IN THE HIGH COURT OF NEW ZEALAND
AUCKLAND REGISTRY

CIV 2013-404-2168
[2014] NZHC 1343

IN THE MATTER	of the New Zealand Bill of Rights Act 1990 and the Government Communications Security Bureau Act 2003
BETWEEN	KIM DOTCOM First Plaintiff
AND	MONA DOTCOM Second Plaintiff
AND	BRAM VAN DER KOLK Third Plaintiff
AND	JUNELYN VAN DER KOLK Fourth Plaintiff
AND	MATHIAS ORTMANN Fifth Plaintiff
AND	FINN BATATO Sixth Plaintiff
AND	ATTORNEY-GENERAL in respect of the New Zealand Police First Defendant
AND	ATTORNEY-GENERAL in respect of the Government Communications Security Bureau Second Defendant

Hearing: 24 & 25 March 2014

Appearances: P Davison QC, W Akel & H Steele for First and Second Plaintiffs
G Foley for Third to Sixth Plaintiffs
K McDonald QC, A Boadita-Cormican & M Cooke for First Defendant (New Zealand Police)
D Boldt for Second Defendant (GSCB)
S Grieve QC, Special Advocate

Judgment: 16 June 2014

RECALLED JUDGMENT OF WINKELMANN J

This judgment was delivered by me on 16 June 2014 at 2.00 pm pursuant to Rule 11.5 of the High Court Rules.

Registrar/ Deputy Registrar

I Introduction

[1] In this proceeding the plaintiffs allege that in the course of a police operation, codenamed "Operation Debut", the New Zealand Police subjected them to unreasonable and illegal search and seizure in breach of s 21 of the New Zealand Bill of Rights Act 1990 (NZBORA). Operation Debut involved the New Zealand Police's search of two sites and the seizure and subsequent treatment of electronic items pursuant to warrants obtained under the Mutual Assistance in Criminal Matters Act 1992. The plaintiffs also allege that the Government Communications Security Bureau (GCSB) has unlawfully undertaken surveillance of them. The plaintiffs seek awards of damages in respect of trespass to goods, land and breach of the plaintiffs' rights under the NZBORA and breach of privacy. The proceeding is in its interlocutory phase.

[2] The plaintiffs and defendants have each applied for further and better discovery. The plaintiffs have also applied for non-party discovery, and for an order that particular documents obtained by them in these proceedings can be used in the extradition proceedings in respect of the first plaintiff, Mr Dotcom.

II Plaintiffs' applications

(i) Plaintiffs' application for particular discovery

[3] The plaintiffs seek an order for particular discovery in respect of eight categories of documents, which I will address in turn. But first, something as to the relevant principles.

[4] Rule 8.19 of the High Court Rules provides that particular discovery may be ordered if it appears to a Judge "from the evidence or from the nature or circumstances of the case or from any document filed in the proceeding" that there are grounds for believing that a party has not discovered documents that should have been discovered. The applicant need not show that there has been a breach of a

discovery order. The rule encompasses the possibility that a discovery order requires variation, and also the obligations of a continuing discovery.[1]

[5] As to what the expression "should have been discovered" means for the purposes of the rule, I proceed upon the basis that standard discovery as provided for by r 8.7 of the High Court Rules has been ordered in this case. Neither party argues for a variation of the scope of discovery required where standard discovery is ordered. Rule 8.7 describes the requirements of standard discovery as follows:

> **Standard discovery**
>
> Standard discovery requires each party to disclose the documents that are or have been in that party's control and that are –
>
> (a) documents on which the party relies; or
>
> (b) documents that adversely affect that party's own case; or
>
> (c) documents that adversely affect another party's case; or
>
> (d) documents that support another party's case.

Category 1

[6] The plaintiffs seek discovery of:

> All documents held by, on behalf of, or under the control of the Commissioner of Police – Peter Marshall, Deputy Commissioner Operations – Mike Bush, and Deputy Commissioner Resource Management –Viv Rickard, personally or held in their respective offices, informing them or in any way keeping them advised of developments and/or seeking any approval or comment in relation to Operation Debut, both pre and post determination, and/or in relation to surveillance of any of the plaintiffs or any interception of the communications.

[7] The plaintiffs' principal submission in support of this order is that no documents within the category have been discovered, and it is inconceivable that there would be no documents.

[8] The defendants oppose the making of this order, saying that they have already provided discovery of this category of document, and seven documents that fit this description have already been disclosed. The plaintiffs nevertheless seek at

---

1 *Southland Building Society & Barlow Justice Ltd* [2013] NZHC 1125 at [18]-[30].

least a sworn statement that there are no documents that ever came into the possession of the named individuals or their officers.

[9] The r 8.19 threshold has not been met in respect of this category of documents. There is no evidence or circumstances to suggest that there are further documents. Indeed, the only evidence available to me suggests quite the opposite, as it shows that an effort has been made to discover this category of document.

Category 2

> With reference to document CLO.008.00198, all documents held by, or created by, Detective Inspector Cramer in his role as liaison officer with Special Agent Poston of the FBI.

[10] Document CLO.008 00 198 evidences that Detective Inspector Cramer was responsible for liaising between New Zealand Police and the United States authorities. The plaintiffs say these communications would clearly be relevant to the planning and knowledge of the police surrounding Operation Debut. They accept that some documents in this category have been discovered, but say they are surprised that there is no correspondence or record of communications between Detective Inspector Cramer and the FBI beyond these documents or at least an indication that such documents previously existed but no longer exist.

[11] The defendants dispute that all documents in the category identified by the plaintiffs are relevant, but in any case say they have already discovered 13 documents in this category.

[12] Again, there is no evidence to suggest that there are further documents which should be discovered that have not already been disclosed, or that there are any such documents which existed, but which no longer exist.

