

**IN THE HIGH COURT OF NEW ZEALAND  
AUCKLAND REGISTRY**

**CIV-2012-404-1928  
[2012] NZHC 1494**

UNDER the Judicature Amendment Act 1972

IN THE MATTER OF an application for judicial review and  
application for order for interim relief  
pursuant to section 8

BETWEEN KIM DOTCOM  
First Plaintiff

AND FINN BATATO  
Second Plaintiff

AND MATHIAS ORTMANN  
Third Plaintiff

AND BRAM VAN DER KOLK  
Fourth Plaintiff

AND ATTORNEY-GENERAL  
First Defendant

AND THE DISTRICT COURT AT NORTH  
SHORE  
Second Defendant

Hearing: 22 and 23 May, 6 June 2012

Counsel: P Davison QC (22 & 23 May only), W Akel and R Woods for First  
Plaintiff  
G J Foley for Second, Third & Fourth Plaintiffs  
M Ruffin (22 and 23 May only), F Sinclair for First Defendant (joined  
in capacity as representative of New Zealand Police)  
J Pike and A Toohey (6 June only) for First Defendant (joined in  
capacity as the Central Authority for the purposes of the Mutual  
Assistance in Criminal Matters Act 1992)

Judgment: 28 June 2012

---

**JUDGMENT OF WINKELMANN J**

---

*This judgment was delivered by me on 28 June 2012 at 3.30 pm pursuant to  
Rule 11.5 of the High Court Rules.*

*Registrar/ Deputy Registrar*

## TABLE OF CONTENTS

<b>Introduction</b>	[1]
<b>A. Were the warrants invalid?</b>	
(i) Factual background	[9]
Execution of warrants and items seized	[20]
(ii) Judicial review of search warrants issued under the MACMA	[27]
(iii) Is the offence adequately described in the warrants	[36]
(iv) Was there adequate definition of the authority to search and seize	[51]
(v) Should conditions have been imposed?	[78]
<b>B. Did the Police seize items outside the scope of the search warrant?</b>	[87]
<b>C. Was the provision by the Police of copies of digital files to the FBI unlawful?</b>	[90]
(i) Does s 49 regulate physical custody of an item only?	[93]
(ii) Did the plaintiffs consent to images of computer hard drives being shipped to the FBI offshore?	[98]
First phase	[104]
Second phase	[118]
Third phase	[122]
Was there consent?	[134]
(iii) Would the Solicitor-General have consented to the shipment?	[141]
<b>Summary of findings</b>	[144]
<b>Relief</b>	[145]

## **Introduction**

[1] The government of the United States of America seeks extradition of the plaintiffs in relation to charges stemming from their operation of the Megaupload business, a business which allows customers to upload bulk amounts of data to the internet, and share that data with others. The allegation is that the Megaupload platform has been used by customers in widespread breach of copyright. The United States has asked the Attorney-General of New Zealand for the New Zealand Police's assistance with the investigation of that suspected criminal offending. That request has been made under the Mutual Assistance in Criminal Matters Act 1992 (MACMA), an Act to facilitate the provision and obtaining of international assistance in criminal matters.

[2] In fulfilment of that request the Police have taken a number of steps including arresting the plaintiffs, carrying out searches, seizing assets, and obtaining orders freezing assets. The plaintiffs seek a judicial review of three search warrants issued by the North Shore District Court and executed by police in January 2012 at addresses associated with the first plaintiff, Mr Dotcom, and the fourth plaintiff, Mr Van Der Kolk, but at which assets of all four plaintiffs were seized.

[3] The plaintiffs allege that the search warrants were unlawful. They contend that the warrants were unreasonably broad in their terms; lacking specificity as to the charges to which the searches related, and as to the items to be searched for. It is further argued that the warrants should have prescribed a process for dealing with items taken away following the search, because the warrant authorised the search and seizure of digital storage devices which would inevitably store at least some irrelevant information. It was also known that the items seized were to be sent to the investigating authorities in the United States. It is argued that the Court should have stipulated conditions for the return to the plaintiffs of the original items, or at least

clones<sup>1</sup> of those items, and a procedure for safeguarding irrelevant and privileged material from access by the investigating authorities.

[4] The plaintiffs also seek to review the actions of the Police in executing the search warrants, on the grounds that they exceeded their powers in seizing and holding the items that they did.

[5] The first defendant was originally joined in the proceedings for, and on behalf of the Police. During the course of the initial hearing of the application for review, I was told by counsel for the first defendant that the Police had allowed the FBI to ship to the United States images of the content stored on the digital storage devices, that is to say, clones of the hard drives of those devices. The Police sought leave to file further evidence explaining the circumstances in which this occurred. That leave was granted and the initial hearing came to an end.

[6] Following the receipt of the additional information, the plaintiffs sought leave to amend their pleadings to add to the relief sought a declaration that removal from New Zealand of clones of the hard drives was unlawful. That leave was granted unopposed. At the request of the first defendant, there was then a further day's hearing in respect of this new aspect to the proceeding. I gave leave to Mr Pike and Ms Toohey to appear as counsel for the first defendant, but appearing for the Attorney-General in the Attorney's capacity as the Central Authority for New Zealand. "Central Authority" is defined in the MACMA as "the person or authority for the time being designated by that country for the purposes of transmitting or receiving requests made under or pursuant to" MACMA.<sup>2</sup>

[7] The plaintiffs now seek relief in the amended statement of claim which includes declarations that the warrants and removal of clones from New Zealand were unlawful, and also the making of orders as to how the items seized are to be dealt with by the Police.

---

<sup>1</sup> Throughout this judgment the expressions cloning and imaging are used interchangeably. There is some evidence that the processes involved in cloning and in forensic imaging may be different, but that difference is not material for the purposes of this judgment.

<sup>2</sup> Mutual Assistance in Criminal Matters Act 1992, s 2.

[8] The issues that arise in this proceeding are as follows:

- (i) Were the warrants invalid because of lack of detail as to the offences to which they related, and the parameters of the search, and/or because of the failure to attach sufficient conditions?
- (ii) In any case, have the Police exceeded the authority conferred upon them by the warrants?
- (iii) Did the Police act unlawfully in allowing the FBI to transport clones of hard drives overseas?
- (iv) What, if any relief should be granted in connection with any invalidity or illegality?

**A. Were the warrants invalid?**

**(i) *Factual background***

[9] The plaintiffs have interests in the Megaupload group of companies, which includes Megaupload Limited, Megavideo Limited and Megastuff Limited, the latter a New Zealand registered company. The plaintiffs Mr Dotcom and Mr Van Der Kolk are resident in New Zealand.

[10] On 5 January 2012, prosecuting authorities in the United States obtained an indictment from a Grand Jury in the State of West Virginia, charging the plaintiffs, along with other individuals and corporate entities (including Megaupload Limited), with breach of copyright, conspiracy to breach copyright, conspiracy to racketeer and money laundering. Under United States law, “racketeering” involves a criminal enterprise that is focused on committing or furthering any of a number of criminal offences, including money laundering and criminal breach of copyright.

[11] The charges flow from the activities of the Megaupload business. The FBI contends that the plaintiffs and companies in the Megaupload group were part of a

conspiracy, which the FBI for operational purposes has called the “mega-conspiracy”. The criminal objects of the conspiracy are alleged to have been to administer internet websites which were used by others to reproduce and distribute infringing copies of television programmes, software, music and motion pictures, and also to conduct monetary transactions with the proceeds of those unlawful activities. The FBI’s case is that Megastuff Ltd was involved in the transfer and distribution of illicit proceeds generated from the website.

[12] From early 2011 the Police were involved in providing direct assistance to the FBI in relation to the FBI’s investigation. Police assistance was initially provided informally, on an agency to agency basis, but in a letter dated 11 January 2012 the United States Central Authority<sup>3</sup> requested the Attorney-General for assistance on a government to government basis.<sup>4</sup> The letter stated that various authorities, including the FBI were investigating the “mega-conspiracy”, its officers and employees, including Mr Dotcom and Mr Van Der Kolk and Megastuff Ltd. It was alleged that members of the mega-conspiracy knew how their websites were used by others, had themselves used the systems to upload as well as reproduce and distribute copyrighted content and were aware that they had benefited financially directly from massive infringement of copyrighted material. The United States Central Authority sought assistance including:

... assistance in the search of property and seizure of evidence located in New Zealand; in the interviewing of witnesses and targets; and in the collection of other business and official records.

[13] The letter of request stated that evidence was needed in order to further demonstrate that the mega-conspiracy’s directors and employees were aware that Megaupload’s websites were regularly used to reproduce and distribute infringing copies of copyright works, to gain a better understanding of and document the mega-conspiracy’s activities, and to identify additional individuals who were working with the mega-conspiracy. The United States Central Authority requested that two properties of Mr Dotcom be searched at a time when it was known that Mr Dotcom’s

---

<sup>3</sup> Department of Justice of the United States of America.

<sup>4</sup> The Department of Justice is the requesting, and the Attorney-General the receiving, Central Authority.

business associates, Mr Batato and Mr Ortmann, would be present, attending Mr Dotcom's birthday celebration. The property of Mr Van Der Kolk was also to be searched. Law enforcement authorities were asked to seize "all evidence, fruits and instrumentalities of the crime being investigated, including, but not limited to, the following ...". The letter then listed six categories of documents and things that should be seized, and concluded, at page 36:

Please have the seizing officials complete the attached Certificate With Respect to Seized Items and forward the seized articles with the certificate to the appropriate authorities for transmittal to the United States.

[14] On 17 January 2012, the Deputy Solicitor-General, acting with the delegated authority of the Attorney-General,<sup>5</sup> issued an authorisation for the Police to apply for search warrants for the search and seizure of "evidence, fruits and instrumentalities" including but not limited to the six categories of documents and things. The authorisation stated that the relevant offences alleged to have been committed under United States law for the purposes of the warrant were:

Conspiracy to commit racketeering, in violation of title 18 United States Code, Section 1962(d), which carries a maximum penalty of twenty years of imprisonment.

Conspiracy to commit copyright infringement, in violation of Title 18, United States Code, Section 371, which carries a maximum penalty of five years of imprisonment.

Conspiracy to launder monetary instruments, in violation of Title 18, United States Code, Section 1956(h), which carries a maximum penalty of twenty years of imprisonment.

Criminal copyright infringement by distributing a work on a computer network, and aiding and abetting of criminal copyright infringement, in violation of Title 18, United States Code, Sections 2 & 2319, and Title 17, United States Code, Section 506, which carries a maximum penalty of five years of imprisonment.

Criminal copyright infringement by electronic means, and aiding and abetting of criminal copyright infringement, in violation of Title 18, United States Code, Sections 2 & 2319, and Title 17, United States Code, Section 506, which carries a maximum penalty of five years of imprisonment.

---

<sup>5</sup> See: Constitution Act 1986, s 9C.

