLY ARMFIELD**
	PLAINTIFF
AND	**BRADLEY NAUGHTON**
	DEFENDANT

AT NEW PLYMOUTH

BEFORE:
Mr RPG Haines QC, Chairperson
Mr GJ Cook JP, Member
Mr BK Neeson, Member

REPRESENTATION:
Ms T Corbett and Mr L Hansen for Plaintiff (7 and 8 February 2013)
Mr L Hansen for Plaintiff (15 April 2013)
Mr B Naughton in person
Ms K Evans for Privacy Commissioner

DATE OF HEARING: 7 and 8 February 2013; 15 April 2013

DATE OF DECISION: 6 October 2014

DECISION OF TRIBUNAL

[1] Mr Naughton and his wife operate a small Bed and Breakfast business at their home, 16 Havelock Place, Blagdon, New Plymouth. The house is situated in a quiet residential suburb down a cul-de-sac. On their northern boundary is 18 Havelock Place occupied by Mr Armfield, his partner Ms Halls and their three children, the eldest of whom was three years of age at the time.

[2] Although initially on good terms, Mr Naughton and Mr Armfield had a falling out. This resulted in Mr Naughton installing a surveillance system in the form of eight cameras monitored from the television screen situated in the lounge of the Bed and Breakfast. Three of the surveillance cameras were installed down the side of the Bed and Breakfast adjoining the Armfield residence and were pointed in the direction of Mr Armfield's home.

[3] Mr Armfield and his wife believed that the cameras were surveilling and recording their and their children's activities in the privacy of their home or at least in what they believe should be the privacy of their own home. They held concerns about Mr Naughton's motivation and the use to which the collected information was to be put. When they asked Mr Naughton for access to their personal information held by Mr Naughton, he refused. These proceedings followed. The primary issue for determination by the Tribunal is whether Mr Naughton complied with his obligations under Information Privacy Principles 1 to 4 and 6. We acknowledge with gratitude the substantial assistance given to the parties and to the Tribunal by the submissions presented on behalf of the Privacy Commissioner.

THE EVIDENCE

The view

[4] Immediately after the hearing commenced on 7 February 2013 the Tribunal held a "view" at 16 and 18 Havelock Place in the presence of the parties. Mr Naughton did not, however, allow Mr Armfield to enter 16 Havelock Place on the grounds that a trespass notice served by Mr Naughton on Mr Armfield on 21 April 2012 was still in force. Ms Halls was permitted entry. The information obtained during the view aided an understanding of the evidence later given by the parties. It also allowed the Tribunal to see the surveillance system in operation and in particular to sight the images displayed on the monitor situated in the lounge of the Bed and Breakfast. For the first time it emerged that the field of vision of two of the cameras in question had been partially masked.

[5] Although possibly unnecessary to do so, we record that information obtained at a view may be used as though that information had been given in evidence. See s 82 of the Evidence Act 2006, s 106(4) of the Human Rights Act 1993 and s 89 of the Privacy Act 1993 (PA).

Neighbours in dispute

[6] Mr Naughton and his wife moved into 16 Havelock Place in about September or October 2010. Mr Armfield and his partner did not oppose the address being converted into a Bed and Breakfast business. Initially Mr Armfield, a practical man who maintains his home and its grounds to a very high standard, assisted Mr Naughton with tasks Mr Naughton would otherwise have found difficult, such as pruning trees and making and laying concrete. The reasons why this relationship changed for the worse are not directly material. It is sufficient to note only that Mr Naughton attributes to Mr Armfield responsibility for such things as mud appearing on the washing hung on the back lawn of the Bed and Breakfast (which adjoins a reserve) and the slashing of tyres of motor vehicles parked in the street, including those belonging to clients of the Bed and Breakfast. It must be added that Mr Armfield vigorously denies responsibility for these alleged incidents and the Tribunal emphasises that there is no evidence whatsoever before it to support the claims made by Mr Naughton.

[7] Mr Naughton says he has always got on well with Ms Halls.

31 March 2012 – installation of the cameras

[8] Without notice to or consultation with Mr Armfield or Ms Halls, Mr Naughton on 31 March 2012 affixed three surveillance cameras to the side of the Bed and Breakfast which adjoins and runs parallel to the common boundary with 18 Havelock Place. In this decision the cameras will be described as follows.

> **[8.1]** Camera 1. This camera is located on the front corner of the Bed and Breakfast, that is, it is closest to the road frontage and surveils part of the front lawn of the Armfield property as well as part of the footpath in front of both the Bed and Breakfast and the Armfield property.
>
> **[8.2]** Camera 2. This camera is half way down the side of the Bed and Breakfast and, as initially installed, looked out over the front of the Armfield property seemingly directly into their lounge which has large windows. Mr Naughton has claimed at times that the intended purpose of the camera was to provide a view of Mt Taranaki which is beyond the Armfield home and potentially within the field of view of Camera 2, depending on the angle at which it is set. He added it was contemplated that the view provided by this camera would be streamed live to the Bed and Breakfast website to provide a real-time picture of the mountain. In that case it would also provide a live view of the front of the Armfield property and of their lounge.
>
> **[8.3]** Camera 3. This camera is situated at the back corner of the Bed and Breakfast and looks down the common boundary line towards the road frontage.

[9] The remaining five cameras are installed at the back of the Bed and Breakfast (Camera 4), along the side of the Bed and Breakfast which adjoins 14 Havelock Place (Cameras 5 and 6) and at the front of the Bed and Breakfast (Cameras 7 and 8). These five cameras are not material to the case and will not be referred to.

Impact of Cameras 1, 2 and 3 on the Armfield property

[10] The Armfield house is set well back from the street frontage. The front of the property comprises a large, open grassed area and at the front corner adjoining the Bed and Breakfast property is a swing used by the Armfield children. On the same side of the Armfield property but closer to their house is an outdoor table with seating. Further up the fence line, opening from the side of the Armfield home is a spacious and well-laid out outdoor living and entertainment area comprising a spa pool, a play area for the children, a barbecue and seating. The two properties are divided by a fence which is about one metre plus in height. The three cameras sit well above the fence line and allow an almost unobstructed view into the entire front, side and rear sections of the Armfield property.

[11] The 31 March 2012 installation of the cameras at three strategic points overlooking their home gave Mr Armfield and Ms Halls the clear impression that their most private if not cherished living spaces together with their children's play area were now being watched and filmed by a neighbour who had not spoken to them about what he was doing and who seemed unconcerned if not pleased at their reaction to his actions.

The request for access to personal information

[12] On observing the installation of the cameras Mr Armfield and Ms Halls on 31 March 2012 approached Mr Naughton and asked why he was pointing the cameras into their property. He replied that "the cameras are pointing across your property at the mountain [Mt Taranaki]". When Ms Halls, sceptical of this claim, asked to see the footage being collected Mr Naughton responded "No, not without a search warrant". Mr Armfield and Ms Halls then asked Mr Naughton to redirect his cameras off their property. Mr Naughton refused.

Letter from Taranaki Community Law dated 13 April 2012

[13] By letter dated 13 April 2012 Ms Corbett, a solicitor at Taranaki Community Law, wrote to Mr Naughton on behalf of Mr Armfield and Ms Halls. Her letter advised:

> **[13.1]** Mr Armfield and Ms Halls believed the cameras were collecting information from their property and from inside their home without lawful purpose in breach of the Privacy Act.
>
> **[13.2]** Mr Naughton had refused their request to see the information unless they obtained a search warrant. This was not an appropriate response to a request for access to personal information.