Category 3

[13] The category of documents sought is:

> With reference to document CLO.004.09382, including an email from Detective Sergeant Nigel McMorran to various addressees on 7 November

> 2011 at 15:18, all documents relating to the presentation for "the highrachy" (sic) referred to, including the names of all those present at the presentation.

[14] The defendants respond to this request by saying that there are no further discoverable documents. The plaintiffs say however that the defendants should name the hierarchy referred to which would enable the plaintiffs to identify relevant documents.

[15] This request also does not met the criteria of r 8.19. The request for clarification of the meaning of "highrachy" is a request for information not documents.

Category 4

[16] The documents requested are:

> With reference to document CLO.004.09261, any documents relating to any steps taken by, or on behalf of, the New Zealand Police directed at obtaining information regarding the plaintiffs' communications during the course of their remand in prison, including any communications between the Police the administration of the Mt Eden Corrections Facility or its contractors or agents.

[17] The plaintiffs say that these documents are relevant to the breach of privacy and unreasonable search and seizure causes of action. They say that any continued surveillance and/or monitoring of the plaintiffs' communications while they were held on remand, either at the instigation of or with the knowledge of the police would be a continuing breach of s 21 of the NZBORA and/or privacy breach.

[18] The defendants accept monitoring occurred but say that it was lawful monitoring, authorised by the provisions of the Corrections Act 2004, ss 106 and 113. I am not called upon to decide whether any monitoring or use of intercepted material by Corrections was lawful as I consider that the defendants are correct in their argument that absent an allegation in the statement of claim of unlawful monitoring following Mr Dotcom's arrest, these documents cannot be said to be relevant in terms of r 8.7.

Category 5

[19] The plaintiffs seek discovery of:

> Any documents relating to the use of the interception device known as StingRay to carry out surveillance and/or interceptions on the plaintiffs; or documents relating to any other product or device of a similar kind or having similar utility that would enable the interception of telephone communications.

[20] The defendants say that this question has been asked and answered on a number of occasions. In the answers to interrogatories provided by Malcolm Burgess on behalf of the police, Mr Burgess states that neither the New Zealand Police nor any organisation on its behalf intercepted, taped or captured any communication or data in relation to any of the plaintiffs' electronic addresses. He also says that the New Zealand Police have no knowledge of the interception of communications or surveillance by means of any device or software located or concealed in any property or vehicle of the plaintiffs at any time from 1 January 2012 to today.

[21] The plaintiffs respond that these answers were given in September 2013 - before the plaintiffs were able to narrow their questioning concerning the surveillance down to the use of the StingRay system. They say that in his judgment of 6 December 2012, Judge Dawson found that:

> It would appear likely that some form of surveillance and/or interference with telephone communications has happened.

The plaintiffs therefore say that there is evidence which constitutes grounds for believing that the Police have not discovered documents.

[22] In correspondence after Judge Dawson's judgment, and in response to Mr Davison's request in relation to the StingRay system, the Crown confirmed on behalf of the New Zealand Police that neither Mr Dotcom nor his associates have been the subject of electronic surveillance by police since the arrests. They confirmed that for these purposes, "surveillance" includes surveillance using any system. Again, I accept the defendants argument that in the circumstances, and on the evidence, the threshold for an order under r 8.19 has not been met.

Category 7

[23] Particular discovery is sought in respect of:

> Any correspondence any/or memoranda passing between NZ Police and GCSB relating to the Ministerial Certificate dated 16 August 2012.

[24] The plaintiffs say they do not challenge Crown Law's claimed privilege for legal advice in connection with the issue of the Ministerial certificate. The focus of the application is on communications passing between GCSB staff and Police as to the need for such certificate. The plaintiffs say that the sequence of events appears to be as follows. Detective Inspector Wormald of New Zealand Police gave evidence on 9 August 2012 that, so far as he was aware, there was no surveillance of the plaintiffs by a surveillance team or any other government organisation prior to 19 January 2012. The plaintiffs say that because he had been involved in arrangements with the GCSB, he knew that statement was incorrect. Immediately after that hearing, steps were taken by persons unknown to the plaintiffs for the drafting and obtaining of the Ministerial certificate. The effect of the Ministerial certificate would have been to authorise the withholding of any information from the plaintiffs that would reveal the true involvement of the GCSB – information that would also directly contradict Detective Inspector Wormald's evidence that there had been no such surveillance. The plaintiffs wish to argue that the true reason for obtaining the Ministerial certificate was to obscure the involvement of the GCSB and its surveillance.

[25] I accept the plaintiffs' argument that if this were proven, attempts to conceal the breach of privacy might be relevant to credibility issues and also possibly relevant to the assessment of damages as a factor aggravating the breach.

[26] As to the evidence that there are further documents, the plaintiffs maintain that the decision to seek such a certificate would have been evaluated and considered by the first and second defendants' senior representatives, and that there would have been communications between them in addition to the privileged communications with Crown Law.

[27] The defendants respond that there are no such documents and that if there had been such documents, they would have been listed in both lists of documents. They do not contest that such documents, if they existed, would be relevant.

[28] In this case, I consider that the plaintiffs are on stronger ground with their argument that the circumstances of the case suggest there are likely to be documents that fall within this category. I have taken into account the defendants' submissions that there is an existing list of documents which contains the standard confirmations as to search, and the completeness of what is contained there. Nevertheless, the absence of any documents within this category is surprising in all of the circumstances. Seeking a Ministerial certificate is a significant step. The chronology of events suggests a possible link between events in Court and the obtaining of the certificate. It is therefore appropriate to put the defendants to the trouble of filing an affidavit stating what documents in this category are or have been in the first and second defendants' control and if they have been but are no longer in that party's control, the party's best knowledge and belief as to when the documents ceased to be in the party's control and who now has control of them.

Category 8

[29] The plaintiffs seek the following documents:

> With reference to page 18, paragraph 29 of the Kitteridge Report, being document CLO.100.00806, any documents pertaining to the legal justification and circumstances surrounding the surveillance of the 88 people described as having been subjected to GCSB surveillance.