[15] Crown counsel and legal advisors to the Police appeared before Judge McNaughton in the District Court at North Shore on 18 January. The Judge did not have time to deal with the application for the warrants at that time and it was stood down, the application coming again before the Judge on 19 January 2012. At that time, Detective Sergeant Nigel McMorran swore an affidavit before the Judge which formed the application for search warrant, made under ss 43 and 44 of the MACMA. Those sections provide:

**43 Assistance in obtaining article or thing by search and seizure**

- (1) A foreign country may request the Attorney-General to assist in obtaining an article or thing by search and seizure.
- (2) Where, on receipt of a request made under subsection (1) of this section by a foreign country, the Attorney-General is satisfied—
  - (a) That the request relates to a criminal matter in that foreign country in respect of an offence punishable by imprisonment for a term of 2 years or more; and
  - (b) That there are reasonable grounds for believing that an article or thing relevant to the proceedings is located in New Zealand,—

the Attorney-General may authorise a member of the Police, in writing, to apply to a District Court Judge for a search warrant in accordance with section 44 of this Act.

**44 Search warrants**

- (1) Any District Court Judge who, on an application in writing made on oath, is satisfied that there are reasonable grounds for believing that there is in or on any place or thing—
  - (a) Any thing upon or in respect of which any offence under the law of a foreign country punishable by imprisonment for a term of 2 years or more has been, or is suspected of having been, committed; or
  - (b) Any thing which there are reasonable grounds for believing will be evidence as to the commission of any such offence; or
  - (c) Any thing which there are reasonable grounds for believing is intended to be used for the purpose of committing any such offence—

may issue a search warrant in respect of that thing.

- (2) An application for a warrant under subsection (1) of this section may be made only by a member of the Police authorised under section 43(2) of this Act.

...

[16] The application repeated much of the material in the United States Central Authority's letter of request, but no mention was made in the body of Detective Sergeant McMorran's affidavit that the seized items were to be sent to the FBI in the United States. The letter of request referring to that fact was, however, attached as an exhibit to the affidavit. The memorandum filed in support of the application for the warrants did not address the issue of what was to be done with the items seized. For reasons not explained in the affidavits filed in this proceeding, warrants were sought only in respect of the suspected breach of copyright and money laundering offending, and were not sought in respect of conspiracy to commit copyright infringement, conspiracy to commit racketeering or conspiracy to money launder.

[17] Warrants were issued in respect of the three addresses for which the request was made. The warrants authorised search and seizure of items pursuant to s 44(1)(a) and (b), but not s 44(1)(c).

[18] Each warrant was issued in the following form:<sup>6</sup>

To: Every Constable

(or to \_\_\_\_\_, constable)

**I am satisfied** on an application

(in writing made on oath/affirmation)

...

**THAT** there is reasonable ground for believing that there is (are) in any building, aircraft, carriage, vehicle, box, receptacle, premises or place situated at [the address], the following thing(s), namely:

As per Appendix "A"

---

<sup>6</sup> With minor immaterial variations.

(upon or in respect of which an offence of Breach of Copy Right and Money Laundering has been or is suspected of having been committed)

(or which there is reasonable ground to believe will be evidence as to the commission of an offence of Breach of Copy Right and Money Laundering)

...

**THIS IS TO AUTHORISE YOU** at any time or times within 14 days from the date of this warrant to enter and search the said building, aircraft, carriage, vehicle, box, receptacle, premises or place situated at [address], with such assistants as may be necessary, and if necessary to use force for making entry, whether by breaking open doors or otherwise, and also to break open the box (receptacle) (any box or receptacle therein or thereon) by force if necessary; and also to seize:

(any thing upon or in respect of which the offence has been or is suspected of having been committed)

(or any thing which there is reasonable ground to believe will be evidence as to the commission of the offence)

...

**DATED at Auckland** this 19<sup>th</sup> day of January 2012.

[19] Appendix A attached to each of the warrants read as follows:

All evidence, fruits, and instrumentalities of the crimes being investigated including, but not limited to, the following:

- Indicia of occupancy or residence in, and/or ownership of, the property;
- All documents and things in whatever form relating to the reproduction and distribution of copyrighted works, including, but not limited to, motion pictures, television programs, musical recordings, electronic books, images, video games, and other computer software;
- All records and things in whatever form, including communications, relating to the activities of the Mega Conspiracy, including, but not limited to, Megaupload, Megavideo, and Megastuff Limited;
- All bank records, deposit slips, withdrawal slips, cheques, money orders, wire transfer records, invoices, purchase orders, ledgers, and receipts;
- All documents that reference shipments, imports, exports, customs or seizures;
- All digital devices, including electronic devices capable of storing and/or processing data in digital form, including, but not limited to;

- Central processing units;
- Rack-mounted, desktop, laptop, or notebook computers;
- Web servers;
- Personal digital assistants;
- Wireless communication devices, such as telephone paging devices;
- Beepers;
- Mobile telephones;
- Peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media;
- Related communication devices, such as modems, routers, cables, and connections;
- Storage media, including external hard drives, universal serial bus (“USB”) drives, and compact discs;
- Security devices.

*Execution of warrants and items seized*

[20] The warrants were executed on 20 January 2012. In an affidavit filed in this proceeding the officer in charge of the operation, Detective Inspector Grant Wormald, describes how all police involved in the search received briefings as to the nature of the case before that search. The briefings included what was evidence and what was likely to contain evidence relevant to the proceedings in the United States. The additional staff called upon to assist were also fully briefed, either in the days leading up to or on the morning of the execution of the search warrant.

[21] Once on site Detective Inspector Wormald relied on the expertise of the Police Electronic Crime Laboratory (“ECL”) staff to determine which items would be required and were relevant in terms of the search warrant. He said that Police protocol for dealing with electronic items dictates that electronic items seized under warrant are not to be examined by the searchers because of the risk the data will be lost or altered and the integrity of the exhibit thereby harmed. The protocol necessitates that items specified in the warrant, in this case essentially all of the data

storage devices, had to be seized so the content could be forensically examined offsite, under forensically sound conditions and by appropriately qualified staff.

[22] He describes the approach when seizing items. Documentary items were primarily seized at the scene on the basis they might contain relevant information for the investigators and therefore evidence. He continues:

Similarly to computers and electronic storage devices it is all but impossible to interrogate the significance of a document at a scene with certainty, thus in practice those deemed to be covered by the search warrant are seized for closer inspection by those investigators able to make the final determination.

[23] Detective Inspector Wormald said that although the Police were able to decide what documents and digital storage devices should be seized on the basis that they might contain relevant information for the United States investigators, the Police had and have no request from the Central Authority to proceed to assess those things for relevance. In this case, the assessment for relevance will have to be done by the United States authorities, as they are the investigators. The Police are not in a position to undertake that assessment. It was also his understanding and instruction in planning the operation, that the Attorney-General would direct that the items seized pursuant to the warrants would immediately be sent to the United States to be forensically processed and examined there. The digital items were not to be examined in New Zealand.

[24] Detective Inspector Wormald was aware that Mr Dotcom employed several domestic staff, some of whom lived on either of his two properties. He was aware that the applications for the warrants did not set out proposed conditions as to how to deal with the property of third parties or other irrelevant items, but he believed there was no requirement that they do so. In his experience no search warrant application made domestically (save for a search warrant to be executed in a lawyer's office) would set out any such conditions.

[25] In an affidavit filed in this proceeding Mr Allan Langille, the Supervisor of Digital Forensics at ECL confirms that ECL has not analysed any of the devices. He is however, able to estimate that 150 terabytes of data has been seized. It is common ground that a large number of digital storage devices and a very large volume of data

has been seized. Mr Langille says that the ECL does not have the capacity to undertake the imaging, storage and analysis of the amount of data seized during the investigation without expending a considerable amount of money to employ staff, purchase analysis equipment and for storage of the forensic images.

[26] Mr Thomas Song, Deputy Director of the United States Department of Justice, Criminal Division Cybercrime Laboratories has also filed an affidavit in which he says that he has been told by FBI agents that some of the digital storage devices contain encrypted drives or volumes. The plaintiffs have not provided the passwords to enable that material to be easily accessed. He says that it is essential that the Department of Justice's Cybercrime laboratory maintain custody and control of the original digital evidence to preserve its integrity. This will avoid the necessity for a technical expert from New Zealand to travel to the United States to testify at trial. He continues:

In addition, this is necessary, in part, because by the time the criminal matter goes to trial, new issues may have arisen, often due to arguments raised by the defence, which would require searching the electronics with different keywords and topics.

(ii) ***Judicial review of search warrants issued under the MACMA***

[27] Since *Entick v Carrington*<sup>7</sup> the Courts have been prepared to review the issue and execution of warrants where their legality is challenged. The fundamental duty of the Courts is to uphold the rule of law. In this context the Court's role is to ensure that those who wield the powers of State do so in compliance with the law.

[28] A search warrant authorises a significant invasion of privacy and interference with the exercise of property rights. Section 21 of the New Zealand Bill of Rights Act 1990 provides:

Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

---

<sup>7</sup> *Entick v Carrington* (1765) 19 St Tr 1029.

Intrusions upon the privacy and property rights of individuals must have a proper legal basis. A search warrant is a document evidencing judicial authority to search. For this reason the Courts have insisted that warrants be drawn so as to make clear the precise parameters of the authority to intrude upon those rights. Thus in *Tranz Rail Ltd v Wellington District Court* the Court of Appeal said:<sup>8</sup>

For centuries the law has set its face against general warrants and held them to be invalid. Entry onto or into premises pursuant to an invalid warrant is unlawful and a trespass: *Leach v Money* (1765) 19 State Tr 1002; *Chic Fashions (West Wales) Ltd v Jones* [1968] 2 QB 299; and *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728 at p 733 per McCarthy P. A general warrant in this context is a warrant which does not describe the parameters of the warrant, either as to subject-matter or location, with enough specificity.

[29] It is not every defect in a search warrant that will justify the grant of relief on judicial review. A Court is unlikely to grant relief where the defect is of a minor or technical nature. The applicants have to show that the defect is fundamental,<sup>9</sup> but general warrants are fundamentally deficient. If a warrant is invalid then any search and seizure undertaken in reliance upon it is unauthorised and therefore illegal.

[30] For the first defendant reliance is placed on dicta of the Court of Appeal in *Gill v Attorney-General*<sup>10</sup> to support the submission that judicial review is an exceptional remedy and that the Courts are reluctant to review the legality of the issue and execution of warrants. This is said to be particularly so when an investigation into alleged criminal offending is at an early stage, as is the case here, and particularly where other remedies are available to the subject of the search, including the ability to have any evidence excluded under s 30 of the Evidence Act 2006.

[31] Mr Pike for the New Zealand Central Authority takes this submission further. He submits that the current litigation is a collateral attack on the search warrant process because there is no criminal process in train in New Zealand; the relevant trial process has commenced in the requesting state with the filing of indictments.

---

<sup>8</sup> *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 at 793.

<sup>9</sup> *Gill v Attorney-General* [2010] NZCA 468, [2011] 1 NZLR 433 at [16] – [29].

<sup>10</sup> *Ibid.*

Although he concedes that the New Zealand courts can review the legality of the warrants and their execution, the purpose of the MACMA process and the underlying international legal principles should inform the approach to that challenge. He submits that, just as was observed in *Gill*, where the challenge is based on questions that in a criminal setting would go to admissibility, the question must be whether those matters are better and more appropriately resolved by the trial court; in this case, the trial court of the requesting state.