[14] Through Ms Corbett, Mr Armfield and Ms Halls proposed that Mr Naughton:

> **[14.1]** Cease collecting information about them and their family.
>
> **[14.2]** Cease collecting information from any part of their property.
>
> **[14.3]** Delete any information collected about them, their family and property.
>
> **[14.4]** Move the cameras to a position where they could not collect personal information from the Armfield property.

[15] Mr Naughton was asked to respond by 18 April 2012. Mr Naughton received the letter but did not reply to it or respond in any way.

The redirection of the cameras and the trespass notice

[16] On 21 April 2012, while standing on his own property, Mr Armfield redirected two of the cameras away from his home by using a long pole.

[17] At approximately 10pm that evening (21 April 2012) Mr Naughton arrived at their door and banged loudly, waking the young children and causing concern to Mr Armfield and Ms Halls. On Mr Armfield opening the door Mr Naughton served a trespass notice, claiming Mr Armfield had been on the Bed and Breakfast property without consent.

[18] On 22 April 2012, while Mr Armfield and Ms Halls were entertaining guests in their outdoor entertainment area, Mr Naughton ostentatiously mounted a ladder and redirected both cameras back to face the Armfield property. Camera 2, which had previously pointed into the Armfield lounge window, now appeared to be pointed directly onto the deck area where the spa pool is located together with the children's playground and entertainment area. Camera 3, located at the rear of the property, was redirected to point across the boundary fence and on to the front of the Armfield property. In his evidence Mr Armfield detailed subsequent adjustments made by Mr Naughton to the

positioning of the cameras but we do not consider it necessary to go into this level of detail.

The complaint to the Privacy Commissioner and the further attempt by Mr Armfield to reach an amicable solution

[19] A few days earlier, on 19 April 2012, Mr Armfield had lodged a complaint with the Privacy Commissioner but the Commissioner was ultimately unable to resolve what was perceived as a conflict of evidence. The investigation was discontinued in July 2012, the Commissioner suggesting that the appropriate forum for the resolution of the case being the Tribunal.

[20] By letter dated 17 August 2012 Ms Corbett wrote again to Mr Naughton recording that despite repeated requests the surveillance cameras continued to point into the Armfield property in such a way as to breach the privacy of the family and of their guests. Once again Mr Naughton was asked to cease and desist and to permanently move all cameras to a position where they could not collect personal information from the Armfield property. Once again Mr Naughton studiously ignored the letter and made no response. The present proceedings were then filed on 3 September 2012.

[21] It is to be noted that in neither of the letters sent by Ms Corbett was Mr Naughton asked to remove the cameras. The request was only that they be repositioned to avoid collecting personal information from the Armfield property.

Mr Naughton's evidence

[22] At a teleconference convened by the Chairperson on 17 October 2012 case management directions were given to ensure (inter alia) that written statements of the evidence to be given by the parties were filed and exchanged well before the hearing. Those directions were confirmed by the Chairperson's *Minute* issued on the same date. Mr Naughton was directed to file and serve his written statement of evidence by 7 December 2012. That statement was not received by the Tribunal until 11 January 2013, less than a month before the hearing. Unbeknown to the Tribunal the statement had not been served on Mr Armfield or his lawyers. The first Mr Armfield and Ms Halls became aware of the existence of the statement was when it was read out by Mr Naughton while giving evidence on the second day of the hearing (8 February 2013).

[23] Regrettably, most of Mr Naughton's evidence was a sustained and at times vindictive attack on Mr Armfield's character. There is no evidence whatever to justify the hurtful and at times extravagant allegations made by Mr Naughton. What emerged is that Mr Naughton is seemingly preoccupied with Mr Armfield and incapable of being objective (even to the slightest degree) about a crisis which he himself has largely brought about.

[24] We do not intend setting out Mr Naughton's evidence in full. We note only the main points of the admissible evidence, that is evidence which was not wilful allegation, innuendo and suspicion:

> **[24.1]** Mr Naughton holds the subjective belief that Mr Armfield is responsible for "events" in the Havelock Place neighbourhood.
>
> **[24.2]** Mr Naughton chose to install the cameras on 31 March 2012 because Mr Armfield was then at home and "he would know from day one that I had the cameras". At no time did Mr Naughton mention to Mr Armfield or Ms Halls or discuss with them his intended installation of the surveillance system.

[24.3] When Mr Armfield and Ms Halls asked to see what information was being collected Mr Naughton refused the request because at that time he had only hung the cameras and while this could not be seen by an external observer, they were not then wired to the hard drive and monitor. He did not want Mr Armfield and Ms Halls to know that the cameras were not then in operation. Cameras 1 and 3 only went "live" a few days or a week later while Camera 2 went live in May 2012.

[24.4] Mr Naughton studied the Privacy Act and the Privacy Commissioner's *CCTV Guidelines* prior to purchasing the surveillance system.

[24.5] The surveillance software allows the field of vision of each camera to be masked or cropped so that not everything in that field of vision can be seen live on the monitor or recorded on the hard drive. Camera 3 (at the rear of the Bed and Breakfast) was at some indeterminate point partly masked to obscure the view of the Armfield outdoor living area which would otherwise have been monitored. Camera 2, which at some stage was pointed to face Camera 3, was also masked for the same reason. Mr Naughton accepts that without such masking the two cameras would provide a good view of the Armfield house and outdoor living area. Camera 1 (pointed across the Armfield front lawn), on the other hand provides a good view of the swing used by the Armfield children. It is not and never has been masked. He is aware the Armfield children play on the swing and the field of view of Camera 1 means that their activities are both monitored and recorded. He accepts that any adult person or child within the field of view of the camera will be easily identifiable.

[24.6] All cameras have infra-red night vision. There is reflection and refraction from the white walls of the Bed and Breakfast with the result that the cameras must be pointed away from the walls. This may give the appearance of the cameras being focused unnecessarily on the Armfield premises. While aware of the Privacy Commissioner's *CCTV Guidelines* and the need to minimise any intrusion, he still had to ensure that the cameras were effective in protecting him and his clients.

[24.7] The hard drive of the surveillance system stores ten days of information. To log into the hard drive one needs a user name and password but the system can be set so that neither is required. The monitor is the large flat television screen located in the lounge of the Bed and Breakfast. The lounge and the television are used by guests. They would be able to see the surveillance images if the surveillance system was accessed in their presence. It was unclear whether access to the system has at all times being protected by a password.

[24.8] When the masking of the field of view of Cameras 2 and 3 was discovered by the Tribunal during the "view" and Mr Naughton asked why he had not made mention of masking in any of the documents filed by him, Mr Naughton said that he "didn't feel [he] needed to explain how the system was set up". He accepted that he was possibly doing himself a disservice but "didn't think of it". He accepted, however, that without the masking of Cameras 2 and 3, the intrusion on the Armfield property would be unreasonable.

[24.9] Mr Naughton accepts that when asked on 31 March 2012 to allow Mr Armfield and Ms Halls to see what the cameras were recording, he had answered "No, not without a search warrant". He accepts that this response was a refusal of access. He claims he was not obliged to give a reason for his refusal as there

was nothing to see. At the time he was angry, did not give much thought to the request and said the first thing that came to his mind.