[30] The "Kitteridge Report" is a report prepared by Ms Rebecca Kitteridge following a review she undertook into aspects of the operation of the GCSB. The review was initiated because of the revelation that the GCSB had undertaken illegal surveillance of the first plaintiff, Mr Dotcom, his family and an associate. The surveillance was unlawful because it involved intercepting the communications of New Zealand permanent residents, in breach of s 14 of the Government Communications Security Bureau Act 2003 (the GCSB Act). Ms Kitteridge was seconded to the GCSB as Assistant Director to review compliance systems and processes. In the course of that review Ms Kitteridge identified that GCSB had been

providing assistance to domestic agencies on the basis that the agency had a warrant, and GCSB was merely acting as its agent in conducting surveillance activity. It also, on request from New Zealand agencies, intercepted metadata, on the basis of an understanding that the metadata was not a communication for the purposes of the s 14 prohibition. In paragraph 29 of the report, Ms Kitteridge expressed the following views:

> The consequence of these developments is that the lawfulness of some of GCSB's past assistance to domestic agencies is now called into question. In relation to NZSIS, the relevant period is between 1 April 2003, when the GCSB Act came into force, and 26 September 2012, when such assistance ceased. During that period GCSB provided 55 instances of assistance to NZSIS, which potentially involved 85 New Zealand citizens or permanent residents. In relation to the New Zealand Police, the relevant period is between 1 April 2003 and 1 January 2009, because (as already noted) every case of assistance to Police after that date has already been investigated by the Inspector-General of Intelligence and Security and determined to be lawful (with the exception of the case involving Mr Dotcom and his associate). During the relevant period, GCSB provided assistance to the Police in one instance, which potentially involved three New Zealand citizens or permanent residents.

[31] The plaintiffs say that in determining the level of damages it is important to establish whether this was a one-off mistake by GCSB with regard to the plaintiffs, or whether there was a systemic disregard for the legal parameters of the GCSB Act that had been on-going for some time and led to the unlawful surveillance of others, including the 88 people referred to in the Kitteridge Report.

[32] Although the plaintiffs acknowledge that these documents are likely to raise serious confidentiality issues, they say that this could be dealt with by using the special advocate process developed for other documents in respect of which confidentiality is claimed.

[33] The GCSB say that if an error was made in the case of the 88, it was different to the error in this case. It was not, as it was in the case of the plaintiffs, a mistake as to the immigration status of the subjects of the surveillance.

[34] I accept that information gathered by Ms Kitteridge, and set out in her report, shows that the error on the part of the GCSB in respect of the 88 individuals was of a different nature to the mistake in relation to the first three plaintiffs. I do not

consider that those documents fall within the definition of documents to be discovered under r 8.7. They are not relevant in the sense now employed in standard discovery.

[35] I do not discount the possibility that discovery could assist the plaintiffs in making out a case of "systemic disregard" by GCSB of legal parameters, that would be of only marginal relevance to Mr Dotcom's case. Requiring discovery in respect of those 88 would therefore open up a collateral but very broad field of enquiry with the accompanying obligation to discover documents the plaintiffs seek. That would impose a disproportionate obligation upon GCSB. One of concepts that runs through the discovery regime is proportionality. Rule 8.2 of the High Court Rules requires parties to co-operate to ensure that the processes of discovery and inspection are proportionate to the subject matter of the proceeding.

Category 6

[36] An application for further discovery is made in respect of:

> Any documents relating to the plaintiffs, and in particular Kim Dotcom, held by the Prime Minister as the Minister responsible for GCSB, or his office, or the Department of the Prime Minister and Cabinet and/or any of its subset business units including any documents held by the senior DPMC official who attended part of the debrief of the GCSB component of Operation Debut on 16 February 2012.

[37] The content of the further discovery sought under category 6 overlaps with the application for non-party discovery, and I consider the issue under that head.

(ii) Plaintiffs' application for non-party discovery

[38] The plaintiffs seek non-party discovery from Mr Roy Ferguson and the Department of Prime Minister and Cabinet (DPMC). Mr Ferguson was the intelligence coordinator at DPMC at the times relevant to these proceedings. The order for non-party discovery sought is in the following terms:

> (a) that within the time fixed by the Court, an authorised representative of the Department of the Prime Minister and Cabinet (DPMC) and Mr Roy Ferguson file an affidavit stating whether the following documents relating to the matters in issue in this proceeding are or

have been in their control, and if they have been but are no longer in their control, stating when they ceased to have control of them and who now has control of them:

(i) all documents held by the DPMC including both documentary material and electronically held material relating to the plaintiffs or any of them and

(ii) documents held by Mr Roy Ferguson relating to Operation Debut, his knowledge of GCSB involvement in Operation Debut and his attendance at the briefing at GCSB headquarters on 16 February 2012.

[39] An application for non-party discovery is governed by r 8.21(1). That rule provides that non-party discovery may be ordered if it appears that a person who is not a party to a proceeding may be or may have been in control of one or more documents or a group of documents that the person would have had to discover if the person were a party to the proceeding. An order made under r 8.21(1) can require the non-party to file an affidavit stating whether the documents are or have been in the person's control, and if they have been but are no longer so, the person's best knowledge and belief as to when the documents ceased to be in the person's control and who would now have them. An order can also be made to require the non-party to make the documents available for inspection. The order may be made on the terms that the applicant pay the person from whom discovery is sought the whole or part of that person's expenses, including solicitor client costs.

[40] The application as framed is plainly too broad, but during the course of argument, Mr Davison confirmed that the plaintiffs seek only documents that might have a bearing upon:

(a) the legality of GCSB's surveillance operation in connection with the plaintiffs; and

(b) GCSB's knowledge of the illegality of those operations, and the timing of that knowledge.