[32] The point that the purposes of the MACMA regime must be taken into account when considering its provisions is well made. Underlying the MACMA regime is the concept of international comity, and also the expectation that assistance provided by the Police will be reciprocated when required. The international background to the MACMA is the Harare Scheme (a Commonwealth mutual assistance regime) and the United Nations Model Treaty on Mutual Assistance in Criminal Matters (adopted by General Assembly Resolution 45/117 of 14 December 1990). In *Solicitor General v Bujak*<sup>11</sup> the Court of Appeal discussed the implications of the MACMA as follows:

[25] The MACMA's enactment to implement the Treaty recalls an observation in *Avowal* at [21]:

A regime of obstruction has been replaced by one containing a large element of cross-border cooperation.

As was stated in *A Ltd v Director of the Serious Fraud Office* HC AK CIV-2005-404-6833 28 March 2007 at [113]:

... New Zealand accepts responsibility as a member of the world community to promote and maintain the rule of law internationally.

The MACMA is to be construed and applied in that light.

[33] The obligations of cross-border co-operation do not of course require a hands-off approach from the courts, and the MACMA regime only contemplates the provision of assistance permitted by our domestic laws. It would not be consistent

---

<sup>11</sup> *Solicitor General v Bujak* [2008] NZCA 334.

with the object of promoting the rule of law internationally, were the domestic courts to refuse to review the lawfulness of warrants obtained under the MACMA regime.

[34] It is also significant that the New Zealand Parliament chose to model the provisions relating to the issue of search warrants on other domestic statutory provisions relating to the issue of search warrants including s 198 of the Summary Proceedings Act 1957. In *R v Bujak* the Court of Appeal was addressing different provisions in the MACMA, but the reasoning in the following passage applies with equal force in this case:<sup>12</sup>

In short, in a general way the New Zealand Parliament elected to give as much assistance in New Zealand to overseas law enforcement agencies as it would to New Zealand authorities, but no more. For it would be a rather odd result if a foreign law enforcement agency could get more by way of pre-conviction relief here than would be had by a New Zealand agency.

[35] The domestic courts are best placed to determine compliance with domestic laws, and for these plaintiffs there is no alternative remedy in New Zealand for any invalidity and illegality involved in the search and seizure process. If having conducted a review, it is determined that there was a fundamental defect in the warrant, it is difficult to see why a Court should decline to declare as much, even where trial processes are engaged in another jurisdiction. The issue of the engagement of criminal trial process counts, if it counts, at the point of time of determining what relief should be granted. As to the first defendant's reliance on *Gill*, that case was concerned with very different facts. Judicial observations that there is something exceptional about the availability of judicial review need to be viewed within the particular context in which they arise. Where genuine (non technical) grounds for review are made out, it will be the refusal of relief (even if only in the form of a declaration) that is the exceptional course, rather than the reverse.<sup>13</sup>

---

<sup>12</sup> *R v Bujak* [2007] NZCA 347 at [47].

<sup>13</sup> *Tranz Rail Ltd v Wellington District Court* at [45].

*(iii) Is the offence adequately described in the warrants?*

[36] It is logical to start with the statutory requirements as to the form and content of a MACMA warrant. Those particulars are set out in s 45:

**45 Form and content of search warrant**

- (1) Every warrant issued under section 44 of this Act shall be in the prescribed form.
- (2) Every warrant issued under section 44 of this Act shall be directed to any member of the Police by name, or to any class of members of the Police specified in the warrant, or generally to every member of the Police.
- (3) Every warrant issued under section 44 of this Act shall be subject to such special conditions (if any) as the District Court Judge may specify in the warrant.
- (4) Every warrant issued under section 44 of this Act shall contain the following particulars:
  - (a) The place or thing that may be searched pursuant to the warrant:
  - (b) The offence or offences in respect of which the warrant is issued:
  - (c) A description of the articles or things that are authorised to be seized:
  - (d) The period during which the warrant may be executed, being a period not exceeding 14 days from the date of issue:
  - (e) Any conditions specified by the Judge pursuant to subsection (3) of this section.

[37] The prescribed form referred to is form 5 in the Schedule to the Mutual Assistance in Criminal Matters Regulations 1993. It requires that the country under whose laws the offence is alleged to have been committed be stipulated.

[38] As s 45(4)(b) provides, any warrant issued must relate to the particular offence or offences in respect of which it was sought. When ss 44 and 45 are read together, it is clear that the authority to search and seize conferred by the warrant must also be so limited. In the absence of detail limiting the warrant in this way, the

warrant is a general warrant. The MACMA does not authorise the issue of general warrants, and as previously noted, the law “sets its face against them.”<sup>14</sup>

[39] Here, the critical detail in the warrants related to the allegation of breach of copyright offending. It is common ground that the money laundering offence alleged was contingent upon the breach of copyright, and flowed from it. Without proper definition as to the primary offence, there could be little definition as to what was relevant to that secondary offence of money laundering.

[40] As is properly conceded by Mr Ruffin for the Police, there are deficiencies in the description of the offences in this case. The warrants do not stipulate that the offences of breach of copyright and money laundering are offences under the law of the United States of America, nor that they are punishable by a sentence of imprisonment of two years or more. They do not refer to any statutory provision to enable the subject of the warrant to understand the nature of the offences referred to. The failure to refer to the laws of the United States on the face of the warrants, would no doubt have caused confusion to the subjects of the searches. They would likely read the warrants as authorising a search for evidence of offences as defined by New Zealand’s law. The only clue that they are not is that each warrant is headed “The Mutual Assistance in Criminal Matters Act 1992”. That is not much of a clue.

[41] Mr Davison does not argue that these deficiencies on their own render the warrants invalid, but rather that they contribute to the lack of precision infecting the entirety of the warrants. He says that in describing the offence simply as breach of copyright, without stipulating the country in which the offence was alleged to have been committed, or the nature of the alleged breach of copyright, the warrant provided inadequate definition of the offence. A necessary consequence of that was that it also provided inadequate definition of what could be searched for. Copyright can exist in many things. A breach of copyright can be effected in many ways. These were general warrants both in form and reality.

---

<sup>14</sup> *Tranz Rail Ltd v Wellington District Court* at [38], above n 7.

[42] In *Auckland Medical Aid Trust v Taylor*,<sup>15</sup> a warrant was classified as general where it stipulated the offence as “abortion” rather than specifying a particular instance of illegal termination of pregnancy.<sup>16</sup> McCarthy P said:<sup>17</sup>

If then a warrant can only be issued following information relating to a particular offence and in respect of that offence, one would expect to see in the warrant particulars which indicate the offence with sufficient particularity at least to enable the officer executing it and the person in respect of whose premises it is issued to know what the offence is.

[43] After discussing the inadequacy of the description of the offence, McCarthy P went on to say of the applicant police officer:<sup>18</sup>

... what he wanted and what he thought he got, was a general warrant to search for evidence of any of the offences covered by ss 182 to 186 of the Crimes Act. In my view, it would be contrary to the role which the Courts of our tradition have always adopted of protecting the integrity of a man's premises and of viewing in a conservative way the extension of statutory powers to interfere with privacy, if we were to uphold the warrant in this case.

[44] The warrant must be framed with as much specificity as the relevant context permits.<sup>19</sup> Detail of the specific offence is important because it is a requirement of the statutory scheme. It is a requirement of the statutory scheme because it defines the extent of the authority to search and seize. It informs the person or persons searching of the parameters of the Police’s authority to search and seize goods. It also provides the subject of the search with enough information to enable the subject to obtain legal advice about the permitted limits of that search. For this reason s 47 of the MACMA requires that the police officer executing the warrant issued under s 44 have the warrant with him or her, and produce it on initial entry and at any subsequent time.

---

<sup>15</sup> *Auckland Medical Aid Trust v Taylor and Ors* [1975] 1 NZLR 728.

<sup>16</sup> A point taken on appeal was that there was no such offence as “abortion”, the type of offence referred to was “procuring an abortion”. However the Court said that a misdescription of that type in the warrant, provided it would not mislead anyone, was a defect or irregularity of form which did not invalidate the warrant. A much more fundamental error was the failure to stipulate the particular offence or offences rather than simply the type of offence.

<sup>17</sup> At 736.

<sup>18</sup> At 737.

<sup>19</sup> *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 (CA) at [75].

[45] I agree with the plaintiffs that the words “breach of copyright” do not comply with the requirements of the Act or those of the regulations. They describe the type of offence, and then do so inaccurately. They provide no detail as to the particular offence or offences. The requirement imposed by s 45 is not to describe the type of offence, but rather *the* offence or offences in respect of which the warrant was sought and obtained.

[46] Copyright may be breached in a multiplicity of ways, and a breach of copyright may involve a multiplicity of media. The warrant authorised the Police to search for any offence of breach of copyright. Because warrants should be construed as a whole, I have considered what other material there is that might assist in defining the offence.<sup>20</sup> Although close inspection of Appendix A reveals clues that the suspected breach or breaches of copyright involved the use of electronic media, that was neither a necessary nor obvious conclusion. Particularly since there were contraindications in the list such as the item “All documents that reference shipments, imports, exports, customs or seizures”. In any case the subject of the warrant should not be left to attempt to guess the purposes of the warrant through deductive reasoning. It should be spelt out plainly in the required part. And to say a breach of copyright involves the use of electronic media scarcely limits the field.

[47] There is evidence in this case that greater specificity was immediately to hand in relation to the suspected breached of copyright and could have been provided. The terms of the authorisation to apply for search warrant addressed to Detective Sergeant McMorran described the breach of copyright offending in the following way:

Criminal copyright infringement by distributing a work on a computer network, and aiding and abetting of criminal copyright infringement, in violation of Title 18, United States Code, Sections 2 and 2319, and Title 17, United States Code, Section 506, which carries a maximum penalty of five years of imprisonment.

Criminal copyright infringement by electronic means, and aiding and abetting of criminal copyright infringement, in violation of Title 18, United

---

<sup>20</sup> *Rural Timber Ltd v Hughes* [1989] 3 NZLR 178; *R v Sanders* [1994] 3 NZLR 450, 454.

States Code, Sections 2 and 2319, and Title 17, United States Code, Section 506, which carries a maximum penalty of five years of imprisonment.

[48] I am inclined to think that even that level of detail fell short of what could and should have been provided, lacking as it did reference to the involvement of the Megaupload business in the alleged offending. There is reference to the “mega-conspiracy” in the appendix, but because there is no description or definition of what that was, the reference adds to, rather than removes the confusion.

[49] To conclude on this point, the warrants did not adequately describe the offences to which they related. Indeed they fell well short of that. They were general warrants, and as such, are invalid.

[50] Before I leave this topic, there is one further peculiarity about the form in which the warrants were sought and issued which I record: the applications did not extend to racketeering, or to conspiracy to commit copyright infringement. It included money laundering rather than conspiracy to commit money laundering. The Police were authorised to apply for a warrant in relation to the five listed offences and Appendix A list was linked by the United States Central Authority to those offences. It is perhaps understandable why an application was not made in respect of “racketeering” as the evidence would likely be the same as for the other offences, and there may have been a concern that racketeering is an offence unfamiliar to a New Zealand Judge. But the allegation of conspiracy brought in to the mix inchoate offending, which the allegation of breach of copyright and money laundering did not. Appendix A was clearly framed in light of that additional level of offending, referring as it does to evidence of the mega-conspiracy. However, since this aspect of the application and warrant was not explored in argument, and was in any event not likely to be determinative, I put it to one side for the purposes of this judgment.

