ARTICLE:

HERE'S THE THING:[1] THE CYBER SEARCH PROVISIONS OF THE SEARCH AND SURVEILLANCE ACT 2012

By **Judge David J. Harvey**[2]

Introduction

The Law Commission described the state of the law relating to search and seizure as outdated and a mess in its 2007 report 'Search and Surveillance Powers'.[3] Its comprehensive report made recommendations for a complete reform of the law relating to search, surveillance and seizure in the course of the investigation of crime or offending which resulted in the introduction of the Search and Surveillance Bill. This legislation was not without controversy. It was finally enacted as the Search and Surveillance Act 2012.

The Act is seen as an all-embracing piece of legislation. Its purpose is set out in s 5. It modernises the law of search, seizure and surveillance. It takes into account advances in technologies and regulates the use of those technologies in the process of search, seizure and surveillance. It emphasises the importance of the provisions of the New Zealand Bill of Rights Act 1990, the Privacy Act 1993 and the Evidence Act 2006, and recognises that the exercise of coercive powers by the state should be subject to clear and principled controls. The Act also ensures that investigative tools are effective and adequate for law enforcement needs.

Prior to the Act, the law relating to search and seizure was framed as if most information was held in hard copy. The recognition of the existence of electronic information was partial and inadequate. This created difficulties for law enforcement agencies in obtaining evidence needed to prosecute and convict offenders. The Law Commission observed that a search and seizure regime that clearly provided for access to and preservation of computer based information in a form that could be used in court was long overdue.[4]

The Law Commission devoted chapter 7, comprising some 43 pages to the issue of computer searches. This discussion is not a critique of the report although it is helpful in considering the rationale and the background for the computer and electronic search provisions of the Search and Surveillance Act.

The Law Commission did not consider it necessary for the enactment of a separate code to deal with the powers to obtain access to and search devices storing intangible evidential material and retrieving copies of the data. However, it suggested that a form of 'functional equivalence' should apply to search powers and procedures for computers. The principles underlying search powers and procedures relating to tangible items should generally apply to intangible evidential material with such modifications as should be necessary.[5]

The Commission observed, for example, that the power to copy material should provide for forensic copying or cloning of a hard drive or a storage device containing information.[6] The 'use of force' provisions should be adapted to provide for access to data held in a storage device.[7] It proposed a specific provision to ensure that once the examination of a forensic copy of data made under the authority of a search power was completed the copy should be destroyed unless there was proper basis for its retention.[8] Recommendations were also made to extend the application of a statutory requirement for a person to assist an enforcement officer gain access to

1 *'Thing' includes an intangible thing (for example, an e-mail address or access information to an Internet data storage facility), Search and Surveillance Act 2012, s 97.*

2 *I wish to express my gratitude to Chris Dale, Sharon Wing and Lech Janczewski of the University of Auckland who have made helpful comments on an earlier draft of this paper and to members of the New Zealand Information Security Forum whose comments following a presentation discussion matters raised in this paper have been of considerable assistance.*

3 *NZ Law Commission Search and Surveillance Powers: Report 97 (NZ Law Commission, Wellington, 2007), p 14.*

4 *Search and Surveillance Powers: Report 97 p 15.*

5 *Search and Surveillance Powers: Report p 23, para 23.*

6 *Search and Surveillance Powers: Report p 23, para 24.*

7 *Search and Surveillance Powers: Report 97 p 23, para 24.*

8 *Search and Surveillance Powers: Report 97 p 23, para 24.*

data held in or accessible from the place that is being searched.[9]

The Commission identified the issue of remote searching of computers as one of the most difficult areas it had to deal with.[10] It suggested that the power to execute computer searches remotely should not be recommended as a general law enforcement tool, nor was it recommended where it involved obtaining access to remotely stored private communications as a parallel power to the interception warrant regime.[11]

However recommendations were made for search warrants to authorise enforcement officers to conduct remote searches:

(a) to obtain access to network computer data where it is accessible from a computer found at the place being searched;

(b) where there is no identifiable physical location where the data is stored – such as internet data storage facilities.[12]

Recommendations were also made to permit cross border searches in those two situations where it involved publicly available data or where it was specifically authorised by a warrant.[13]

In this paper I shall address the provisions of the Search and Surveillance Act 2012 that deal with computer searches and remote access searching – or it could be generally and popularly classified as 'cyber searching'. I shall first consider the structure of the search and seizure provisions as they relate to data and to computer systems. I shall then comment upon whether or not these provisions provide the answer to the problems identified by the Law Commission. It will be argued that although the legislation provides generalised solutions, considerable care will have to be undertaken by the authority seeking a search warrant and the officer issuing a search warrant to ensure that:

(a) the warrant is properly issued,

(b) it is properly grounded in terms of the pre-requisites before the issue of a search warrant, and

(c) it properly describes the target or subject of the search.