[24.10] Mr Naughton said that he did not respond to Ms Corbett's letter dated 13 April 2012 as he didn't believe there was any reason to and that it would not have been "helpful" to respond. He elaborated on this by saying that he believed he would be required to remove the cameras and that this "wasn't going to happen". When it was pointed out that the letter did not ask him to remove the cameras Mr Naughton said he believed that nothing but removal would satisfy Mr Armfield. He acknowledged, however, that it was open to him to contact Ms Corbett but he had not taken this step. He stressed that in his opinion there is no obligation to respond to a request for access to information if the request is "false". For similar reason he had not responded to Ms Corbett's later letter dated 17 August 2012.

[24.11] Although he had issued a trespass notice against Mr Armfield, Ms Halls was "always welcome" to see anything and had needed only to ask. That "[had] always been the case". It should be observed, however, that Mr Naughton never communicated this to Ms Halls and the Tribunal notes that on 31 March 2012 it had been Ms Halls who asked to view the information collected by the cameras.

Credibility assessment

[25] To a substantial degree the broad outline of events is not in dispute, particularly the events of 31 March 2012 when the cameras were installed and the request for access to personal information made and denied. It is also accepted by Mr Naughton that he elected to ignore the two letters from Ms Corbett which asked not for the removal of the cameras, but for their redirection.

[26] In our view Mr Armfield and Ms Halls were both credible witnesses and in the event of any conflict between them and Mr Naughton, we prefer their evidence to his. It is they who have acted rationally from the time the cameras were first installed. Their written requests to Mr Naughton have been couched in reasonable and moderate language and we have no reason not to accept them both as honest and reliable witnesses.

[27] Mr Naughton, on the other hand is in a different category. Our assessment of his credibility has been affected by his determination to ensure that right or wrong, he remains free to operate his surveillance system not as the law requires, but as he wishes. He claims to have studied the Privacy Act and the *CCTV Guidelines* but if he has, it appears little has been understood or learnt. For example, the three cameras in question were installed without notice to Mr Armfield and Ms Halls. Indeed, Mr Naughton chose to install them in a confrontational manner. When asked what information was being collected, he could have replied that the system was not then in operation. Instead he chose to give an aggressive answer which suggested personal information was indeed being collected. In spite of claiming to have no axe to grind with Ms Halls, he never invited her to see for herself what the cameras were recording. He chose to ignore the reasonable proposals put forward by Mr Armfield and Ms Halls through their solicitor. He chose to interpret the letters, quite unreasonably, as a request to take the cameras down when no such request was made. His taking out of a trespass notice and his decision to serve it at 10pm at night was uncalled for and again, confrontational. His written statement of evidence read to the Tribunal was littered with provocative statements and gratuitous insults.

[28] We conclude he is a man of poor judgment and that he cannot be relied on to give balanced and objective evidence. We therefore have substantial reservations as to the

degree to which we can rely on his testimony. This assessment has relevance when we come to address the question of remedies.

THE LEGAL ISSUES

Legal issues confined to the Privacy Act

[29] The legal issues in the present case must be determined within the four corners of the Privacy Act. The jurisdiction of the Tribunal is statute-based and limited by Part 8 of the Act to the grant of a remedy if, and only if, Mr Armfield establishes an interference with his privacy as defined by s 66 of the Act. It is the not the function of the Tribunal to determine whether Mr Naughton committed the tort of invasion of privacy (*Hosking v Runting* [2005] 1 NZLR 1 (CA)) or breached Mr Armfield's right to security against unreasonable search and seizure (s 21 New Zealand Bill of Rights Act 1990 and *R v Williams* [2007] 3 NZLR 207 (CA)) or committed the tort of intrusion upon seclusion (*C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672 and *Faesenkloet v Jenkin* [2014] NZHC 1637). Nor is this decision concerned with targeted surveillance by law enforcement and regulatory agencies (Search and Surveillance Act 2012).

[30] Furthermore the Tribunal is not required to address the "domestic affairs" exemption in s 56 of the Privacy Act. Mr Naughton made it clear that the surveillance system was installed to protect his Bed and Breakfast business and clients from a perceived "threat". He said that the cameras also assisted dealing with issues which arise from time to time with his Bed and Breakfast clients.

Surveillance and the Privacy Act

[31] As noted by the New Zealand Law Commission in its Report *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC R113, January 2010) at [2.3] to [2.5], surveillance is becoming more pervasive in everyday life and technologies of surveillance are developing apace. Many uses are beneficial to individuals and society. In particular, surveillance is used in a wide range of contexts: state security and intelligence; law enforcement and regulation; environmental and road traffic regulation; personal and public safety and security; commercial; domestic; research; media; work place; and private investigation.

[32] At the same time the Report notes that it is important to recognise that surveillance can have significant negative effects, including the use of information obtained through surveillance for criminal purposes such as identity theft, blackmail, fraud or burglary; a chilling effect on the exercise of civil liberties; loss of anonymity; stress and emotional harm; the creation of a record of personal information which can be stored permanently, disseminated widely, analysed in great detail, and taken out of context; excessive collection of personal information; insecurity and loss of trust; use for voyeuristic or other questionable purposes; discrimination and misidentification; and desensitisation to surveillance, leading to a narrowing of people's reasonable expectations of privacy. We add that it has even been reported that security camera footage from inside homes, offices and shops across the United Kingdom is being intercepted and broadcast live on the internet without the owners' knowledge.

[33] The Law Commission Report further notes at [4.10] that surveillance by cameras, sometimes referred to as closed-circuit television (CCTV) has become one of the most widely used forms of mass surveillance and its use continues to grow both overseas and in New Zealand:

4.10 CCTV looms large in any discussion of surveillance, and with good reason. It has become one of the most widely-used forms of mass surveillance, and its use continues to grow both overseas and in New Zealand. Even in the period since we released our issues paper, several cities and towns in New Zealand have introduced CCTV systems or expanded their existing systems. CCTV is also widely used by businesses in New Zealand to protect the security of their property and employees. There is a widespread belief that CCTV makes communities safer, although the evidence of CCTV's effectiveness in deterring (as opposed to detecting and prosecuting) crime is not particularly strong. At the same time, CCTV can be used to collect large amounts of information about people's movements and activities, and thus clearly has significant implications for privacy. Advances in technology are greatly increasing the capability of users to capture and analyse personal information using CCTV. [Footnotes omitted]

[34] The Report concluded at [4.12] that the Privacy Act is the most appropriate regulatory framework for CCTV:

4.12 We believe the Privacy Act is the most appropriate regulatory framework for CCTV. While there are a range of concerns about CCTV, most of them boil down to a concern about the ways in which CCTV is used to collect personal information, and about how the personal information that is collected is stored, who has access to it, how long it is retained for, and how it is used and disclosed. These are all core Privacy Act issues. The Privacy Act provides a framework within which the perceived benefits of CCTV can be obtained while at the same time protections can be put in place against the possible threats to privacy. CCTV differs from the more intrusive forms of visual surveillance that we believe should be covered by criminal offences under the Surveillance Devices Act (although if CCTV were to be used to conduct intimate covert filming or visual surveillance of the interior of a dwelling, an offence under the Surveillance Devices Act would be committed). It is used in public and semi-public places where people's expectations of privacy are lower than in private places; it is not usually covert, because the cameras can be seen and ideally there will be signs in place notifying people that the area is under surveillance; and it is not targeted at particular individuals. There are still legitimate privacy concerns about CCTV, but these can be adequately dealt with under the Privacy Act. [Footnotes omitted]

[35] As will be known, the Privacy Act regulates the way in which personal information is collected, held, used and disclosed. Agencies that deal with personal information must comply with the twelve privacy principles set out in the Act and if they fail to do so a complaint can be made to the Privacy Commissioner. Proceedings before the Tribunal can follow.