*(iv) Was there adequate definition of the authority to search and seize?*

[51] As outlined above, the adequacy of the definition of the scope of the search is not capable of separation from the issue of specificity as to the definition of the offence. If there is inadequate specificity as to the offending to which the warrant

relates, it is likely that there is inadequate specificity as to the extent of the authority bestowed by it to search and seize items. Nevertheless, there are some particular points raised by the plaintiffs that relate to Appendix A that need to be addressed separately.

[52] The plaintiffs note that the warrant commences with the statement that the issuing judicial officer is satisfied that there are reasonable grounds for believing that the items listed in Appendix A in effect, fall within either s 44(1)(a) or (b). They argue that the warrant therefore authorised the seizure of the Appendix A items and that the categories in Appendix A were so broadly drawn that it was inevitable that the Police would seize irrelevant documents and irrelevant digital files, the latter stored within the hard drives of the digital devices.

[53] For the defendant, Mr Ruffin says that the categories stipulated in Appendix A are limited by the fact that the warrant only authorised the seizure of “anything upon or in respect of which the offence has been or is suspected of having been committed (or anything which there is reasonable ground to believe will be evidence as to the commission of the offence)”.

[54] Again, the starting point is the MACMA. The warrants could only lawfully authorise seizure of items to the extent allowed under the MACMA. Section 46 describes the powers conferred by the warrant, and s 46(1)(d) provides that subject to any special conditions specified in the warrant, every warrant issued under s 44 authorises the Police to search for and seize anything referred to in s 44(1).

[55] I accept the plaintiffs’ submission that even when each of the warrants is construed as a whole, their form is such that they would most likely be read as authorising the seizure of all of the items in Appendix A. This is because the issuing Judge has expressed himself as satisfied that “all” of the items within the second to sixth listed bullet points in the appendix fall within s 44(1)(a) or (b).

[56] The issuing judge could not have been satisfied that there were reasonable grounds for suspecting that *all* of the things listed in Appendix A were evidence of breach of copyright or the related money laundering, when those categories were so

broadly drawn. For example, had he turned his mind to it, he would have identified that the digital devices listed in Appendix A would most likely store some irrelevant material, probably a large volume of irrelevant material, since the warrants were to be executed at domestic properties. He might also have identified the real possibility that not all of the accounting material or shipping documents would be relevant.

[57] Mr Davison makes an additional point in relation to the following item in Appendix A:

All records and things in whatever form, including communications, relating to the activities of the Mega Conspiracy, including but not limited to, Megaupload, Megavideo and Megastuff Limited.

[58] He submits that because of the inclusion of the expression “Mega Conspiracy” in this item, its meaning is obscure. I accept his submission that without definition of the “Mega Conspiracy” it is hard to imagine what falls within this category.

[59] Mr Ruffin would have been on stronger ground with his arguments if Appendix A had simply listed categories coherently described within which items of evidence might exist. That would have clearly cast the onus upon the Police to undertake the sorting and sifting exercise that would be expected. Appendix A is not, however, drafted in that way.

[60] I have reflected upon whether this is an overly technical construction of the warrants. I do not think that it is, and indeed the evidence suggests that the Police sought warrants that authorised the seizure of entire categories of items because of the methodology they had settled upon for complying with the request for assistance. It is clear from the evidence of Detective Inspector Wormald that it was the intention of the Police to seek warrants that authorised the seizure of anything that might possibly be relevant, in the knowledge that irrelevant material would be caught up in the net that was cast. As Detective Inspector Wormald explained, the Police needed to seize such broad categories of items because the Police were not able to assess relevance, and indeed had no request to do so. That would have to be done by the FBI and the FBI would do that offshore. Seizing the categories of items was the assistance which the Police were requested to provide.

[61] The Police clearly believed that they had obtained a warrant that authorised this approach, and one can understand the operational imperatives that drove this, given the need to leave the ultimate determination of relevance to the FBI. There were ways around this however, and operational difficulties cannot expand the scope of the authority it was possible to confer on the Police under ss 44, 45 and 46 of the MACMA.

[62] It is also argued that the seizure of all digital devices was authorised because they were devices on which the offence had been committed. Special Agent Poston refers to the significance of electronic fingerprints on the electronic devices. That could justify retention of the hardware involved in a digital storage device but not the irrelevant digital information contained on it. These digital devices were to be taken from residential properties. In this day and age computers (and even phones) are used by individuals and families to store a wide range of material and information, family photos and films; personal correspondence (emails) and generally information of a private and purely personal nature.

[63] It is true, as Detective Inspector Wormald identifies, that a practice has grown up of police taking away from a search site material for the purposes of undertaking a sorting exercise offsite to separate the relevant from the irrelevant, and, given that approach, it is inevitable that some irrelevant material will be taken from the search site. The practice that Detective Inspector Wormald describes has been the subject of judicial consideration in the past. A review of the cases reveals, as one would expect, that this is a practice which has parameters.

[64] In *A Firm of Solicitors v District Court at Auckland*<sup>21</sup> the Court of Appeal addressed two conflicting English authorities which dealt with the extent of the authority of police officers to take from a search site material for the purpose of offsite sorting of relevant from the irrelevant. In *Reynolds v Commissioner of Police of the Metropolis*<sup>22</sup> the English Court of Appeal held that a warrant issued under the Forgery Act 1913 (UK) could not authorise the police officer executing it to

---

<sup>21</sup> *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586.

<sup>22</sup> *Reynolds v Commissioner of Police of the Metropolis* [1985] QB 881, [1984] 3 All ER 649 (CA).

indiscriminately remove from premises every book, file, bundle or document he could lay his hands on, even for the purpose of temporary sorting. Removing material, even for the purpose of sifting offsite, was a seizure. But the officer executing the warrant was entitled to remove from premises files, books, bundles or documents which, at the time of removal, he reasonably believed contained forged material or material which might otherwise be of evidential value. If that occurred, any subsequent sorting process had to be carried out expeditiously, with non-evidential material being returned promptly.

[65] The conflicting authority the Court of Appeal considered is *R v Chesterfield Justices, ex p Bramley*.<sup>23</sup> In that case, Kennedy LJ limited the application of the principles enunciated in *Reynolds* to the specific legislation. He accepted the approach described in *Reynolds* was a common-sense answer to the situation faced by an officer executing a warrant, when dealing with a large volume of material. However, the practice of offsite sorting could not be authorised by a statutory provision which permits the person executing the warrant to seize only items which he or she reasonably believes are evidence in relation to an offence under investigation. Where seizure involves items which do not fit within those categories, unless the consent of the owner of the premises is obtained, the person executing the warrant would have no defence to an action for trespass to goods based on unjustified seizure of the material.

[66] In *A Firm of Solicitors* one of the issues for the New Zealand Court of Appeal was whether Serious Fraud Officers were justified in removing computer drives from a law office, cloning them for the purpose of offsite sorting of relevant material from irrelevant and then returning the originals. The clones were sealed by an independent computer expert pending resolution of privilege claims. The Court of Appeal said:

[95] While *Reynolds* and *Bramley* dealt with different statutory provisions, we do not find the reason given in *Bramley* for distinguishing *Reynolds* particularly convincing. To the extent that the existence of a “quick and effective remedy” may be relevant, it could be argued that, at least in so far as privilege is concerned, there is a quick procedure in the SFO Act in s 24(5) for the resolution of disputes relating to privilege, which could be seen

---

<sup>23</sup> *R v Chesterfield Justices, ex p Bramley* [2000] QB 576; at 588.

as having some features in common with that applying under the Forgery Act which applied in the *Reynolds* case. However, s 24(5) does not deal with the problem which would arise where the material seized includes irrelevant material.

[96] If the approach taken by the majority in *Bramley* were followed in this case, it could be argued that an SFO officer executing a search warrant issued under s 12 could never remove from the searched premises a computer hard drive containing data other than data which was relevant to the investigation, or privileged material. Nor would cloning of such a computer hard drive on site, followed by removal of the clone, ever be permitted. We do not consider that to be the law in New Zealand, at least in the context of the SFO Act. We did not hear argument about the position applying to searches made under other New Zealand statutes and express no view on those other statutory provisions.

[97] To the extent that the judgment of the majority in *Bramley* and the judgment of Slade LJ in *Reynolds* conflict, we prefer the latter. The approach suggested by Slade LJ in *Reynolds* represents a reasonable balance between the competing interests of respect for privacy rights and effective law enforcement in cases involving large amounts of documentary material or computer data.

[67] Mr Ruffin submits that cases such as *A Firm of Solicitors* should be limited to their particular facts, and submits it is significant that they were cases concerned with the protection of legal privilege. I do not consider the principles described there should be so limited in their application. Ultimately what was at issue in that case, and what is at issue here, is the scope of statutory authority to search and seize. The Court in *A Firm of Solicitors* expressly addressed itself to the issue of non-privileged but irrelevant material in [95], because the statute under investigation provided the statutory scheme to deal with privileged material. I also note that *Reynolds*, the reasoning of which was adopted by the Court of Appeal, was a case concerned with a search of the plaintiff's home.

[68] Assuming then that the Police were operating under a valid warrant, what were the Police entitled to do in this case? They were required to conduct a preliminary sorting exercise at the premises, as the warrants could not authorise an officer to removed from the premises indiscriminately all documents and records. In this case the Police faced the additional difficulty that they were not the investigating officers and had limited knowledge of the operation. Although this is not a point taken by the plaintiffs (and therefore is not a point which I attach weight to in this judgment) the Police would have had limited ability to do this sorting. Given the

state of knowledge of the Police, it would have been a proper approach for them to involve officers from the FBI in this exercise. Section 46(1) authorises the use by police of “such assistants as may be reasonable in the circumstances for the purpose of the entry and search”. Because the assistants would have been foreign law enforcement officials it may have been prudent to have them as named assistants in the warrants authorising the search.

[69] Providing the Police act reasonably in so doing, following the initial sorting exercise, they were then entitled to remove from the premises those things which at the time they reasonably believed contained material which might be of evidential value. This included the digital storage devices enclosed within computers and other electronic devices. Any necessary offsite sorting process in relation to those items removed should then have been carried out promptly and those items which were not found to fall within either of the two categories identified in the warrant should then have been returned promptly to the owner.

[70] The ability to search computer hard drives onsite is of course limited, given the need to preserve the integrity of the contents through the search process. It would have been reasonable for the Police to take the hard drives offsite and clone them. Either the original or the cloned hard drive should then have been returned to the owner (depending upon whether there was any evidential value in the hard drive for which the clone is not an adequate substitute).<sup>24</sup> This approach was necessary because there was no legal basis upon which the Police were entitled to retain material which did not fall within the two categories in s 44(1). It would have been necessary to have the assistance of the FBI in this exercise.

[71] As to what could be retained following this process, the word “evidence” in ss 44 and 46 must be considered, in context, to have a wider meaning than its usual meaning when used in court proceedings. Its meaning in comparable provisions in the equivalent United Kingdom legislation (the Criminal Justice (International Co-

---

<sup>24</sup> This would of course also be subject to the proviso that material which would enable further offending should not be returned. This might be the case in relation to unlawful material which is found on the hard drive.

operation act 1990) was discussed by the English Court of Appeal in *Regina v Secretary of State for the Home Department and Others Ex Parte Fininvest S.p.A and Others*, as follows:<sup>25</sup>

When, therefore, one is speaking of ‘evidence’ in the context of a criminal investigation, the permissible areas of search must inevitably be wider than once that investigation is complete and the prosecution’s concern is rather to prove an already investigated and “instituted offence”.