These issues will involve, at times, a consideration of the way in which a particular technology operates or the use of programs that are employed, especially in the field of remote searches.

The issue of data acquisition by search can often involve large quantities of data some of which will be relevant and some irrelevant. The Act does not address any processes that should be undertaken in assessing relevance or protecting privilege, although ss 136 to 147 of the Act address issues of privilege and confidentiality. This is in contrast to the procedures that are in place for example for examination orders.[14] These are quite specific in terms of process and the provision of protections. The vexed question of remote access will be considered together with a discussion of issues arising in the context of extraterritorial searches. I shall consider the applicability of the 'plain view' doctrine as it applies to computer searches, and some of the problems that arise from Cloud based materials.

The Search and Surveillance Act 2012

Many of the provisions in individual pieces of legislation relating to powers of search and seizure have now been subsumed into the Search and Surveillance Act 2012. For example, the provisions relating to tracking devices[15] are contained in Part 3 Subpart 1 of the Search and Surveillance Act 2012 which deals with surveillance device warrants. Section 337 repeals ss 198 to 200 of the Summary Proceedings Act.[16]

What the Search and Surveillance Act 2012 does is bring into one place and standardises rules relating to searches with warrants, searches without warrants, powers of entry, examination orders (a form of compelled questioning), surveillance orders and production orders. Protections for privilege are provided and procedures are set in place for dealing with seized or produced materials and their disposal. There are also provisions for immunities.

Computer and remote access searches

Within this structure there are provisions in the Act dealing with computer systems searches and remote

9 *Search and Surveillance Powers: Report p 23, para 24.*
10 *Search and Surveillance Powers: Report 97 p 24, para 25.*
11 *Search and Surveillance Powers: Report 97 p 24, para 25.*
12 *Search and Surveillance Powers: Report 97 p 24, para 25.*
13 *Search and Surveillance Powers: Report 97 p 24, para 25.*
14 *Search and Surveillance Act 2012, ss 33 – 43.*
15 *Summary Proceedings Act, ss 200A – 200P. Similarly the transitional provisions apply in respect of Summary Proceedings Act s 200A – 200P, pursuant to s 337 of the Act which repeals them but the transitional provisions are provided in s 349 relating to applications made before the 18 April 2012.*
16 *Section 348 – a transitional provision – provides that those sections remain in force for the purposes of any enactment that incorporates or refers to those provisions. Section 348 expires on the 30 June 2014.*

searches of 'things' that are authorised by a warrant. These provisions are contained in Part 4 of the Act dealing with search, surveillance and inspection powers. Remote searching and computer system searching take place within the context of Part 4 subpart 3 dealing with the issue of search warrants and Part 4 subpart 4 dealing with the carrying out of search powers. I characterise these general powers under the heading of 'cyber-searches'.

Definitions

Before embarking upon a discussion of the cyber-search powers it is necessary to consider some of the definitions in the legislation. Some are identical to those contained in other legislation. A 'computer system' defined in s 3 is identical to the definition of a computer system contained in s 248 of the Crimes Act:

> '"computer system"—
>
> (a) means—
>
> (i) a computer; or
>
> (ii) 2 or more interconnected computers; or
>
> (iii) any communication links between computers or to remote terminals or another device; or
>
> (iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and
>
> (b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.'

Similarly, 'access' in relation to a computer system in the Search and Surveillance Act 2012 replicates the definition contained in s 248 of the Crimes Act.[17]

'Access information' is a new definition and 'includes codes, passwords, and encryption keys, and any related information that enables access to a computer system or any other starter storage device'.[18]

A 'remote access search' is defined as 'a search of a thing such as an internet data storage facility that does not have a physical address that a person can enter and search.'[19]

A 'thing' is defined as including 'an intangible thing (for example, an email address or access information to an internet data storage facility)'.[20] Thus the reference to 'access information' in the definition of a 'thing' must be cross referenced to the definition contained in s 3(1).