[41] Mr Boldt who took responsibility on behalf of the Attorney-General for arguing the application, says in reply that the narrowing of the scope of the order sought will at least bring the category within the requirements of specificity for non-

party discovery. However he says to the extent that there are documents that could bear upon the legality of GCSB's involvement and GCSB's knowledge of the illegality of the operation, those documents have already been discovered. He asks, since all the materials have been discovered by GCSB itself, what more could these parties have?

[42] Although GCSB may have discovered those documents falling within this category which are in its possession or control, it appears from the evidence and the circumstances that the non-parties will have documents which fall within the narrow category now described by Mr Davison. It is not at issue that Mr Ferguson, in fulfilment of a responsibility he had as an employee working for DPMC, attended a briefing on the issue of the illegality of the surveillance. It is likely that he at least took or prepared notes of that briefing. I am satisfied that those documents would be relevant for the purposes of r 8.7 as they may bear upon the circumstances in which the GCSB undertook its illegal surveillance operation. Accordingly, I am satisfied that it is appropriate to make the orders sought, but amending (i) to read:

> All documents held by DPMC (including both documentary material and electronically held material) relating to GCSB's surveillance of the plaintiffs, the legality of that surveillance, and GCSB's knowledge of the illegality of that surveillance.

(iii) Plaintiffs' application for order for access to and use of documents in extradition proceedings

[43] The plaintiffs seek leave to use a limited number of documents provided to them through discovery in this proceeding, in another proceeding. They wish to use the documents as evidence in support of an application in the extradition proceedings in the District Court[2] for disclosure from Immigration New Zealand and the New Zealand Security Intelligence Service (NZSIS).

[44] The context of the application is that Mr Dotcom has applied in his extradition proceedings for disclosure orders in respect of Immigration New Zealand and the NZSIS. The discovery is to enable him to explore improprieties in process be believes arose out of political involvement and interference in matters relating to

---

[2] Proceedings in which the United States of America seeks the extradition of some of the plaintiffs.

the extradition proceedings. He intends to argue that the process by which his applications for New Zealand residency was granted in 2010 was contaminated by political interference. In preparation for the filing of that application, the plaintiffs sought the consent of the defendants to the use of some documents that have been discovered by the defendants in this proceeding. Consent to the use of those documents has been declined by the defendants.

[45] The plaintiffs say that all of the documents sought relate specifically to Immigration New Zealand or the NZSIS, and are directly relevant to the application for disclosure before the extradition Judge. The documents would provide the basis for an argument that the extradition proceeding amounted to an abuse of process. Mr Dotcom wishes to make a case that around the time his and his wife's applications for permanent residence were lodged, the NZSIS engaged in discussions with the FBI about some or all of the plaintiffs. The documents illustrate that the applications were put on hold to allow communication of concerns the NZSIS had in respect of the applicant. The hold was then lifted and the application approved. The plaintiffs will argue that the real reason the application was granted in this way was to ensure Mr and Mrs Dotcom came to New Zealand, because in New Zealand Mr Dotcom could be subject to extradition processes. They say that this manipulation forms part of a broader picture which demonstrates that the processes of the New Zealand Courts have been abused.

[46] Mr Dotcom says that the documents are necessary to lend an air of reality to the District Court application - they add colour and detail to the argument that there has been manipulation of systems and processes to such an extent that the extradition proceedings before the Court are an abuse of process. If required the documents could be obtained under the Official Information Act 1982, but this is a simpler, more direct procedure.

[47] In the District Court the requesting authority[3] has applied for summary dismissal of the application on the grounds that the Supreme Court decision in

---

3 The United States of America.

Dotcom v United States of America[4] makes plain that the plaintiffs have no entitlement to any disclosure in the context of extradition proceedings.

[48] The starting point for consideration of Mr Dotcom's application for leave is the principles underlying the procedure of discovery. Discovery of relevant documents entails an invasion of the privacy of the providing party.[5] It is an invasion of privacy because it involves an inroad on the rights of individuals to keep their documents private. However the public interest in ensuring that all relevant information is available to the adjudicative process justifies the court's powers to order disclosure.[6] That interest has been held to override the private and public interest in the maintenance of confidentiality.[7]

[49] To respond to the perils associated with discovery, the common law developed safeguards. Those safeguards included limiting discovery only to the extent that it was necessary in order to enable a court fairly to decide the case before it.[8] A further restriction was that a lawyer who obtains possession of documents belonging to his client's adversary during a proceeding gives an implied undertaking to the court not to use that material for any purpose other than the proper conduct of that action on behalf of his or her client.[9] The undertaking was also based in part on public policy: "for otherwise litigants may be deterred from making full and frank disclosure".[10]

[50] Our High Court Rules do not use the wording of "implied undertakings". The relevant rule provides:

> **8.30 Use of documents**
>
> …
>
> (4) A party who obtains a document by way of inspection or who makes a copy of a document under this rule—

---

4 *Dotcom v United States of America* [2014] NZSC 24.
5 *Telstra New Zealand Ltd v Telecom New Zealand Ltd* (1999) 14 PRNZ 108 (HC) at 113.
6 A Zuckerman *Zuckerman on Civil Procedure: Principles of Practice* (Thomson Reuters, London, 2013) at [15.168].
7 *Harman v Secretary of State for the Home Department* [1983] 1 AC 280 (HL).
8 Zuckerman, above n 6, at [15.168].
9 *Harman*, above n 7.
10 *Crest Homes plc v Marks* [1987] 1 AC 829 (HL) at 857.

(a) may use that document or copy only for the purposes of the proceeding; and

(b) except for the purposes of the proceeding, must not make it available to any other person (unless it has been read out in open court).