The "collection" issue

[36] The first four of the information privacy principles have as their focus the collection of personal information. As they are the primary focus of this part of the discussion they are reproduced here in full. Each uses the word "collect":

Principle 1
Purpose of collection of personal information

Personal information shall not be collected by any agency unless—
(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
(b) the collection of the information is necessary for that purpose.

Principle 2
Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.
(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—
  (a) that the information is publicly available information; or
  (b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or
(d) that non-compliance is necessary—
  (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  (ii) for the enforcement of a law imposing a pecuniary penalty; or
  (iii) for the protection of the public revenue; or
  (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(e) that compliance would prejudice the purposes of the collection; or
(f) that compliance is not reasonably practicable in the circumstances of the particular case; or
(g) that the information—
  (i) will not be used in a form in which the individual concerned is identified; or
  (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(h) that the collection of the information is in accordance with an authority granted under section 54.

Principle 3
Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—
  (a) the fact that the information is being collected; and
  (b) the purpose for which the information is being collected; and
  (c) the intended recipients of the information; and
  (d) the name and address of—
    (i) the agency that is collecting the information; and
    (ii) the agency that will hold the information; and
  (e) if the collection of the information is authorised or required by or under law,—
    (i) the particular law by or under which the collection of the information is so authorised or required; and
    (ii) whether or not the supply of the information by that individual is voluntary or mandatory; and
  (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
  (g) the rights of access to, and correction of, personal information provided by these principles.
(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.
(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.
(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—
  (a) that non-compliance is authorised by the individual concerned; or
  (b) that non-compliance would not prejudice the interests of the individual concerned; or
  (c) that non-compliance is necessary—
    (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
    (ii) for the enforcement of a law imposing a pecuniary penalty; or
    (iii) for the protection of the public revenue; or
    (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
  (d) that compliance would prejudice the purposes of the collection; or
  (e) that compliance is not reasonably practicable in the circumstances of the particular case; or
  (f) that the information—
    (i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4
Manner of collection of personal information

Personal information shall not be collected by an agency—
(a) by unlawful means; or
(b) by means that, in the circumstances of the case,—
(i) are unfair; or
(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

[37] In broad terms these four principles give effect to the Collection Limitation Principle in the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)*:

Collection Limitation Principle

7. There should be limits to the collection of personal data and such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

[38] Principles 5 to 12 of the information privacy principles in the Privacy Act do not use the word "collect". These principles deal with information an agency "holds". Principles 10 and 11 also refer to the purposes for which information was "obtained". The only term defined by the Act, however, is "collect".

"Collect" – the definition

[39] The Privacy Act defines "collect" in negative terms. That is, the definition defines what is **not** meant by "collect" in the Act:

collect does not include receipt of unsolicited information

[40] As the Act does not limit the term "collect" other than to exclude receipt of unsolicited information, the meaning of "collect" must be ascertained from the text and purpose of the Privacy Act. See the Interpretation Act 1999, s 5. That purpose is stated in the Long Title of the Privacy Act as the promotion and protection of individual privacy in general accordance with the *OECD Guidelines*:

An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular,—
(a) to establish certain principles with respect to—
(i) the collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
(ii) access by each individual to information relating to that individual and held by public and private sector agencies; and
(b) to provide for the appointment of a Privacy Commissioner to investigate complaints about interferences with individual privacy; and
(c) to provide for matters incidental thereto
[Emphasis added]

[41] It has been suggested that surveillance of an individual by means of a monitoring device is not collection for the purposes of the Act because the information is not solicited in the sense of a request for the information being made to the individual. See Roth *Privacy Law and Practice* (LexisNexis, Wellington) at [PVA2.5]. In our view there is a clear answer to this suggestion:

[41.1] The term collect is intended to have a broad meaning and is not a synonym of "solicit". It is to be given the purposive meaning of "gathering together, the seeking of or acquisition of personal information". See the *Oxford English Dictionary Online* (Oxford University Press, June 2014) and the *New Shorter Oxford English Dictionary*. In addition, the term solicit is not to be restricted to "ask for". In the context of the Privacy Act it is to have the meaning of "to seek after, to try to find, obtain or acquire. See the *Oxford English Dictionary Online*. Thus interpreted the word "collect" does **not** require a "request" to the subject in question. It is not permissible for the negative "does not include receipt of unsolicited information" to govern the meaning of "collect". Collect cannot be read as meaning "to ask for". While "collect" certainly includes the receipt of information asked for, it is not limited to this single meaning.

[41.2] A narrowing of the protection of the Privacy Act to those circumstances in which information is collected by soliciting in the sense of "to ask for" would be inconsistent with the promotion and protection of personal privacy. Surveillance usually results in the collection of personal information and information collection is one of the main purposes for which surveillance is used. In fact the Group of Experts state in their *Explanatory Memorandum* to the *OECD Guidelines* at [52] that the second part to the Collection Limitation Principle is directed against the use of surveillance devices:

> 52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement.…

As stated by the Law Commission in its June 2011 Report at [2.81], the current definition of "collect" is not intended to exclude the obtaining of personal information by means of surveillance devices. The purpose of and background to the Act suggest that surveillance should be considered to be a form of collection. The decision in *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (CA) is of limited relevance to a situation where an agency deliberately installs a camera and uses it to obtain information about people in a particular area.

[42] The submission of the Office of the Privacy Commissioner to the Law Commission was that "unsolicited" is to be narrowly defined as information which comes into the possession of the agency in circumstances where the agency has taken no active steps to acquire or record that information. See the Report at [2.84]. That is, the "unsolicited" exception excludes only:

> … those situations where the agency cannot in practice be held accountable for informing the individual about the collection, for the manner of collection, or for justifying why it needs the information. For instance, "unsolicited information" can be defined as "information that comes into the possession of the agency in circumstances where the agency has taken no active steps to acquire or record that information".

[43] We are of the view that this is the correct interpretation and it is adopted.

Conclusions on "collect"

[44] Our conclusions on "collect" are in summary:

[44.1] The Act does not limit the term "collect" other than to exclude receipt of unsolicited information. The meaning of "collect" must therefore be ascertained from the text and purpose of the Privacy Act.

[44.2] That purpose is stated in the Long Title of the Privacy Act as the promotion and protection of individual privacy in general accordance with the *OECD Guidelines.*

[44.3] Individual privacy will be promoted and protected by giving to the term collect a broad meaning. The term is not a synonym of "solicit". It is to be given the purposive meaning of "gathering together, the seeking of or acquisition of personal information".

[44.4] The word "collect" does **not** require a "request" to the subject in question.

[44.5] While "collect" certainly includes the receipt of information asked for, it is not limited to this single meaning. "Collect" does not in this context mean "received".

[44.6] A narrowing of the protection of the Privacy Act to those circumstances in which information is received and then only by soliciting in the sense of "to ask for" would be inconsistent with the promotion and protection of personal privacy.

[44.7] The definition of "collect" is not intended to exclude the obtaining of personal information by means of surveillance devices. The purpose of and background to the Act suggest that surveillance should be considered to be a form of collection.