[72] I would add to that, to fall within s 44(1)(a) or (b) the item must at least be relevant to the investigation. If not that, then there is no meaningful limit to what can be seized. This construction is consistent with the fact that the trigger for the authorisation for a search warrant under s 43 is the Attorney-General’s satisfaction that there are reasonable grounds for believing that an article or thing relevant to the foreign country’s criminal proceeding is located in New Zealand.

[73] The *Ex Parte Fininvest* case is an example of the type of approach that could have been employed by the Police in this case to both meet the operational difficulties they faced and comply with the domestic statutory framework. In *Fininvest* the applicants for judicial review were alleged by Italian authorities to be involved in a very large scale fraud. A request for assistance was received from the Italians, sent under the provisions of the United Kingdom Criminal Justice (International Co-operation) Act 1990. The request was that a search be undertaken for specified documents. A search warrant was duly obtained. Named Italian investigators were permitted to accompany any police constable executing the warrant so they could advise whether documents fell within the terms of the warrant. Documents were removed from the search site and examined, in the United Kingdom, by the Italian authorities to determine which were relevant and which were required for transmission to Italy. Some were returned to the applicants. Some were sent to the Home Secretary. None were transmitted to Italy pending the hearing of the application for judicial review.

---

<sup>25</sup> *Regina v Secretary of State for the Home Department and Others Ex Parte Fininvest S.p.A and Others* [1997] 1 WLR 743 at 752.

[74] One of the grounds of judicial review in the proceeding was that the warrant was impermissibly wide, and amounted to a fishing expedition. In finding the warrant valid Simon Brown LJ said:<sup>26</sup>

In short, the request for assistance here is not, as the applicants contend, vague and speculative; rather it is as precise and focused as such a request could sensibly be in these circumstances. It is impossible to know just what documents are both in London and relevant. To discover that, it is necessary to find, examine and appraise them. Given, however, that these are the type of documents invariably germane to any major company fraud investigation, it is highly likely that many will be relevant. And in so far as any of the documents seized prove not to be, they will not be transmitted to Italy.

[75] The Police here could have had the assistance of the FBI in the initial execution of the warrants. In any event they should have moved promptly through the offsite process permissible when dealing with large quantities of material. The purpose of that sorting is to extract the relevant from the irrelevant, and it seems to me inevitable that the FBI should have been able to assist with that.

[76] Under the provisions of MACMA the United States Central Authority is not entitled to irrelevant material seized during the search. Although Mr Song says the FBI wishes to keep all material against the possibility that some new issues will emerge, issues of relevance must be determined at the time of the search and offsite sorting process. There is no construction of s 46 which would permit the seizure of material which is irrelevant at the time of search against the possibility it subsequently becomes relevant.

[77] To conclude, the warrants were expressed to authorise the search for and seizure of very broad categories of items. These categories of items were defined in such a way that they would inevitably capture both relevant and irrelevant material. The Police acted on this authorisation. The warrants could not authorise seizure of irrelevant material, and are therefore invalid.

---

<sup>26</sup> At 753.

(v) *Should conditions have been imposed?*

[78] Mr Davison argued that the warrants should have contained conditions to deal with the issue of irrelevant material. Mr Ruffin argues that it is only in situations involving significant issues of legal privilege that conditions should be imposed. He refers to *Gill* as supporting the proposition that conditions should not readily be attached to warrants.

[79] I do not consider that *Gill* stands as authority for the proposition that Courts should be reluctant to impose conditions on warrants. The passage in *Gill* which Mr Ruffin relies upon is one in which the Court of Appeal refers with approval to an earlier decision of that Court in *Television New Zealand Ltd v Attorney General*.<sup>27</sup> In *Television New Zealand* the Court of Appeal expressed the need for care in expressing principles applicable to warrants so as not to constrain the necessary discretion of the issuing Judge. In the course of reviewing the issue of the warrant, the first instance Judge had attempted to formulate detailed guidelines for the issue of warrants in relation to media organisations, including a set of standard conditions. On appeal, the Court emphasised that cases vary greatly and that it was inappropriate to go further than identifying general principles to be borne in mind when the reasonableness of granting or executing a warrant was under consideration. The comment relating to the imposition of conditions set out in *Gill* was in response to the suggestion that warrants in connection with media organisations should have, as a matter of course, special conditions attaching. The Court went no further than saying that conditions may be imposed but that they will not be the norm.

[80] Section 45(3) contemplates that special conditions may be imposed in relation to MACMA warrants. It creates a discretion that is to be exercised in the particular circumstances of the case.

[81] In this case I acknowledge that it is a rather academic exercise to consider whether conditions should have been imposed, given the finding that the warrants

---

<sup>27</sup> *Television New Zealand Limited v Attorney-General* [1995] 2 NZLR 641 (CA).

were invalid. But since the issue may be relevant to the grant of relief, I will address it. If the warrants had been adequately specific as to offence and scope of authorised search, it may have been appropriate to impose conditions because those conditions could have addressed just how the offsite sorting exercise was to be undertaken. In considering whether to impose conditions it was relevant for the Judge in this case to weigh the inevitability of an offsite sorting exercise, the likely size of that exercise, and the requirements for cloning the content of the digital storage devices. It was also relevant that there was no information provided in the warrant applications as to when or where the sorting exercise was to take place, or who was to do it. Finally, it was relevant that there was information available to the Judge (although this information was not prominent in the material presented in support of the application) that the Police intended to deliver the items seized to the FBI in the United States.

[82] To achieve an appropriate balance between the investigative needs of the FBI and the right of the plaintiffs to be free from unreasonable search and seizure of their property and correspondence, it may well have been appropriate to impose conditions. The failure to do so meant that the subjects of the warrants were left unsure of their rights in relation to the material taken offsite, and also risked irrelevant material being released to the FBI, beyond the jurisdiction of the New Zealand Courts to order its return.

[83] As to the nature of appropriate conditions, in *A Firm of Solicitors*, a case involving as its name suggests, the search of a firm of solicitors, the Court of Appeal said:<sup>28</sup>

... conditions attaching to Anton Piller orders made in the civil jurisdiction of the High Court may provide some guidance, though there would obviously need to be adaptations to suit the circumstances of the case. It would be necessary to ensure that the cloning exercise, and the subsequent extraction of evidential material, was undertaken by an appropriately qualified and independent expert. It may be that the process should be supervised by the issuing Judge or a person appointed by the issuing Judge for the purpose.

---

<sup>28</sup> At [108].

[84] In this case, however, there is no evidence of significant volumes of privileged material and any conditions needed to reflect the concerns they were intended to address. In any search privileged material may fall within the net. But when a search of a legal office is contemplated, it is a concern that should be at front of mind for the Police and the issuing officer. There is considerable expense involved in some of the procedures contemplated by the Anton Piller procedures. I consider that a less onerous set of conditions would have been appropriate where privileged material was not of particular concern. The conditions should have provided for the cloning exercise and extraction of relevant material, what was to be done with irrelevant material, and whether the plaintiffs were to have returned to them the original hard drives returned, or clones.

[85] As is plain from my earlier comments I also do not consider that the conditions needed to keep from the FBI the content of the hard drives. Indeed, to enable the MACMA regime to achieve its purposes, it seems inevitable that in complex cases the investigating authorities must be engaged in the sorting exercise, which proper execution of the warrant requires.

[86] To conclude on this issue, if the warrants had been adequately specific as to offence and scope of search, it may still have been appropriate for the issuing Judge to impose conditions to address the offsite sorting process that was inevitable in this case. The conditions could have provided for the cloning of hard drives, the extraction of relevant material and the return to the plaintiffs of the original hard drives, or their clones.

**B. Did the Police seize items outside the scope of the search warrant?**

[87] I have held that the warrants were invalid because they were general warrants lacking adequate specificity as to the offence and to the scope of the items to be searched for. Moreover, the warrant authorised the seizure of items falling outside the parameters of s 44(1). Search and seizure pursuant to an invalid warrant involves the Police in a trespass and unauthorised seizure of property.

[88] If I am wrong that the warrants were invalid, then it is nevertheless clear that the Police, in executing the warrants, have exceeded what they could lawfully be authorised to do. This is because they continue to hold, along with the relevant, material they concede will be irrelevant. They have taken few steps to identify that material, and no steps where the material resides on the computer hard drives. The Police say they have no intention of sorting the evidence or potential evidence, from the irrelevant. They intend to allow the FBI to do that in the United States. That is an approach that is not available to them. Section 46 of the MACMA only authorises seizure of items referred to in s 44(1), and it is only things seized under s 44(1) that are amenable to a s 49(2) direction that the items be sent to a foreign investigating authority.

[89] No one addressed the issue of whether the Police conduct also amounted to an unreasonable search and seizure. My preliminary view is that it did, but as I have not heard counsel on this, I make no finding at this point. If the issue requires to be dealt with, it can be dealt with when I hear the parties in relation to relief.

**C. Was the provision by the Police of copies of digital files to the FBI unlawful?**

[90] During the course of the first hearing of this application for review, it emerged that hard drives had been imaged and shipped by the FBI to the United States. The plaintiffs say the shipment of those images was unlawful because it was contrary to the Solicitor-General's direction given under s 49(2) on 16 February 2012 that any items seized were to remain in the custody and control of the Commissioner of Police until further direction.

[91] Section 49 of the MACMA provides:

**49 Custody and disposal of things seized**

- (1) Where any member of the Police seizes any thing pursuant to a warrant issued under section 44 of this Act, that member of the Police shall deliver the thing into the custody of the Commissioner of Police.
- (2) Where a thing is delivered into the custody of the Commissioner of Police under subsection (1) of this section, the Commissioner of Police shall arrange for the thing to be kept for a period not exceeding

1 month from the day on which the thing was seized pending a direction in writing from the Attorney-General as to the manner in which the thing is to be dealt with (which may include a direction that the thing be sent to an appropriate authority of a foreign country).

- (3) Where, before the expiry of the period referred to in subsection (2) of this section, the Attorney-General gives a direction in respect of the thing, the thing shall be dealt with in accordance with the direction.
- (4) If no direction is given by the Attorney-General before the expiry of the period referred to in subsection (2) of this section, the Commissioner of Police shall arrange for the thing to be returned to the person from whose possession it was seized as soon as practicable after that period has expired.

[92] It is common ground that there was no document directing the release of images, signed by the Attorney-General, the Solicitor-General or the Solicitor-General's delegate, and that, at the time the images were sent to the United States, the s 49(2) direction which applied was that of 16 February. Mr Pike for the New Zealand Central Authority argues that s 49(2) is only concerned with physical custody, and, notwithstanding the provision of copies, as the originals remained in the physical custody of the Police, no direction under s 49(2) was required to allow shipment. Alternatively, he argues that any unlawfulness involved was of a technical nature because the plaintiffs had consented to the release of images to the FBI and, in any event, the Deputy Solicitor General would have directed the provision of the images if he had been asked to.