Nevertheless the Court of Appeal has maintained the use of "undertakings" terminology and so preserved the ability of the Court to permit collateral use in limited circumstances.[11] If the undertaking is to the Court, then the Court may relax its insistence on that undertaking. Given the significance of the implied undertaking, the Court will not release or modify the prohibition on collateral use save in special circumstances and where the release will not occasion injustice to the person giving discovery.[12] It is important that exceptions not be allowed to "swamp the rule".[13]

[51] The discretion to allow use of documents is to be exercised on a case by case basis. Some observations in existing case law are nevertheless of assistance. If the parties to the litigation are the same, the primary concerns are not as great. But it has been stressed that to relax the implied undertaking given in one proceeding in order to give disclosure of documents that could not be obtained through an application for discovery in the collateral proceeding would undermine the public policy behind the rule against collateral use.[14] In determining whether circumstances exist such as to justify collateral use the Courts have had regard to whether declining to permit the use of the documents would, because of the severity of its effect on the plaintiff, be a disproportionate outcome.[15] It is also relevant to consider whether the disclosure is in the public interest, as where the revenue department sought to use disclosed documents to pursue tax evasion. The public interest identified was that all tax and revenue penalties be paid and evaders be convicted and sentenced.[16]

---

11 *Wilson v White* [2005] 3 NZLR 619 (CA).
12 *Crest Homes*, above n 10, at 860; discussed and followed in *Wilson v White*, above n 8.
13 *Wilson v White*, above n 11, at [64].
14 *Crest Homes*, above n 10, at 857.
15 *Hunter Grain Ltd v Price* HC Tauranga CIV-2008-470-192, 23 April 2010 at [47].
16 *A v A (ancillary relief), B v B (ancillary relief)* [2000] 1 FLR 701 (FC).

[52] The defendants say that:

(a) No special circumstances exist to justify departure from the restriction on use set out in r 8.30 as the plaintiffs are not entitled to disclosure in any case. The Supreme Court has ruled that the plaintiffs are not entitled to disclosure in the context of the extradition proceedings.

(b) The extradition and damages proceedings involve different parties and jurisdictional procedures, and they raise different legal and factual issues for resolution.

(c) There are significant privacy concerns. Five of the six documents which were the subject of the application derive from a police investigation of people other than the plaintiffs. The defendants contest the plaintiffs' assertion they could have been obtained under the Official Information Act. They say that these documents would, absent the discovery order, have been kept confidential to the extent permitted by law. The sixth document is a compilation of emails received by the second defendant from a third party whose views as to their potential release under the Official Information Act, or Privacy Act, are not before the Court as evidence, and should not be speculated upon.

[53] I do not consider that the Supreme Court in the *Dotcom* decision has ruled out the possibility that disclosure orders against New Zealand agencies could be made in the context of extradition proceedings.[17] In *Dotcom* the Supreme Court was addressing the possibility of disclosure orders made against the requesting authority, which is a different type of application then the application for disclosure by a New Zealand agency.

[54] I also agree with the applicants that these documents all relate to public officials either conducting public business or recounting their involvement in the

[17] Although some rights are likely to be very constrained. See discussion in *United States v Kwok* [2001] SCR 532 at [97]–[106].

conduct of public business — therefore privacy interests do not weigh very heavily. Any such legitimate concerns could be met with the making of appropriate confidentiality and suppression orders in the District Court. Nevertheless as mentioned above, the policy considerations behind the rule embodied in r 8.30 are wider than privacy considerations – they reflect the concern that litigants not be deterred from making full and frank disclosure.

[55] The defect in the plaintiffs' application is that Mr Dotcom has failed to show adequate reasons for a departure from the rule against collateral use. The documents identified by the applicants appear to establish no more than that the NZ SIS was consulted in the immigration process and that the process was put on hold while they were consulted. They could scarcely be said to give an air of reality to the abuse of process argument. Therefore denying Mr Dotcom the ability to use them for this collateral purpose will not cause him undue hardship. I therefore decline the application.

II Defendants' applications

(i) Defendants' applications for further and better discovery of schedule 1 documents

[56] The defendants bring a number of applications for further and better discovery. They seek orders that Mr Dotcom file a further affidavit listing (and then to make available for inspection) the schedule 1 documents set out below. The schedule 1 documents are as follows:

> **SCHEDULE 1**
>
> 1. Dictation tapes or other electronic recordings and transcripts of interviews of the all or any of the plaintiffs by Mr David Fisher (or any person working with Mr Fisher), in researching or drafting *The Secret Life of Kim Dotcom: Spies, Lies and the War for the Internet* to the extent that material relates to the events that are the subject of these proceedings, including Operation Debut, its aftermath, the defendants or the proceedings themselves.
>
> 2. Communications (including but not limited to emails, text messages and other forms of social media messaging) between all or any of the plaintiffs and Mr Fisher, (or any person working with Mr Fisher) that contain references to the events that are the subject of these

> proceedings, including Operation Debut, its aftermath, the defendants or the proceedings themselves.

Schedule 1 documents

[57] The defendants ground their application squarely upon the contents of the book *The Secret Lift of Kim Dotcom: Spies, Lies and the War for the Internet*, a book released on 18 November 2013 and authored by David Fisher, a journalist working for the New Zealand Herald. It is common ground that the book contains extensive references to interviews with Mr Dotcom regarding the searches and related seizing of items in January 2012, and their aftermath.

[58] The defendants initially sought the information from Mr Fisher who has declined to provide it saying that to do so "would have a chilling effect on the general public's right to freedom of speech." The defendants now say that they are entitled to access to the documents through Mr Dotcom because although the documents are Mr Fisher's, they are nevertheless within the control of Mr Dotcom. He has control over them in the sense that he has a legal right to inspect or copy the documents. That legal right is derived from the Privacy Act 1993, because the transcripts and audio copies of interviews with Mr Dotcom constitute information about an identifiable individual within the meaning of the Privacy Act 1993. Mr Dotcom has an enforceable right to access such information pursuant to privacy principle 6. For the purposes of discovery, the defendants argue that a document is in the control of a party even if in the possession of another, if the party has an enforceable right to access the document under the Privacy Act 1993, relying upon the decision *Johansen v American International Underwriters (New Zealand) Ltd*.[18]

[59] Mr Dotcom concedes that some of the schedule 1 material may be relevant, but he says that he does not have a right of access under the Privacy Act to any documents held by Mr Fisher or at least not an unequivocal right, such as to oblige him to provide discovery of that information.