[44.8] "Unsolicited" is to be narrowly defined as information which comes into the possession of the agency in circumstances where the agency has taken no active steps to acquire or record that information.

[45] Given these conclusions we further conclude that the information privacy principles, particularly Principles 1 to 4 were engaged by the surveillance system installed by Mr Naughton.

The point at which Principles 1 to 4 are engaged

[46] In view of Mr Naughton's evidence that when the request for access to personal information was made by Mr Armfield and Ms Halls the surveillance system was not then operational, it is necessary to address the question of the point at which Privacy Principles 1 to 4 are engaged in such situation.

[47] For the reasons which follow we are of the view that the "collection" principles in Principles 1 to 4 have operation prior to the information being collected and received. They prescribe the framework or process for collection which must be in place before information is received:

[47.1] Principle 1 prohibits the collection of personal information "**unless**" the separate and cumulative requirements in paras (a) and (b) are satisfied. The lawful purpose must exist along with the necessity prior to collection. Compliance with Principle 1 must therefore necessarily precede the receipt of the information:

> Principle 1
>
> *Purpose of collection of personal information*
>
> Personal information shall not be collected by any agency **unless**—
>
> (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
>
> (b) the collection of the information is necessary for that purpose.
>
> [Emphasis added]

[47.2] Principle 3 explicitly emphasises that there is a duty on an agency to take certain steps "**before the information is collected**":

> (2) **The steps referred to in subclause (1) shall be taken before the information is collected** or, if that is not practicable, as soon as practicable after the information is collected.
>
> [Emphasis added]

[47.3] Principle 4 limits the manner in which personal information can be collected (no unlawful or unfair means, no unreasonable intrusion) and stipulates the preconditions which must be satisfied before collection is undertaken. Those preconditions continue to apply during the collection process. So too in the case of Principle 2(1).

[47.4] The principles are inter-related and partly overlapping and must be studied as a whole. See the Explanatory Memorandum by the Expert Group to the *OECD Guidelines*:

> 50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole….

So viewed, the "collection" principles are clearly engaged before the information is collected.

[48] We do not, on the facts, need to consider whether the "collection" principles apply to attempts to collect information.

The point at which Principle 6 is engaged

[49] We now address the point at which Principle 6 is engaged. The answer lies in the clear wording of the Principle:

> 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.
> (3) The application of this principle is subject to the provisions of Parts 4 and 5.

[50] While this Principle opens with the words "[w]here an agency **holds** personal information", the Principle goes on to make clear that it does not operate only in situations where information is actually held:

[50.1] The right is to **confirmation whether or not the agency holds personal information** and only if it does, to have access to that information.

[50.2] A permitted ground for refusing the request is that the information does not exist or is not held. See s 29(2):

> (2) An agency may refuse a request made pursuant to principle 6 if—
> (a) the information requested is not readily retrievable; or

(b) the information requested does not exist or cannot be found; or
(c) the information requested is not held by the agency and the person dealing with the request has no grounds for believing that the information is either—
  (i) held by another agency; or
  (ii) connected more closely with the functions or activities of another agency.

[51] While Principle 6 is often referred to in the shorthand as a right to personal information, it is more accurately a right to confirmation whether the agency holds personal information and if it does, to have access to that information. If none is held, s 29(2) recognises such circumstance as a statutory ground for refusing the request. It is significant that the "does not exist, is not held" ground is attached to the permitted grounds for refusal. The holding of personal information by the agency is not a precondition to the exercise of the right to obtain confirmation whether or not the agency holds information. Put another way, the holding of information is not a precondition to the operation of the right in Principle 6 to obtain confirmation whether or not the agency holds personal information. The Principle 6 right operates irrespective whether personal information is held by the agency and section 40 (decisions on requests) and 44 (reasons for refusal to be given) operate with the same rigour whether personal information is held or not.

[52] It follows that when on 31 March 2012 Mr Armfield and Ms Halls asked to see what was being collected by Mr Naughton, it was not an adequate response for him to reply "No, not without a search warrant". In terms of Principle 6, Mr Armfield and Ms Halls were entitled to obtain confirmation whether Mr Naughton held their personal information. If no such information was held, it was permissible for Mr Naughton to have responded that none was held as the system was not on that date operative. However, this was the very information he wished to conceal from them. Nevertheless, his response (flat refusal without reasons) was not a permitted response.

Privacy enhancing technologies

[53] Masking software is known as a Privacy Enhancing Technology (PET) and its use is recommended by the OECD 2013 *Revised Guidelines* at para 19(g):

> [Member countries should] consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy.

[54] In our view leveraging technology to enhance privacy is a valuable approach and is to be encouraged. Unsurprisingly there are provisos:

> **[54.1]** The initial set up of the surveillance system must comply with Information Privacy Principles 1 to 4.
>
> **[54.2]** The masking, pixilation or other technology must be applied to ensure or to enhance such compliance.
>
> **[54.3]** The software must prevent the monitoring system from both seeing and recording the masked off area. Provided the information cannot later be accessed or recovered, there can be no principled objection to the use of the technology.

[55] This is not an exhaustive list. Provided technology or software is deployed in a manner that allows the surveillance system to comply not only with the letter but also with the spirit of the information privacy principles, there is no objection in principle to its use.

[56] There will, however, remain an information asymmetry. The person or persons whose privacy is being (potentially) intruded upon will be conscious only of the cameras pointed in their direction. They will not know whether masking technology has been employed to exclude the collection of their personal information and if so, the degree to which it has been successful. Only the agency will have that information. This highlights the importance of the Principle 6 right to confirmation whether the agency holds personal information and of the duties imposed by the collection principles. But if the field of vision can be and is edited or masked by the software so that no personal information is collected, there will be no breach of Principle 4. As conveniently summarised in the submissions for the Privacy Commissioner:

> **[56.1]** Prior to the use of the technology or software, the cameras must be positioned so that personal information is not collected by means that, in the circumstances, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual(s) affected.
>
> **[56.2]** If the intrusion cannot be minimised further through adjustments of the camera position or angle, then masking technology (or other PET) can be used to ensure information is not in fact collected in a way that intrudes to an unreasonable extent upon the personal affairs of the individual concerned.
>
> **[56.3]** If the masking technology or PET cannot successfully reduce the intrusion to a level which complies with Principle 4, the camera must not be operated at all.

[57] We address now our findings on the facts.

Application of the law to the facts – Principles 1 to 4

[58] As the collection principles overlap and are interrelated we address them together and not necessarily in numerical order.

[59] Principle 3. Neither at the time the surveillance system became operative nor at any subsequent time did Mr Naughton discharge his obligation under Principle 3 to inform Mr Armfield and Ms Halls of the fact that their personal information was being collected (they were not to know when the system went live), the purpose for which the information was being collected, the intended recipients of the information and of their rights of access to, and correction of, personal information provided by the information privacy principles. Mr Naughton had no reasonable grounds to believe that any of the grounds in Principle 3(4) applied. We accordingly find he was in clear breach of Principle 3.