*(i) Does s 49 regulate physical custody of an item only?*

[93] Mr Pike's essential submission for the Central Authority is that neither the language nor the context of s 49 support the argument that all dealings with seized items held by the Commissioner, even those that do not affect legal custody of the original items seized, must be supported by a s 49 "direction". Things seized are kept by the Commissioner pending a written direction. Once a written direction (of the sort dated 16 February 2012) is issued, the things are no longer kept pending direction but rather kept pursuant to the direction issued. That in itself, Mr Pike submits, tells against the construction that access to or other actions relating to the seized things not affecting their physical custody, or their status as items seized pursuant to the MACMA, requires a s 49 "direction".

[94] An interpretation of s 49 that required a direction to authorise each and every dealing with an exhibit whilst it is in the custody of the Commissioner of Police would be inconsistent with the purpose of the MACMA legislation. In executing a search warrant obtained pursuant to a MACMA request, the Police are likely to have to allow foreign law enforcement agencies access to items seized. Consequently, custody is to be given a broad and liberal meaning: if an item seized remains under the control of the Police, it is within their custody.<sup>29</sup> Whether a s 49 direction is required when it is proposed to send to law enforcement agencies overseas an exact replica of the items is a rather more difficult question. The original physical item seized remains in the possession of the Police. However, once a clone of a hard drive is sent offshore, the Police have lost the ability to control what is done with information stored on that hard drive. The same may also be true of copies of the documents involved. The wording of the legislation does not address how replicas (effectively identical twins of the item) fit within this regime.

[95] Fortunately in this case this is not an issue that I have to decide, because a direction under s 49(2) was made. The Commissioner of Police was directed to keep the items in his custody and control. Mr Pike suggested the inclusion of the word “control” in that direction was simply a case of lawyers including a boiler plate type provision and that it could be disregarded. While the basis upon which it would be appropriate to ignore the words of the direction is unclear, it seems in any case that there was some intent behind the particular words used. Ms Madeline Laracy, a solicitor with Crown Law, has filed an affidavit in opposition to the application for review dated 25 May 2012. In that affidavit she says there were two reasons why the Solicitor-General did not direct the items seized be sent offshore immediately. The first was that the Police and Crown Law, representing the Central Authority, were concerned to ensure that there was a register which clearly identified every single item and every document. The second was notification of the proposed filing of judicial review proceedings by Mr Dotcom to challenge the warrant and prevent the computer items leaving the country before arrangements had been made which were satisfactory to preserve the applicant’s ability to access data. It is apparent from the

---

<sup>29</sup> *Rural Timber Ltd v Hughes* [1989] 3 NZLR 178 (CA) at 186.

correspondence on the file that the plaintiffs' were also concerned from an early stage that irrelevant items had been seized. Therefore both challenges as to the legality of the warrants and to the extent of items seized required some resolution.

[96] The hard drives seized contain information in the form of digital files. Those files are part of the relevant hard drive. The information is the property of the plaintiffs, just as much as the private papers were the property of the plaintiff in *Entick v Carrington*. Once clones of the digital files were shipped offshore, the Police no longer had control over what was done with them. They could not, for instance, compel their return, nor prevent the FBI dealing with them as it chose, even if it was subsequently determined that there was any invalidity affecting the warrant, or that items outside the scope of s 46(1)(d) had been seized. The direction that the items remain under the custody *and control* of the Commissioner during the 'sorting out' period was therefore a sensible one. It gave time for some sort of resolution of the various issues to be worked out with the plaintiffs, or time for those issues to be determined by the Courts. The failure to observe the direction, by permitting or allowing the shipments, may have involved an irrevocable seizure of material.

[97] To conclude on this issue, the release of the cloned hard drives to the FBI for shipping to the United States was contrary to the 16 February direction given under s 49(2) of the MACMA that the items seized were to remain in the custody and control of the Commissioner of Police. This dealing with the cloned hard drives was therefore in breach of s 49(3) of the MACMA.

***(ii) Did the plaintiffs consent to images of computer hard drives being shipped to the FBI offshore?***

[98] Extensive affidavit material has been filed in relation to this aspect of the hearing. Most of that affidavit evidence relates to discussions between Crown counsel (who were at the time representing the New Zealand Central Authority), plaintiffs' counsel and the Police concerning the cloning of the hard drives with a view to providing those copies to the FBI and to the plaintiffs.

[99] Mr Pike explained in submissions that this affidavit material was produced because it was understood that allegations of serious misconduct on the part of the Crown had been raised and that as a consequence the Court had directed the filing of evidence. I had not however, directed the filing of evidence. During the first phase of the hearing, in response to a question from me, Mr Ruffin said that images of computer files had been taken by the FBI and sent to the United States of America. Both Mr Davison and Mr Foley expressed surprise at that; Mr Davison noting that an application for interim relief in the present proceedings had been resolved on the basis that all items continued to be held pursuant to the s 49(2) direction of 16 February. I asked Mr Ruffin for clarification and he sought leave to file affidavits from those who had been involved at that earlier stage (including counsel and police). That leave was granted.

[100] At the hearing on 6 June, counsel for the plaintiffs confirmed that, while no allegation of bad-faith was made, it was contended on the plaintiffs' behalf that the transfer of the material offshore had been unlawful, the plaintiffs had not consented to it, and that the plaintiffs had been misled in these present proceedings. The latter because the plaintiffs had withdrawn their applications for interim relief on Mr Ruffin's assurance that the material seized by Police would continue to be held in accordance with the s 49(2) direction of 16 February and that the direction preserved the status quo.

[101] Having reviewed the chronology of events as revealed through the affidavits of the participants and correspondence in Court documents, three phases in the dealings between the parties emerge. The first phase, immediately following the search and seizure, continued through until early March. During that phase, Crown Law negotiated with the plaintiffs with a view to obtaining agreement upon a basis on which all original items could be shipped to the FBI and the Crown could be provided with passwords which would enable the FBI to access the encrypted files.

[102] The second phase of the dealings was one in which it became apparent that no resolution of these wider issues would be able to be reached. During this phase the Crown attempted to settle a basis upon which the Crown could nevertheless

despatch original items to the FBI, setting aside only those in respect of which there was dispute.

[103] During the final phase, which overlapped significantly with the second phase, the plaintiffs' placed before the Court the issues, in one form or another, as to the status of the items seized, and what was to be done with them. Images of the hard drives were sent to the FBI in the United States.

*First phase: Initial attempts at a negotiated resolution as to the status of the items:*

[104] Dealings between the various parties in relation to the items seized began as early as 9 February 2012. They commenced with a letter from Mr Davison to Ms Toohey seeking the urgent return of Mr Dotcom's computer and hard drives to enable him to prepare his case in opposition to any extradition proceedings, and suggesting that the files be cloned in short order. On 10 February 2012, Mr Davison sent a further letter noting the volume of material that had been seized by the Police and the fact that no detailed schedule had yet been provided. He wanted to ensure -

... that none of the items seized by the New Zealand Police are sent out of New Zealand or delivered into the custody or possession of representatives of the US Government unless and until Mr Dotcom has had an opportunity of obtaining and being provided with copies of documents or has his computers returned following the electronic copying (cloning) being undertaken with a view to the US Government retaining such clones as evidence as to the contents of seized computers.

[105] Written assurance was sought that none of the items seized by the Police would be provided to the US Government without proper and adequate notice being provided so that Mr Davison could apply to the Court for an order as to the appropriate disposition or retention of the items.

[106] By letter dated 14 February, Mr Davison wrote again to Ms Toohey advising that, in the absence of any satisfactory arrangements as to the status of the exhibits, his client would apply for judicial review challenging the issue of the search warrant and would also apply for an interim order restraining the Crown and the Police from delivering or giving possession to the US Government of all and any of the search items seized by the Police.

[107] The day after the 16 February direction under s 49(2), Mr Foley wrote to Ms Toohey saying that he had instructions to consider whether to challenge the basis upon which the warrants had been obtained. He said until he had received and had a reasonable opportunity to peruse relevant disclosure in relation to the matter, no material or information should be passed over to the US Government or any other government agency or persons. He recorded his expectation that, as part of the investigation, the Police had sought assistance in imaging/cloning various electronic devices and contained data and asked for advice on how long it would take.

[108] Although there was some intervening toing and froing between the parties, the next significant event in the chronology is a letter from Ms Laracy, Crown counsel, to Mr Davison dated 24 February 2012. In that letter Ms Laracy said that although the evidence was required to be sent to the United States in its original form, that had not yet happened and would not happen without advising the plaintiffs first. She proposed that the Attorney-General direct that all original computer items and other exhibits be sent to the United States in order to effect the purpose of the mutual assistance required. In relation to Mr Dotcom's laptop and his two external hard drives, she proposed that they be promptly cloned and the clones provided to Mr Dotcom. The New Zealand or United States authorities were prepared to bear the cost of that in relation to those specific items in order to reach a position which reasonably satisfied competing interests and to achieve an expeditious resolution of the issues. She said that if Mr Davison was not agreeable to the process, the Crown would urgently seek a directions hearing in the District Court.

[109] She said that it was not proposed to return the original hardware to Mr Dotcom as the United States investigators required to examine that in its original form. United States experts and investigators needed to work in their own laboratory environment to analyse and clone the computer items so that they could be assessed in the same conditions, according to the same processes and standards, and by the same investigators as other computer items relating to the Megastuff conspiracies seized in other locations around the world. She said:

In short, it is not possible in the context of an investigation of this nature for computer items to be cloned in New Zealand and the clones alone sent to the United States. Further, it is not feasible or appropriate for the computer

items to be cloned in New Zealand first and the clones retained. That would unduly impede the United States investigation. It would also put an unreasonable burden on the New Zealand authorities.

[110] She noted Mr Dotcom's intention to file a judicial review of the search warrant by which the computer items and other exhibits were obtained, and said:

We do not see that that indication should impede the items being sent to the United States. We believe the United States may be willing to provide an undertaking regarding prompt return of items if the New Zealand search were ultimately held by our Courts to be an unreasonable search and seizure.

[111] Mr Davison responded by letter dated 29 February 2012. He said that there was an issue as to whether all of the "computer items" seized from Mr Dotcom's property were within the ambit of the items that could be legitimately seized and removed pursuant to the search warrants. He provided examples. He continued:

Accordingly, before any final decision is made relating to the handover of any computer items to the US Government, there will need to be a detailed schedule prepared identifying each and every item that was to be handed over to the US Government representatives ...

[112] He thanked Ms Laracy for her advice that no items had been provided to, or sent to the United States and that she would not make any such arrangements without first advising Mr Davison on behalf of Mr Dotcom. He said:

Given your indication that you will "urgently seek a directions hearing from the District Court" to determine any issue of disagreement between us, I take it that no items whatsoever will be transferred to or handed over to the US Government or its representatives in the absence of either agreement being reached between us that that is an appropriate course or an order of the Court authorising and approving the handing over of such items to the US Government or its representatives.

He asked for confirmation that his understanding was correct.