---

[18] *Johansen v American International Underwriters (New Zealand) Ltd* [1997] 3 NZLR 765 (HC).

[60] Mr Dotcom's first argument is that the Privacy Act does not apply to any news medium in relation to its news activities and the activities of Mr Fisher fall within the definition of news activity by a news medium as set out there.

[61] As an alternative argument Mr Dotcom says that this Court is not bound by and should not follow *Johansen*. While r 1.3 provides that "control" in relation to a document means a "right, otherwise and under these rules, to inspect or copy the document", s 11(2) of the Privacy Act states that the privacy principles do not confer any legal right that is enforceable in a Court of law. In addition, the Privacy Act is concerned with access to information contained within documents, rather than access to the documents themselves, and as such the Privacy Act entitlement does not sit comfortably with the discovery obligations under the High Court Rules. Section 42 of the Privacy Act he says, illustrates this. It states that information can be provided to the requesting party "by giving an excerpt or summary of the contents" or "by furnishing oral information about its contents".

[62] Mr Dotcom says that the correct course of action for the defendants is to make an application for non-party discovery in respect of Mr Fisher. Not only would this be the more expeditious and efficient process, it should not be incumbent on Mr Dotcom to seek recourse to the Privacy Commissioner in order to fulfil his discovery obligations.

Analysis

[63] The starting point is that a party is obliged to discover documents in the parties' possession or control. Rule 1.3 provides:

> Control, in relation to a document, means—
>
> (a) possession of the document; or
> (b) a right to possess the document; or
> (c) a right, otherwise than under these rules, to inspect or copy the document[.]

[64] The defendants say that the documents are in Mr Dotcom's control because of the contents of principle 6 of the privacy principles.

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) of this principle, 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 of this Act.

[65] Of the twelve principles, only principle six is enforceable in a court, but only against "public sector agenc[ies]". Section 11 of the Privacy Act provides:

11 Enforceability of principles

(1) The entitlements conferred on an individual by subclause (1) of principle 6, in so far as that subclause relates to personal information held by a public sector agency, are legal rights, and are enforceable accordingly in a court of law.

(2) Subject to subsection (1) of this section, the information privacy principles do not confer on any person any legal right that is enforceable in a court of law.

[66] The first issue raised by Mr Dotcom is whether Mr Fisher is an "agency" for the purposes of Principle 6. Section 2 of the Act provides that a person can be an agency, whether in the private or public sector. However it also excludes from the definition of agency "in relation to its news activities, any news medium". Mr Dotcom says that the book is a news activity of a news medium.

[67] News medium is defined as "any agency whose business, or part of whose business, consists of a news activity". News activity is defined in the Privacy Act as:[19]

(a) The gathering of news, or the preparation or compiling of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public:

---

[19] Privacy Act 1993, s 2.

(b) The dissemination, to the public or any section of the public, of any article or programme of or concerning—

(i) News:

(ii) Observations on news:

(iii) Current affairs.

[68] When the Privacy of Information Bill (which became the Privacy Act) was first introduced to Parliament, there was initially no exception for media. The exception was introduced after strong lobbying by the Press Council.[20] In 2011, when undertaking a review of the Privacy Act the Law Commission discussed the importance of the news media exception:[21]

> The free flow of information through the media is vital to the life of a free and democratic society, and is supported by the protection of freedom of expression in the New Zealand Bill of Rights Act 1990. It is difficult to see how the media could perform this role effectively if it were subject to the Privacy Act's principles. Those principles are ill-aligned to the media function. For example they provide that an agency must collect personal information about an individual directly from the individual; it must allow the individual access to the information it holds about him or her; and it must not disclose the personal information it holds to anyone else … Not only could the media not operate effectively in such a context; they could barely operate at all.

[69] I acknowledge the importance of these principles but on the information available it is clear that the news media exception does not apply. I say this for two reasons. First, Mr Fisher's authorship of the book was not undertaken by a "news medium". It is true that Mr Fisher is a journalist working for a news medium, the New Zealand Herald, and that in that capacity he has written extensively on Mr Dotcom. But his book on Mr Dotcom is not affiliated with the Herald, and was published by an independent publishing agency. There can be no suggestion that Mr Fisher is himself a news medium as that phase is defined in the Privacy Act.

[70] My second reason is that the writing and publication of a book cannot, at least in this instance, be construed as news activity. The definition of news activity

---

20 Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review* (available online at <www.privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform-resources/privacy-commissioner-s-review-of-the-privacy-act>) at [1.4.51].

21 Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R 123, 2011) at [4.26].

protects two different forms of journalistic endeavour in its two limbs: preparing stories and disseminating stories. The first limb protects gathering, preparing, compiling, and making of observations on news, for the purpose of dissemination. The second limb protects the dissemination of the prepared story, provided it is about news, observations on news or current affairs. The end product of the two activities is specifically provided for in the definition: articles and programmes. Investigative journalism takes its form in long, detailed articles, which are covered by the Act's definition. Books, however, are not.

[71] Because Mr Fisher does not have the benefit of the news media exception, he is subject to the Privacy Act, and under information privacy principle 6, individuals are entitled to confirmation of whether information is held about them, and to have access to it.

[72] The definition of personal information is very wide, and is defined as "information about an identifiable individual". It is wide enough to capture the material the subject of this application.