[60] Principle 1. Principle 1 imposes two obligations. First, fundamental to the privacy principles, is the requirement that personal information not be collected by an agency unless the information is collected for a lawful purpose connected with a function or activity of the agency. Second is the requirement that collection of the information be necessary for that purpose. Necessary is here to be understood as reasonably necessary (*Lehmann v Canwest Radioworks Ltd* [2006] NZHRRT 35 at [50]). In the present case the lawful purpose limb is satisfied. The deployment of security cameras in a business setting is not of itself unlawful provided the relevant statutory regimes (eg the Privacy Act and the Search and Surveillance Act are observed and no civil tort is committed). Mr Naughton believed the surveillance system was necessary to protect his property and Bed and Breakfast business. The real issue is whether personal information was being collected from the Armfield property and whether such collection was reasonably necessary for that purpose. To a substantial degree our analysis of this

issue overlaps with the analysis of Principle 4. To avoid unnecessary repetition we will address the two principles together while acknowledging their distinctly different purposes.

[61] Principle 4. Principle 4 prohibits the collection of personal information by unlawful means or by means that, in the circumstances of the case are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

[62] Both Principle 1 and Principle 4 turn on the question whether personal information about Mr Armfield, Ms Halls and their children was collected by Mr Naughton by way of his surveillance system. When the system was initially set up and went live, it appears that the field of view of Cameras 1, 2 and 3 underwent adjustment. We do not have sufficient information to know what adjustments were made and the dates on which this occurred. Nor do we know when the masking of Cameras 2 and 3 occurred. We will assume for the purpose of this decision that the positioning of the cameras, the masking of Cameras 2 and 3 and the operation of the system as seen by the Tribunal during the view held on 7 February 2013 was the stable, long term system which had been collecting information from at least May or June 2012.

[63] As to Cameras 2 and 3 we find no breach of Principles 1 and 4. They have been masked to black out the clear view that would otherwise be afforded of the Armfield property, particularly their outdoor children's play area and entertainment area.

[64] Our finding in relation to Camera 1 is the opposite. This camera has always provided a good view of the front corner of the Armfield property, a corner where the Armfield children play on their swing. The camera is not and never has been masked. It means that when the Armfield children are at play on their swing their activities are both monitored and recorded, as are the activities of any adult person supervising their play.

[65] The intention of Mr Naughton is to surveil the footpath and road outside the Armfield address. That may be so but it was clear from the scene inspection that unless the field of vision of Camera 1 is masked off to prevent the collection of personal information from the Armfield property, the collection of personal information from that property will intrude to an unreasonable extent on the personal affairs of Mr Armfield, Ms Halls and their three children.

[66] We accordingly find that Principle 4 is breached by the operation of Camera 1.

[67] Because the collection of such personal information is not necessary for the purpose of protecting Mr Naughton's property and the Bed and Breakfast business, it follows also that Mr Naughton is in breach of Principle 1 as well.

Application of the law to the facts – Principle 6

[68] We turn now to Principle 6. There has been only one request by Mr Armfield and Ms Halls under this principle, being the request made on 31 March 2012. Speaking for herself and her husband, Ms Halls asked to see the footage being collected. This was a request under Principle 6. It is not required that the requester use the statutory language. It is for the agency to be aware of the obligations under the information privacy principles, principles which Mr Naughton claims to have studied prior to purchasing the monitoring system. It was his responsibility to know that as an agency, he was obliged to confirm whether or not he held such personal information and that the request could be refused on the grounds that the requested information was not held.

[69] Contrary to ss 27 to 29, 30 and 44 of the Privacy Act, no reasons were given by Mr Naughton for the refusal of the request. The question is whether Mr Naughton's monosyllabic response satisfied the requirements of the Act.

[70] An agency which receives a request under Information Privacy Principle 6 for access to personal information has three key obligations:

> **[70.1]** First, to make a **decision whether the request is to be granted**. This decision must be made "as soon as reasonably practicable" and in any case not later than 20 working days after the day on which the request is received by that agency. See s 40(1) of the Privacy Act 1993:
>
> > **40 Decisions on requests**
> >
> > (1) Subject to this Act, the agency to which an information privacy request is made or transferred in accordance with this Act shall, as soon as reasonably practicable, and in any case not later than 20 working days after the day on which the request is received by that agency,—
> > (a) decide whether the request is to be granted and, if it is to be granted, in what manner and, subject to sections 35 and 36, for what charge (if any); and
> > (b) give or post to the individual who made the request notice of the decision on the request.
>
> Failure to comply is deemed to be a refusal to make available the information to which the request relates (s 66(3)). The governing test is "as soon as reasonably practicable". The 20 working day period is the upper limit to what can be said to be "as soon as reasonably practicable". See further *Koso v Chief Executive, Ministry of Business, Innovation and Employment* [2014] NZHRRT 39 at [1] to [6] and [62].
>
> **[70.2]** Second, **to make the information available** without "undue delay". This obligation is contained in s 66(4) of the Act. Where undue delay occurs there is similarly a deemed refusal to make the information available (s 66(4)).
>
> **[70.3]** Third, where the request is refused, **to give reasons for the refusal**. See s 44:
>
> > **44 Reason for refusal to be given**
> >
> > Where an information privacy request made by an individual is refused, the agency shall,—
> > (a) subject to section 32, give to the individual—
> > (i) the reason for its refusal; and
> > (ii) if the individual so requests, the grounds in support of that reason, unless the giving of those grounds would itself prejudice the interests protected by section 27 or section 28 or section 29 and (in the case of the interests protected by section 28) there is no countervailing public interest; and
> > (b) give to the individual information concerning the individual's right, by way of complaint under section 67 to the Commissioner, to seek an investigation and review of the refusal.

[71] The question is whether, by answering the request for access with a monosyllabic "No", Mr Naughton complied with s 40(1) of the Act. Certainly a decision was communicated immediately by Mr Naughton. The question is whether it was a "decision" of the kind required by s 40(1). In our view it was not because no reasons were given. Specifically, none of the reasons for refusal permitted by ss 27 to 29 were given. The duty imposed by s 40(1) on an agency is a duty to decide **and** to give the reason for the refusal. The content of the duty to decide **with** reasons is made plain by Principle 6 read with ss 29(2), 30 and 44. That is, the requester is entitled:

[71.1] To confirmation whether his or her personal information is held by the agency; and

[71.2] If the request is refused, to reasons for the refusal. Only the reasons permitted by ss 27 to 29 can be given; and

[71.3] To information concerning the individual's right, by way of complaint to the Privacy Commissioner, to seek an investigation and review of the refusal.

[72] These obligations flow directly from the mandatory statutory duty imposed by s 44 that the agency "shall" give reasons for any refusal. Should the Act be interpreted as not imposing an obligation to decide **with** reasons, an agency could escape disclosing whether it holds personal information and the requester would be left without remedy. That would frustrate the purpose of Principle 6 and s 29(2)(b) and (c).

[73] Our conclusion is that a decision is not given under s 40(1) unless the reason for the decision is also given, as required by s 44.

[74] As it is common ground that no reason was ever given by Mr Naughton for refusing the Principle 6 request, Mr Naughton breached the s 40 duty to decide "as soon as reasonably practicable, and in any case not later than 20 working days after the day on which the request was received".

[75] This was an interference with the privacy of Mr Armfield and Ms Halls as defined in s 66(2)(a)(i) by reason of s 66(3).

Whether there was an interference with the privacy of Mr Armfield and Ms Halls

[76] The Tribunal has jurisdiction to grant a remedy under s 85 of the Privacy Act only if there has been "an interference with the privacy of an individual". That term is defined in s 66:

> **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.

[77] Where s 66(1) applies the Tribunal must be satisfied not only that an action breaches an information privacy principle but also that, in the opinion of the Tribunal, that action has resulted in one or more of the consequences listed in s 66(1)(b).