[113] Discussions continued between Mr Davison, Mr Foley, Ms Laracy and Ms Toohey in relation to the possibility of cloning some items for the purpose of disclosure to the defence. On 6 March 2012, Ms Laracy emailed Mr Foley and Mr Davison making a 'without prejudice' offer to expedite the issues between the parties in relation to the status of the various items seized. She confirmed again that no items of evidence had left New Zealand and that the Crown would advise the

plaintiffs if it was planned that any would. She said, in relation to the few specific computer items sought by the defence, if they could be cloned or copied safely in New Zealand without compromising the integrity of the originals, the Police might be prepared to use the ECL in New Zealand for that purpose. Once those items were copied and once the plaintiffs had the opportunity to check the copies and establish that they were accurate and readable, those and all other computer items in their original form would be sent directly to the United States. All hard copy documents seized would be scanned by the Police onto disc and the disc sent to the United States with hard copies remaining in New Zealand.

[114] Correspondence then ensued, both by email and by letter, about the exact terms such an agreement might contain and as to the methodology to be employed for cloning. On 7 March, Mr Davison proposed that the Crown prepare a draft undertaking for his consideration. On 13 March 2012, Ms Laracy provided a draft “evidence transfer proposal.” The first paragraph of that proposal recorded that no items obtained under the search warrants production orders were to leave New Zealand or to be transferred into the control of the US authorities until the “specific items” had been imaged and readable copies had been acknowledged as received by the respondents. The ‘specific items’ were listed and were items the plaintiffs had requested copies of.

[115] The second paragraph recorded that originals rather than copies of the items seized other than hard copy documentary items, were to be transferred to the US authorities pursuant to the Mutual Assistance request. The specific items would be imaged by an FBI forensic expert who may use the premises of the Electronic Crime Laboratory in Auckland for that purpose. It also provided that any passwords and information necessary for the FBI expert to properly access the specific items would be provided by the relevant plaintiff to Detective Sergeant Nigel McMorran in advance of the imaging. On receipt of the copies, the plaintiffs would have up to five working days from collection of the images of specific items to advise the Crown Law Office in writing that they had received acceptable images of the content of the specific items. After expiry of that period, the transfer of all evidential items might occur.

[116] The draft agreement then recorded that, notwithstanding the previous provisions,

... any items in respect of which there is a live dispute as to whether they fall within the scope of the search warrant will be set aside for further consideration and not transferred to US custody or control until that matter has been resolved by the parties or by a court. Any other exhibits may, however, be transferred to the US Authorities pursuant to the agreement.

[117] On 15 March 2012, Mr Davison wrote to Ms Laracy saying that some items had already been identified as being allegedly outside the scope of the warrant. He said that he proposed to review the updated police exhibit schedule with a view to identifying any further items which Mr Dotcom contended were outside the ambit of the search warrant or which would be readily recognisable as being of no evidential value. He enclosed an amended agreement which included a new clause 12 which, if accepted, would impose upon the New Zealand authorities an obligation to clone all electronic data before handing either the originals or the cloned copies to the US authorities.

*Second phase: No agreement*

[118] On 16 March, Ms Toohey emailed Mr Davison and Mr Foley to say that the amended agreement was not acceptable to the United States because of the size of the imaging task proposed. She acknowledged however, that it was not possible to estimate the size of the task until the FBI had had an opportunity to preview the contents of the electronic items. She suggested, as an interim arrangement, that two FBI investigators would come to New Zealand to prepare two sets of the 17 specified items. They would take one set back to the United States and leave a second set in New Zealand pending resolution. She said agreement on terms remained possible, and asked for further detail of the “live dispute” items.

[119] On 16 March, Mr Davison replied by letter saying he was taking further instructions in respect of the “live dispute” items. He said:

...pending the receipt of further instructions from Mr Dotcom as to what additional “live dispute” items he contends should be added to the existing list and pending the analysis of the materials to be undertaken by the FBI forensic agents, it would appear premature for either party to take a final

position. Notwithstanding, there is utility and good sense to the proposed action of the preparation of two sets of the 17 specified items.

[120] It seems the FBI agents arrived in New Zealand on 18 March. On 21 March 2012, Ms Laracy and Ms Toohey wrote to Mr Davison recording that no agreement had been reached as to the imaging of the specific items and transfer of all items. They recorded that the FBI agents were in New Zealand, and that:

They will make two images of the original 17 “specific items”. The FBI will return to the United States after the imaging, transferring the originals of the specific items at the same time. You will also receive the images of these items at that time. A possible exception to this is the CCTV content which needs to be imaged and assessed by the Police after imaging.

[121] Further on in the letter they said:

We also propose to send the originals of all other computer/digital items to the United States. In the absence of clear idea of categories of information that your client contends is relevant from the items seized under warrant, it is unreasonable to prevent their transfer to the United States. We would like to give you an opportunity to respond in writing on this issue, setting out also the law you rely on, so that your position can be further assessed. We would need to have your response by 4.00 pm on Tuesday, 27 March 2012. If necessary, we intend to seek directions from the Court. This would have to happen urgently.

*Third phase: Status of items seized raised in District Court:*

[122] Later that same day, Mr Foley emailed the Court, and served upon Crown counsel a copy of a memorandum for the District Court in advance of a telephone conference to be held on 22 March. In that memorandum he addressed a number of issues including status of the various items seized and the validity of the warrant. In relation to the imaging of items seized, his memorandum included the following:

2. (a) New Zealand imaging should be undertaken forthwith and working duplicate copies of those images provided to the respondents without delay to allow a check to be made as to whether the image appears to be in working order;
- (b) No device, nor copy of same, should leave New Zealand until the respondents have had reasonable time to review images provided;
- (c) Working images of the balance of all digital items seized to be provided to the respondents no later than 28 April 2012.

[123] Following the conference on 22 March 2012 the Judge issued a minute recording discussion as to the need for imaging in New Zealand of the information contained on the computers. The Judge went on to schedule a hearing in relation to several issues which included:

To consider whether or not directions should be made regarding the imaging of computers seized in the search and [if] so what those directions should be.

[124] Later that same day Mr Davison wrote to Ms Toohey and Ms Laracy. In the letter he referred to a telephone conversation with Ms Toohey in which he had sought written confirmation that, notwithstanding the terms and contents of the letter of 21 March 2012, having regard to the matters traversed before Judge Harvey, and the intended Court hearing, in the absence of any agreement no items seized would be transferred or delivered to the US government and its agents for removal from New Zealand and transfer to the United States pending determination of the issues by the Court. He noted previous discussions and negotiations were directed at the imaging/cloning of specific items, which process would then be followed by an opportunity for his client to be satisfied that the images provided in relation to his own specified items was fully readable by him before the hardware items were transferred or passed to the US Government representatives for removal from New Zealand. In the new proposal, no such opportunity was proposed. He said that, provided it was possible to get back to an arrangement whereby there was an opportunity for the verification of the readability of certain items, he anticipated no difficulty in reaching an agreement that allowed the United States government agents taking originals back with them.

[125] Ms Toohey responded by email at 5.29 pm on the afternoon of 22 March confirming that the original computer equipment would not leave New Zealand pending the decision of the District Court. However, she continued:

FBI agents who are in New Zealand are currently making two sets of images of the specific items. They will take one set of images. The other set will be made available for disclosure. This preserves your position in terms of access to an image and, if necessary, access to the original for the time being.

She went on in her email to say that a copy of the documentary items which the defence already had would be sent to the US authorities for their assessment of

relevance to the investigation. She apologised for the informality of the email but said that she was on leave from the next day and had little time to respond.

[126] Mr Davison did not respond to this email, but Mr Foley did. On 23 March 2012, he sent an email, copied to Mr Davison, to Ms Laracy and Ms Toohey. I set the detail of that out in full:

Thank you for your email, below.

Images

Might you provide copies of images as they become available to allow any checking at our end to proceed without delay?

Documentary items

In my view the police are required to ensure that only items properly seized pursuant to the MACMA warrant are ultimately made available to the US.

I am told a number of items were seized/obtained by the police likely fall outside the warrant or other statutory powers of seizure. Those items should not be provided to the US, or anyone else. They should be returned at an appropriate time.

My indication during His Honour's telephone conference yesterday followed my memorandum for that conference (further copy attached) – that NZ authorities should go through the material to sort out what might be properly given up and what should not.

I do object to the US receiving this material before the items are checked.

As earlier indicated I would wish to take instructions as to the final list of items to be released, and am available to work co-operatively on this issue once the initial sorting exercise is complete.

Please confirm your agreement, and advise whether or not material has already been provided to US authorities. If so would you please identify the material, date of release, and to whom release was made?

He attached to that email a copy of the memorandum filed for the telephone conference the previous day.

[127] It is this email and Mr Davison's failure to respond to Ms Toohey's email, that the Crown relies upon on as evidencing consent on the part of the plaintiffs to the shipment of the copies. In her affidavit filed in this proceeding Ms Laracy notes that Mr Davison did not respond to the email from Ms Toohey, and that Mr Foley, under the heading of "Images", makes no complaint about the proposed course of

action. She says that the rest of the email relates to the heading “Documentary items”.

[128] Detective Sergeant McMorran’s evidence is that shortly after 5.00 pm on 23 March he was told by the FBI they had arranged for “seven hard drives” to be shipped by FedEx to the United States. There is no direct evidence of what Crown Law had communicated to the Detective Sergeant as to whether the FBI could take the images, but his evidence was that “ultimately” his understanding was that the FBI could. He said he made no report of his discussion with the FBI regarding these “seven hard drives”, and from the next day was on leave.

[129] At 5.06 pm on that day Ms Laracy filed a memorandum in the District Court, served on the plaintiffs’ counsel, in which she recorded that the key issues for resolution were:

Duties and entitlements for New Zealand parties in respect of digital/computer items seized under the MACMA warrants for transfer to, and examination by, the United States authorities; ...

[130] At 5.46 pm on 23 March Ms Laracy responded to Mr Foley’s email confirming that no items of evidence had left New Zealand and setting out an email from Detective Sergeant McMorran. In his email Detective Sergeant McMorran concludes:

The FBI are going to be working through the weekend to get all this completed and hope to have everything finalised by next Thursday and are booked to leave New Zealand on the 31<sup>st</sup> March. Prior to leaving they will run the copies to ensure they can be read and then once satisfied they will return a copy and the original to ECL who in turn will hand them back to OFCANZ for storage pending the outcome of the hearing on the 2<sup>nd</sup>-3<sup>rd</sup> April or directed otherwise by the Crown.

[131] Although Ms Laracy’s email, and its enclosure, created a misleading picture as to the status of the evidence, I accept that timing delays explain the inaccuracy of the information she conveyed.

[132] The next relevant step in the chronology is the filing of an application for orders relating to items seized under the MACMA warrant. This was filed by

Mr Foley on 26 March 2012, and picks up the text of the original memorandum filed by Mr Foley. The first order he sought was as follows:

That in relation to seizure under warrant or otherwise of files or items containing, or capable of containing electronically stored information:

- (a) Imaging of those devices is to be undertaken forthwith and working duplicate copies of those images provided to the applicants without delay to allow checks to be made as to whether the image appears to be in working order;
- (b) That no device, nor copy of the same, is to leave New Zealand until the applicants have had a reasonable time to review images provided and have confirmed and responded in writing that they are able to use the images;
- (c) That the respondent obtain an undertaking from the US authorities that working images of the balance of all digital items seized are to be provided to the applicants no later than 28 April 2012.