[73] Section 11 of the Act, quoted above, renders principle six "enforceable … in a court of law". Crucially, however, its enforceability in a court of law only applies "in so far as that subclause relates to personal information held by a *public sector agency*". Mr Fisher is plainly not a public sector agency as defined in s 2 of the Act.[22]

[74] Any "entitlement", then, must be derived from the procedural pathways set out under Part 5 of the Act relating to access to and correction of personal information, and Part 8 relating to complaints procedures.[23] Individuals may make information privacy requests under principle 6(1)(b). Section 38 provides that "it is the duty of every agency to give reasonable assistance" to those who make information requests. Agencies who receive information privacy requests must decide whether the request is to be granted, and having done so notify the requesting individual as soon as reasonably practicable. A refusal to make information

---

22 A Minister, a Department, an organisation, or a local authority.

23 Privacy Act 1993, s 33.

available may amount to an "interference with the privacy" of Mr Dotcom in respect of which he has a right to complain to the Privacy Commissioner.[24]

[75] Importantly, the Act provides that where the information requested is in a document, that information can be made available in a variety of ways.[25] The individual can be given the opportunity to inspect the document, given a copy, an excerpt or summary, or just by being told about the information orally.[26] The information "shall" be provided according to the applicant's preference, unless to do so would impair efficient administration, be contrary to a legal duty, or prejudice security, defence, international relations, trade secrets, or one of the other enumerated reasons in s 29 for refusing a request.

[76] Accordingly, Mr Dotcom is "entitled" to the information that Mr Fisher holds. Though that entitlement is not one that can be enforced in this Court, it is one for which procedural pathways exist for enforcement.[27]

[77] This is sufficient to bring the situation within the definition of control for the purposes of the High Court Rules, namely a right to inspect or copy the documents. I note that this was the view of Master Kennedy-Grant in *Johansen*, a judgment which has subsequently been followed on several occasions.[28] I see no reason to depart from that line of authority.

[78] That brings me to the detail of the application. The description of documents listed there could include material of no relevance or only the most marginal relevance. I make clear that Schedule 1 information, once obtained by Mr Dotcom, is only to be discovered if it falls within the r 8.7 categories.

---

24 Privacy Act 1993, ss 66 and 67, and see also s 77.
25 Section 42.
26 Section 42(1).
27 Complaint to the Commissioner who can then proceed to the Human Rights Review Tribunal.
28 *Invensys PLC v Load Logic Ltd* HC Christchurch CP73/01, 26 March 2002; *Xuan v Wu* HC Auckland CIV-2002-404-1843, 14 October 2003; *FCA Investment Co v Nelson* HC Auckland CIV-2003-404-4287, 14 October 2003; *Bushetts Transport Ltd v Lowes* HC Wellington CIV-2011-486-131, 11 July 2011; *Body Corp 164399 v Auckland City Council* HC Auckland CIV-2004-404-2395, 20 April 2009; *Guttenbeil v Tower Insurance Ltd* HC Auckland CIV-2010-404-5675, 13 August 2012; and *Maybury v Cook* HC Wellington CIV-2008-485-109, 6 August 2008.

(ii) Defendants' application for further and better discovery of schedule 2 documents

[79] The defendants seek an order that each of the plaintiffs file and serve affidavits stating:

(a) whether any documents in the group of "Schedule 2" documents are, or have been in their control;

(b) and if no longer in their control, when they ceased to be in their control and who now has control of them;

(c) whether they are aware of documents which, although not in their control, would be discoverable if they had control of them;

(d) what steps each has taken to preserve the documents; and

(e) in the case of Mrs Dotcom only, what steps she has taken to search and review electronic files.

[80] Schedule 2 lists a number of categories of documents. I deal with each in turn.

Schedule 2, paragraph 1

[81] This category is as follows:

> 1. Communications (including but not limited to letters, emails, text messages and other forms of social media messaging) sent or received by the plaintiffs personally, including correspondence between and amongst the plaintiffs referring to the events of 20 January 2012, their aftermath, and these proceedings.

[82] The defendants say that the plaintiffs have not disclosed any personal communications whatsoever referring to the events of 20 January 2012, yet it is highly unlikely not one of the six plaintiffs created a single relevant communication in this category. The defendants make the following particular observations:

(a) There is no evidence the second plaintiff, Mrs Dotcom carried out a search for any such communications. The first and third to sixth plaintiffs have confirmed they have done in their affidavits of documents.

(b) There is some evidence that material has been deleted by the first plaintiff. The defendants refer to the part of the first plaintiff's affidavit of documents where he lists "the documents that are no longer in the control of the plaintiff" and where he refers to "electronic copies of documents generated on computer which were deleted every now and again in the ordinary course of business".

(c) The fourth plaintiff's affidavit suggests that relevant material in this category is within her power or control. The defendants say this inference is available from the fact that while the affidavits of the third, fifth and sixth plaintiffs each contain a statement that they:

> … have not made any relevant comment with regard to the raid, or the events following the raid, what would materially affect the outcome of the proceedings.

The fourth plaintiff gives no such confirmation.

(d) In their affidavits the third, fifth and sixth plaintiffs each state:

> I have not arranged for my cellphone or computer to be forensically examined to recover any deleted material as I understand it could be an expensive exercise. However in the period after I had full internet and cellphone access, I believe I have not made any relevant comment with regard to the raid, or the events following the raid, that would materially affect the outcome of these proceedings.

The first, second and fourth plaintiffs have not made the same statement.

[83] On this basis the defendants say in the circumstances there is ample evidence to provide sufficient grounds for believing:

(a) The documents described are relevant to the matters in issue in the proceeding and therefore discoverable.

(b) The plaintiffs are, or were, at material times in possession or control of documents in the category.

(c) The plaintiffs did not seek to preserve this category of documents.

(d) The second plaintiff has not carried out a reasonable search for the documents.

[84] The plaintiffs say that they have no such documents and there are no grounds to believe they do. Their phones and computers were seized as part of Operation Debut. The first, third, fifth and sixth plaintiffs were then in custody for about a month. When they were granted bail they did not have access to the internet for some time, and the cellphones they were allowed to use stored only text messages 20 messages at a time. They were not allowed Smartphones. Further, when released on bail the third to sixth plaintiffs were occupying the same house so any comment between them as to events, passed face to face.