[78] However, where s 66(2) applies, none of the s 66(1)(b) factors are relevant. It must, however, be shown that there was no proper basis for the decision made by the agency under Part 4 or Part 5 of the Act.

[79] In the present case s 66(1) applies to the established breaches of Principles 1, 3 and 4 while s 66(2) applies to Principle 6.

Section 66(1) and Principles 1, 3 and 4

[80] For the reasons given earlier, we have found that Mr Naughton breached Information Privacy Principles 1, 3 and 4. The question is whether Mr Armfield has established also one of the forms of loss or harm listed in s 66(1)(b).

[81] As to loss of dignity, we refer to the description given in *Law v Canada (Minister of Employment and Immigration)* [1999] 1 SCR 497 at [53] where Iacobucci J delivering the judgment of the Supreme Court of Canada stated:

> 53 … Human dignity means that an individual or group feels self-respect and self-worth. It is concerned with physical and psychological integrity and empowerment. Human dignity is harmed by unfair treatment premised upon personal traits or circumstances which do not relate to individual needs, capacities, or merits… Human dignity is harmed when individuals and groups are marginalized, ignored, or devalued….

[82] As to what is included in "injury to the feelings", it was held in *Winter v Jans* at [36] that "injury to the feelings" can include conditions such as anxiety and stress. In *Director of Proceedings v O'Neil* [2001] NZAR 59 at [29] injury to feelings was described in the following terms:

> [29] The feelings of human beings are not intangible things. They are real and felt, but often not identified until the person stands back and looks inwards. They can encompass pleasant feelings (such as contentment, happiness, peacefulness and tranquillity) or be unpleasant (such as fear, anger and anxiety). However a feeling can be described, it is clear that some feelings such as fear, grief, sense of loss, anxiety, anger, despair, alarm and so on can be categorised as injured feelings. They are feelings of a negative kind arising out of some outward event. To that extent they are injured feelings.

[83] In our view the facts establish both significant loss of dignity and significant injury to the feelings of Mr Armfield and Ms Halls. Mr Naughton chose to hang Cameras 1, 2 and 3 when Mr Armfield and Ms Halls were at home. He was confrontational. From their perspective, Mr Armfield and Ms Halls could see cameras pointing directly into their lounge and outdoor area where their spa, children's play area and entertainment area

were situated. They immediately felt under surveillance and believed that Mr Naughton was recording their and their children's intimate family activities in what they had until then regarded as the safety and privacy of their own home. They felt vulnerable, violated and disempowered. This caused substantial concern, upset and anger. The impact of the appearance of the cameras was compounded by the fact that they had had no warning and no idea of Mr Naughton's motivation or of the use to which the personal information could be put. Their distress was amplified by their concerns for their children and discomfort at their being watched. They were concerned about their safety in their own home.

[84] These feelings and emotions only increased when, on asking Mr Naughton to see what was being recorded, they were met with a clear "No, not without a search warrant". This unwarranted confrontational stance was intended to disempower, humiliate and injure Mr Armfield and Ms Halls. As Mr Naughton stated, it was his intended objective that they know he had them under surveillance. Although he did not quite put it this way, he wanted to control Mr Armfield's alleged behaviour and in particular to ensure that the neighbourhood was "safe" from him.

[85] When on 13 April 2012 Mr Armfield and Ms Halls reasonably proposed (through their solicitor) that the cameras be re-aligned so that they did not collect personal information from the Armfield property, Mr Naughton deliberately made a point of not replying. The same happened with the second letter sent on 17 August 2012.

[86] The evidence shows that from the outset Mr Naughton intended to and indeed succeeded in inflicting significant loss of dignity and significant injury to the feelings of Mr Armfield and to Ms Halls.

[87] It follows that all the requirements of s 66(1) are satisfied and Mr Armfield has established an interference with the privacy in relation to Principles 1, 3 and 4.

Section 66(2) and Principle 6

[88] For the reasons given earlier we are of the view that the request under Principle 6 for confirmation whether Mr Naughton held personal information was not "decided" in the statutory sense of a decision plus reasons prior to the expiration of the "as soon as reasonably practicable, and in any case not later than 20 working days" timeline. In terms of s 66(3) that failure is deemed for the purposes of s 66(2)(a)(i) to be a refusal to make available the information to which the request related. That refusal was, without more, an interference with the privacy of Mr Armfield and Ms Halls as there was no proper basis for Mr Naughton's default.

Conclusion on "interference with privacy"

[89] For the reasons given we conclude on the balance of probabilities that an interference with privacy as defined in s 66 of the Act has been established in relation to Principles 1, 3, 4 and 6. It follows that the Tribunal has jurisdiction to grant one or more of the remedies specified in s 85 of the Act.

REMEDIES

[90] Where the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual it may grant one or more of the remedies allowed by s 85 of the Act:

> **85 Powers of Human Rights Review Tribunal**

(1) If, in any proceedings under section 82 or section 83, the Tribunal is satisfied on the balance of probabilities that any action of the defendant is an interference with the privacy of an individual, it may grant 1 or more of the following remedies:
  (a) a declaration that the action of the defendant is an interference with the privacy of an individual:
  (b) an order restraining the defendant from continuing or repeating the interference, or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference, or conduct of any similar kind specified in the order:
  (c) damages in accordance with section 88:
  (d) an 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:
  (e) such other relief as the Tribunal thinks fit.
(2) In any proceedings under section 82 or section 83, the Tribunal may award such costs against the defendant as the Tribunal thinks fit, whether or not the Tribunal makes any other order, or may award costs against the plaintiff, or may decline to award costs against either party.
(3) Where the Director of Human Rights Proceedings is the plaintiff, any costs awarded against him or her shall be paid by the Privacy Commissioner, and the Privacy Commissioner shall not be entitled to be indemnified by the aggrieved individual (if any).
(4) It shall not be a defence to proceedings under section 82 or section 83 that the interference was unintentional or without negligence on the part of the defendant, but the Tribunal shall take the conduct of the defendant into account in deciding what, if any, remedy to grant.

[91] Section 88(1) relevantly provides that damages may be awarded in relation to three specific heads of damage:

88 Damages

(1) In any proceedings under section 82 or section 83, the Tribunal may award damages against the defendant for an interference with the privacy of an individual in respect of any 1 or more of the following:
  (a) pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose:
  (b) loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference:
  (c) humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

[92] The remedies sought in the amended statement of claim dated 30 January 2013 are:

[92.1] A declaration that Mr Naughton has interfered with the privacy of Mr Armfield.

[92.2] An order restraining Mr Naughton from continuing or repeating his actions in collecting the private information of Mr Armfield and his family.

[92.3] An order that Mr Naughton erase or otherwise destroy any private information already obtained.

[92.4] Damages for loss of benefit, humiliation, loss of dignity and injury to feelings.

[93] It is no defence that the interference with privacy was unintentional or without negligence. The Tribunal must nevertheless take the conduct of Mr Naughton into account in deciding what, if any, remedy to grant. See s 85(4) of the Act.

[94] In this regard we see few, if any, mitigating factors. Mr Naughton has from the outset adopted an unhelpful, if not confrontational stance. He presents himself as the victim and is impervious to the hurt and harm he has caused Mr Armfield and Ms Halls. Indeed, he sees the infliction of hurt and harm as "mission accomplished". He claims to have studied the Privacy Act and the Privacy Commissioner's *CCTV Guidelines* prior to purchasing the surveillance system but it was abundantly clear at the hearing that if he has engaged in such study he has understood nothing. In determining the appropriate remedies to be granted we must take these factors into account.