[133] It was after this application was filed that the second instalment of images was shipped by the FBI to the United States (on 28 March). There is no evidence as to the circumstances of this shipment. Detective Sergeant McMorran was away on leave by this time. Detective Inspector Wormald does not seem to have been directly involved in any dealings with the FBI in relation to this second shipment.

*Was there consent?*

[134] It is difficult to construe this sequence of events as evidencing the plaintiffs' agreement to images of the hard drives being released to the FBI. Earlier on the day Ms Toohey sent the email (22 March) on which the Crown relies, Mr Foley, for his clients had raised the status of the items seized, (including copies of those items), as an issue that required resolution by the Court and a hearing date had been set. Mr Davison followed that conference up with both a telephone call and letter in which he requested written confirmation from the Crown that no items seized would be transferred.

[135] Ms Toohey did not provide that written confirmation but rather stated the FBI's intention to take one set of copies, and make one available for disclosure. However, she provided no time frame as to when the FBI would "take" the imaged copies and interest was nothing to indicate it would be the next day. But

Ms Laracy's and Ms Toohey's letter of the previous day proposed that the plaintiffs had until 4.00 pm on Tuesday 27 March 2012 to identify "live dispute" items, those items the plaintiffs disputed fell within the terms of the warrant. This timing was consistent with Detective Sergeant McMorran's statement that the FBI were leaving on 31 March. Given this context, the plaintiffs would not likely have understood the 22 March email as imposing a 24 hour deadline. Indeed it seems that the Police and the Crown also did not expect the clones to be shipped the next day.

[136] As to Mr Foley's response I accept that there is some ambiguity in the setting out of his email, but the most obvious reading of it is not that proposed by Ms Laracy. The email is more sensibly read as containing preliminary comments in relation to both "images" and "documentary items", and then going on to address matters of general process affecting all items seized. This is particularly so when the email is read along with the memorandum it attached.

[137] The fundamental objection to construing what occurred as consent however is that the plaintiffs had by that time squarely placed the status of the items seized, including copies of those items, before the Court. In these circumstances the Crown could not reasonably proceed on the basis that the plaintiffs consented without obtaining their express consent. Silence was not enough (though of course, Mr Foley was not silent). At best the correspondence was ambiguous and given that a hearing date had been allocated for resolution of issues in relation to the status of the items, the Crown needed to proceed with considerable caution to ensure that it did have the plaintiffs' consent, if, indeed it was seeking it.

[138] Ms Toohey, as counsel for the Central Authority has elected not to file an affidavit setting out her communications with the Police. This may cloud the picture. Nevertheless the correspondence and affidavits create a clear impression that there was confusion between the Crown and the Police, and perhaps even within the Crown team, as to what was occurring in relation to the images. This was probably contributed to by the fact that two key people, Detective Sergeant McMorran and Ms Toohey went on leave at the critical time. This may explain why the Crown did not advise the District Court Judge that images had already been shipped by the FBI to the United States. It is hard to see why, if matters proceeded as the Crown

suggests, the duplicate copies that were taken were not then made available to the plaintiffs, when that was what Ms Toohy had proposed in the email of 22 March.

[139] Finally, I mention the Crown's reliance on a telephone conversation between Detective Sergeant McMorrان and Mr Davison that is described in an affidavit filed by Detective Sergeant McMorrان and also recorded in a note of the telephone conversation he kept in his diary and has annexed to his affidavit. He says that he told Mr Davison that copying had taken place and that as far as he was aware some copies of specific items had been sent by the FBI to the United States and he also says that Mr Davison did not object to this. Mr Davison has chosen not to file an affidavit to describe the correspondence and exchanges or to personally respond to any of the Crown material on this issue. To do so would cause him difficulty in his representation of Mr Dotcom in terms of the professional rules of conduct. As it happens I do not attach significance to this conversation, as it is meaningless in this context to speak of consenting to that which has already happened, and in any case, Mr Davison represents only one of the plaintiffs.

[140] To conclude, I find no evidence that the plaintiffs consented to the clones being shipped to the FBI in the United States. Given the confused narrative of events that emerges from the correspondence and affidavits and the incomplete material, I do not propose to make any finding beyond that.

***(iii) Would the Solicitor-General have consented to the shipment?***

[141] The final submission made on behalf of the Central Authority is that the Deputy Solicitor-General (acting as the delegate of the Attorney-General) would have given a direction to the Police to allow the FBI to ship the images if he had been requested for such a direction to enable this to proceed. For this reason, any breach of s 49(2) is of a technical nature only. In this Mr Pike refers to an email dated 16 March 2012 from Ms Toohy to the United States Central Authority, the Police and others in which she says:

I have spoken to our Deputy Solicitor-General this morning in relation to your query. We think it would be acceptable for the two FBI agents to come to New Zealand, but could they do two clones, one set for the US, and one

set to leave behind for disclosure, once agreement or a litigated resolution is reached?

[142] In written submissions the Crown said that this was evidence of the Deputy Solicitor-General's consent to the clones being sent offshore. In oral submissions Mr Pike accepted that although this email was not evidence of a s 49(2) direction, it was evidence that such a direction would have been given if it was requested of the Deputy Solicitor-General.

[143] This argument has the fatal flaw that the email is dated 16 March and refers to different arrangements than those proposed in Ms Toohey's email of 22 March. Moreover it was after that date that the status of the items seized was raised with the Court, and a hearing date allocated. In that context I do not accept that the Deputy Solicitor-General, if properly informed of this background, would have directed the release to the FBI of the copies. The Crown is held to the standards of the model litigant, yet to take such an action would be to defeat at least part of the purpose of the plaintiffs' application to the District Court, and also render futile, at least part of the District Court determination.<sup>30</sup>

#### **D. Summary of findings**

[144] I summarise my findings as follows:

- (a) The warrants did not adequately describe the offences to which they related. Indeed they fell well short of that. They were general warrants, and as such, are invalid.
- (b) The warrants were expressed to authorise the search for and seizure of very broad categories of items. These categories of items were defined in such a way that they would inevitably capture within them both relevant and irrelevant material. The Police acted on this authorisation. The warrants could not authorise seizure of irrelevant material, and are therefore invalid.

---

<sup>30</sup> As it happens the application in the District Court was not proceeded with, the issues having become subsumed in this proceeding and in the application to the District Court for disclosure.

- (c) If the warrants had been adequately specific as to offence and scope of search, it may still have been appropriate for the issuing Judge to impose conditions. Conditions could have addressed the offsite sorting process, which was inevitable for the items taken away from the search sites. The conditions could have provided for the cloning of hard drives, the extraction of relevant material and the return to the plaintiffs of the original hard drives, or their clones.
- (d) The Police relied on invalid warrants when they searched the properties and seized the various items. The search and seizure was therefore illegal. If it is relevant, I will hear counsel on whether in each case this therefore amounted to an unreasonable search and seizure for the purposes of s 21 of the New Zealand Bill of Rights Act 1990.
- (e) If I am wrong that the warrants were invalid, then it is nevertheless clear that the Police, in executing the warrants, have exceeded what they could lawfully be authorised to do. This is because they continue to hold, along with the relevant, irrelevant material. The Police have adopted this approach because they have no request from the United States Central Authority to sort the relevant from the irrelevant, and in any event do not have the ability to undertake this exercise without assistance. The Police faced operational difficulties in executing these search warrants in a lawful manner because they are not the investigating officers with knowledge of the operation. The provisions of the MACMA are however sufficiently flexible to enable the Police to involve overseas investigating officers in the execution of warrants to meet this operational difficulty.
- (f) The release of the cloned hard drives to the FBI for shipping to the United States was contrary to the 16 February direction given under s 49(2) of the MACMA that the items seized were to remain in the custody and control of the Commissioner of Police. It was therefore in contravention of s 49(3) of the MACMA.

- (g) The New Zealand Central Authority argued that any breach of s 49(3) was technical because the plaintiffs consented to the shipment of the clones to the FBI in the United States. I have found that no consent was given by the plaintiffs. Given the confused narrative of events that emerges from the correspondence and affidavits and the incomplete nature of the evidence, I do not propose to make any finding beyond that.
  
- (h) The New Zealand Central Authority also argued that the Deputy Solicitor-General would have given a direction under s 49(2) authorising the shipment of the clones to the FBI in the United States, had he been asked. Any contravention of s 49(3) was therefore technical. I do not accept that the Deputy Solicitor-General would have given such a direction, if informed that the status of all items seized, including copies of those items, was the subject of an application by the plaintiffs to the District Court.

## **Relief**

[145] The substantive relief sought by the plaintiffs is as follows:

- a. An order by way of declaration that the MACMA search warrants were unlawful;
  
- b. An order by way of declaration that the removal of clones from New Zealand was contrary to the Solicitor-General's direction to the Commissioner of Police dated 16 February 2012, was not authorised in accordance with s 49 of MACMA and was accordingly unlawful;
  
- c. An order that none of the items seized nor clones or copies thereof remaining in New Zealand, be permitted to leave New Zealand or be accessed in any way other than in accordance with the process set out in below, subject to further order of the Court;

- d. An order that the first defendant forthwith provide the plaintiffs with the clones of seized items currently held by the New Zealand Police (the existing clones);
- e. An order requiring the first defendant to provide confirmation in writing to the plaintiffs identifying those items, the clones of which have been removed from New Zealand, and confirming whether or not the existing clones are effectively duplicates of the clones removed from New Zealand.
- f. An order providing for the following process:
  - i. The appointment of an independent and appropriately experienced barrister or barrister and solicitor of the High Court of New Zealand (the independent practitioner) to conduct the review set out below and to otherwise assist the parties in effecting this process.
  - ii. The review, by the independent practitioner, of all items seized, for the purpose of identifying irrelevant and privileged material.
  - iii. That clones containing only relevant and non-privileged material located on the seized electronic items (the disclosable clones) be created and provided to the United States authorities; and
  - iv. That the first defendant meet the reasonable costs and expenses of the independent practitioner, including the cost of such technical assistance and/or resource as he/she might reasonably require.
- g. An order requiring that all items identified as containing no relevant material be returned forthwith to the plaintiffs.

- h. An order that complete clones of those seized items which are found to contain any relevant and non-privileged material be provided to the plaintiffs as soon as possible, and in any case, not later than the disclosable clone of that item is provided to the United States authorities.
- i. An order directing the first defendant to notify the relevant United States authority of the Court's decision in this matter, and request the voluntary return of the clones removed from New Zealand, along with any copies/clones or data taken therefrom.
- j. The ability for either party to seek further orders from the Court as required, including in relation to any dispute as to the relevance or privilege attaching to a certain item or items during the review by the independent practitioner.

[146] For the reasons given at paragraph [35] above, I am satisfied that declarations should issue in relation to the validity of the warrants and the transfer of the clones. I will hear counsel in relation to the form of those declarations if counsel are unable to agree on them.

[147] I am not at this point prepared to make the remaining orders sought. Given the extent of the challenges, and the nature of my findings, I require to hear further from counsel as to the appropriate remedy or remedies before making any order. This proceeding can be listed before me at 10 am on 4 July 2012 (prior to the hearing of the related judicial review proceedings) for the purposes of timetabling necessary steps for that purpose.

Winkelmann J

Solicitors:  
Simpson Grierson, Auckland  
Crown Law, Wellington

Counsel:  
P J Davison, Auckland  
GJ Foley, Auckland  
M J Ruffin, Auckland