[85] The plaintiffs have adequately explained the suggestion of the deletion of documents appearing in Mr Dotcom's affidavit of documents. They have explained that because the phones they were allowed to use only stored 20 messages at a time, some messages had to be deleted. Mr Dotcom also states that he did not record Skype conversations. There is nothing to suggest the deletion of material is more widespread than the deletion of text messages from cellphones with limited memory. It seems to me that deletion occurred at a time when these proceedings were not reasonably contemplated. There is therefore no reason to require further affidavits to be filed detailing documents which have passed out of the plaintiffs' control, or to require affidavit evidence as to the steps taken to preserve documents.

[86] Even if such material existed it is unlikely to be of sufficient relevance to bring it within r 8.7. This proceeding concerns allegations of trespass and breach of privacy by the plaintiffs against the defendants. The defendants hope to capture the plaintiffs reactions to those breaches in the aftermath of Operation Debut. Applying the concepts of proportionality in discovery discussed earlier, it seems to me that the obligation the defendants seek to impose upon the plaintiffs is unduly onerous given

the potential rewards for the defendants, documents which at best are likely to be relevant in only the loosest sense.

[87] That issue is not however determinative. For the reasons advanced by the plaintiffs I accept that it is most unlikely that any schedule 2 paragraph 1 communications were created in the immediate aftermath of the January raids. I am not therefore satisfied that there are grounds to believe anything that would fall within r 8.7 exists.

Schedule 2, paragraph 2

[88] This category is as follows:

> 2. Documents showing the plaintiffs were personally liable for the cost of repairing the physical damage at Mahoenui Valley Road in respect of which the claim for special damages at paragraph 88 of the statement of claim is made.

[89] The claim for the cost of repairs to the mansion is in the name of Mr Dotcom, the first plaintiff. Vestor Ltd is the lessee. Mr Dotcom is the sole director and shareholder of Vestor. The defendants complain that Mr Dotcom has not discovered any documents to support his alleged liability to make good the damage. Mr Dotcom says he is liable as a guarantor under the lease, yet no documents establishing liability have been discovered. The defendants submit it is therefore in the interests of justice that the plaintiffs *each* file a further affidavit listing the schedule 2.2 material and making these documents available for inspection.

[90] As noted, Mr Dotcom replies that he is liable as a guarantor under the lease. He also says that the defendants have been advised that if they intend to raise this issue at hearing, the plaintiffs will amend to join Vestor as a plaintiff.

[91] The lease has been discovered. Mr Tim Vestor is a party to the lease as a guarantor. I do not know if Tim Vestor is another name for Mr Dotcom. The lease document either does or does not prove Mr Dotcom is a guarantor. But in any event the points raised by the defendants seem directed to whether Mr Dotcom has the document to prove his claim he is personally liable. If Mr Dotcom does not discover

any such documents he will face considerable difficulty should he subsequently seek to produce them at the hearing. The evidence and circumstances are not such as to meet the r 8.19 threshold.

Schedule 3, paragraph 3

[92] This category of documents is:

> 3. Documents relating to the clones of, and encryption passwords for, the electronic items seized by the first defendant on 20 January 2012 including, in particular, documents showing the number of such passwords and the devices they relate to, that the plaintiffs are or were in possession and control of the encryption passwords to relevant devices and, if they are no longer in the possession and control of such passwords, when they were last in possession and control of them and what has become of them.

[93] The defendants do not seek to pursue this category of documents at this time.

Schedule 2, paragraph 4

[94] This category of documents is:

> 4. Any and all documentation relating to the connection records or configuration of electronic items seized on 20 January 2013 including, without limitation, any booklet or other record contained in the server room at the Mahoenui Valley Road property containing or referring to such information.

[95] The defendant does not pursue the application in respect of the "booklet" contained in the "boiler room". They do however continue to seek particular discovery of documentation relating more generally to the connection records or configuration of electronic items seized on 20 January 2012.

[96] Although I understand that the relevance of those documents is conceded, that relevance has not been explained to me. It is not self-evident. In any case that is not dispositive of this application. The plaintiffs say they have discovered all relevant documents and have nothing more. The evidence and circumstances do not give me grounds to believe there are such documents.

(iii) Defendants' application for production of medical records

[97] The defendant seeks an order requiring the second and fourth plaintiff to make available medical records listed by them in their affidavits of documents. After discussion the parties were able to agree a methodology for that to occur. The defendants will nominate a senior representative acceptable to the second and fourth plaintiffs, who will inspect the records. Counsel for the defendant, Ms McDonald and Ms Boadita-Cormican, are also to have access to the records for the purposes of inspection.

Summary

(1) The plaintiffs' application for further and better discovery is granted, but only concerning the Category 7 documents sought. I am satisfied that correspondence or memoranda passing between the police and GCSB relating to the ministerial certificate is relevant to the plaintiffs' contention that the defendants acted to conceal breaches of their privacy. I am not satisfied that either the evidence or the circumstances of the case suggest further Category 1, 2, 3, 5 documents exist. Nor am I satisfied that the Category 4 and 8 documents, if they exist, would be relevant under r 8.7.

(2) The plaintiffs' application for non-party discovery against Mr Roy Ferguson and the DPMC is granted on the basis set out at [42] above.

(3) The plaintiffs' application for access to and use of documents from this proceeding in the extradition hearing is declined. No sufficient reason to depart from the rule against collateral use has been demonstrated.

(4) The defendants' application for further and better discovery of documents held by Mr Fisher to which Mr Dotcom is entitled by virtue of the provisions of the Privacy Act is granted, but on the limited basis set out at [78] above.

(5) The defendants' other application for further and better discovery are declined. I am not satisfied that the requirements of r 8.19 have been met in respect of any of the categories of documents sought.

(6) The defendants' application for production of medical records is ordered by consent.

(7) I will address any issue as to costs at the next call of this proceeding.