[95] Mr Naughton must understand and accept that the operation of the surveillance system is lawful only if personal information is collected for a lawful purpose connected with his Bed and Breakfast business and the collection of the information is reasonably necessary for that purpose (see Principle 1). Personal information about Mr Armfield, Ms Halls and their children cannot be collected if in the circumstances such collection is unfair or intrudes to an unreasonable extent on their personal affairs (Principle 4). This means that the masking of Cameras 2 and 3 as seen by the Tribunal during the view on 7 February 2013 must continue to block out from the cameras' field of view the Armfield side of the boundary fence. Camera 1 either has to be repositioned so that it does not afford a view of any part of the Armfield property or alternatively, the masking software must be deployed to achieve the same end.

[96] Mr Armfield and Ms Halls have been reasonable from the outset, requiring not the removal of Cameras 1, 2 and 3 but their positioning in such a way that they do not collect personal information from their property or at the very least, do not intrude to an unreasonable extent upon their personal affairs. Their primary difficulty is not only that Mr Naughton refuses to communicate with them or their solicitor, they are forced to deal with him across an information barrier. That is, their relationship with Mr Naughton is asymmetrical. They see three cameras which, to the naked eye, appear to overlook their property and private places. They do not know what is being seen via these cameras, they do not know by whom it is being seen and they do not know whether the information is being distributed or used for purposes unrelated to the security of the Bed and Breakfast.

[97] It is therefore to be hoped that Mr Naughton will make good his assurance to the Tribunal that he is willing to allow Ms Halls access to the system monitor so that she can verify for herself that by a combination of the positioning of the cameras and the use of masking software, no personal information about her, her husband or children is being collected.

[98] To ensure that there is a new start following the delivery of this decision, the system is to be re-set in the light of this decision. This must occur within seven days of the delivery of this decision. The process is to begin with Mr Naughton providing to Mr Armfield and Ms Halls (or their solicitor) written notice of the information required by Principle 3 to be given to persons from whom personal information is to be collected. In particular, that notice is to provide the information stipulated by Principle 3(1)(a) to (g). In the event of any change being made to the surveillance system, to the orientation of the cameras or to the masking of Cameras 1, 2 and 3, notice of such change is to be given by Mr Naughton to Mr Armfield, Ms Halls or their solicitor. In the event of such change the Principle 3 process is to be repeated.

[99] Principle 6 will have an important role to play in the monitoring of Mr Naughton's compliance with the privacy principles. Mr Naughton must understand that Mr Armfield and Ms Halls have an entitlement under Principle 6 to obtain confirmation whether or not

Mr Naughton holds personal information about them. Exercise of this entitlement is not restricted to one occasion or several occasions. It can be exercised any number of times. We are confident that Mr Armfield and Ms Halls will not abuse their entitlement by making pointless requests. However, the entitlement is available to be exercised as an aid to the ongoing monitoring of Mr Naughton's surveillance system to ensure that the system is being operated within the law. Mr Naughton, in turn, is obliged to respond to any Principle 6 request within the timeframes prescribed by s 40(1) and 66(4) of the Privacy Act. The grounds on which any request can be refused are restricted to those, and only those, permitted by ss 27 to 29.

[100] The collection of personal information from the front of the Armfield property via Camera 1 is to cease immediately either by the repositioning of the camera so that it points away from the Armfield property or by the use of masking software, or by both. Within seven days of this decision Mr Naughton is to give written confirmation to Mr Armfield, Ms Halls or their solicitor that these steps have been taken.

[101] We come now to the remedies of a declaration and damages.

Declaration

[102] While the grant of a declaration is discretionary, declaratory relief should not ordinarily be denied. See *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].

[103] On the facts we see nothing that could possibly justify the withholding from Mr Armfield and Ms Halls a formal declaration that Mr Naughton interfered with their privacy and such declaration is accordingly made.

Damages

[104] In closing submissions presented by Mr Hansen on 15 April 2013 the Tribunal was told that any remedy should deter, but not widen the gap between the two neighbours. The signal sent to them should be a balanced one.

[105] Ordinarily, on the facts as found the award of damages under s 88(1)(c) would presently be in the region of $15,000 or more. See the comparable decisions in *Lochead-MacMillan v AMI Insurance Ltd* [2012] NZHRRT 5, *Fehling v South Westland Area School* [2012] NZHRRT 15, *Director of Human Rights Proceedings v Hamilton* [2012] NZHRRT 24 and *Geary v Accident Compensation Corporation* [2013] NZHRRT 34.

[106] However, given that the primary remedies sought here are the "cease and desist" orders and further given the responsible position taken by Mr Armfield and Ms Halls through their counsel that they do not wish to make relations with Mr Naughton worse than they are, we have concluded that an award of $7,000 would be appropriate.

FORMAL ORDERS

[107] For the foregoing reasons the decision of the Tribunal is that:

> **[107.1]** A declaration is made under s 85(1)(a) that Mr Naughton interfered with the privacy of Mr Armfield and Ms Halls by failing to comply with Information Privacy Principles 1, 3 and 4 and by his refusal on 31 March 2012, without good reason, to confirm under Principle 6 whether or not he held their personal information.

[107.2] The surveillance system installed at 16 Havelock Place, Blagdon, New Plymouth is to be reset to comply with the information privacy principles as interpreted and applied in this decision. This must occur within seven days of the delivery of this decision. Within the same seven day period Mr Naughton is to provide to Mr Armfield or Ms Halls (or their solicitor) written confirmation that this has been done.

[107.3] Within seven days of the date of this decision Mr Naughton is to provide to Mr Armfield and Ms Halls (or their solicitor) written notice of the information required by Principle 3 to be given to persons from whom personal information is to be collected. In particular, that notice is to provide the information stipulated by Principle 3(1)(a) to (g). In the event of any change being made to the surveillance system, to the orientation of Cameras 1, 2 and 3 or the masking of those cameras, notice of such change is to be given by Mr Naughton to Mr Armfield, Ms Halls (or their solicitor). In the event of such change the Principle 3 process is to be repeated.

[107.4] The collection of personal information from the front of the Armfield property via Camera 1 is to cease immediately either by the repositioning of the camera so that it points away from the Armfield property or by the use of masking software, or by both. Within seven days of this decision Mr Naughton is to give written confirmation to Mr Armfield, Ms Halls or their solicitor that this step has been taken.

[107.5] Within seven days of the date of this decision Mr Naughton is to erase or otherwise destroy any personal information held by him about Mr Armfield, Ms Halls and their children and within the same seven day period provide to Mr Armfield and Ms Halls (or their solicitor) written confirmation that this has been done.

[107.6] Damages of $7,000 are awarded against Mr Naughton under ss 85(1)(c) and 88(1)(c) of the Privacy Act 1993 for loss of dignity and injury to feelings.

COSTS

[108] Costs are reserved:

[108.1] Mr Armfield is to file his submissions within fourteen days after the date of this decision. The submissions for Mr Naughton are to be filed within a further fourteen days with a right of reply by Mr Armfield within seven days after that.

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

[108.3] In case it should prove necessary we leave it to the Chairperson of the Tribunal to vary the foregoing timetable.

.....	.....	.....
Mr RPG Haines QC	**Mr GJ Cook JP**	**Mr BK Neeson**
Chairperson	**Member**	**Member**