The Law Commission drew the distinction between tangible and intangible material and this is reflected in the definitions of the Search and Surveillance Act. If we consider, for example, a document – information written upon a piece of paper – it is quite easy for a reader to obtain access to that information long after it was created. The only thing necessary is good eye sight and an understanding of the language in which the document is written. Data in electronic format is dependent upon hardware and software. The data contained upon a medium such as a hard drive requires an interpreter to render it into human readable format. The interpreter is a combination of hardware and software. Unlike the paper document, the reader cannot create or manipulate electronic data into readable form without the proper hardware in the form of computers.[21]

Schafer and Mason warn of the danger of thinking of an electronic document as an object 'somewhere there' on a computer in the same way as a hard copy book is in a library. They consider that the 'e-document' is better understood as a process by which otherwise unintelligible pieces of data are distributed over a storage medium, are assembled, processed and rendered legible for a human user. Schafer and Mason observe that in this respect the document as a single entity is in fact nowhere. It does not exist independently from the process that recreates it every time a user opens it on a screen.[22]

Computers are useless unless the associated software is loaded onto the hardware. Both hardware and software produce additional evidence that includes, but is not limited to, information such as metadata and computer logs that may be relevant to any given file or document in electronic format.

This involvement of technology and machinery makes electronic documents paradigmatically different from 'traditional documents.' It is this mediation of a set of technologies that enables data in electronic format – at its simplest, positive and negative electromagnetic impulses recorded upon a medium – to be rendered into human readable form. This gives rise to other differentiation

17 *'access', in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system.*
18 *Search and Surveillance Act 2012, s 3(1).*
19 *Search and Surveillance Act 2012, s 3(1).*
20 *Search and Surveillance Act 2012, s 97.*
21 *Burkhard Schafer and Stephen Mason, chapter 2 'The Characteristics of Electronic Evidence in Digital Format' in Stephen Mason (gen ed) Electronic Evidence (3rd edn, LexisNexis Butterworths, London 2012) 2.05.*
22 *Burkhard Schafer and Stephen Mason, chapter 2 'The Characteristics of Electronic Evidence in Digital Format' 2.06.*

issues such as whether or not there is a definitive representation of a particular source digital object. Much will depend, for example, upon the word processing programme or internet browser used.

I made reference in the introduction to this paper to the issue of 'functional equivalence' and perhaps the only way in which an electronic document may be seen as 'functionally equivalent' to a paper based document may be in the presentation of information in readable form. In the case of a *Firm of Solicitors v The District Court Auckland*,[23] Heath J noted that s 198A of the Summary Proceedings Act 1957 was designed to deal with a paper based environment but that now more often than not, information is stored primarily in electronic form. He adopted a functional equivalence approach to executing a search warrant.

With respect I consider that 'functional equivalence' is an unhelpful concept, although to make the statute work in 2004, it was probably the only option available to Heath J. Functional equivalence can relate only to the end product and not to the inherent properties that underlie the way in which the material or information is created, stored, manipulated, re-presented and represented.

It is interesting that the complexity of electronic information is something that is capable of being searched for or 'seized' yet is described as an 'intangible' thing. The ultimate fruit of the search will be the representation of the information in comprehensible format, but what is seized is something paradigmatically different from mere information, the properties of which involve layers of information. It is clear that the legislation contemplates the end product – the content contained in the electronic data – yet the search also involves a number of aspects of the medium as well. In the 'hardcopy' paradigm the medium is capable of yielding information such as fingerprints or trace materials, but not to the same degree of complexity as its digital equivalent. Although Marshall McLuhan intended an entirely different interpretation of the phrase, 'the medium is the message,'[24] it is a truth of information in digital format.

The context for cyber searches – search warrants

A search warrant may be obtained by way of an application.[25] This discussion is not intended to cover the application process in any great detail other than to observe that the application for the warrant must contain, in reasonable detail:

(a) the address or other description of the place, vehicle, or other thing proposed to be entered or entered in searched, inspected, or examined, together with

(b) a description of the item or items or other evidential material believed to be in or on the place, vehicle, or other thing that is sought by the applicant.[26]

Section 98 does not contain any specific provisions relating to what is required by way of particulars to support an application for a search – remote access or otherwise. That is left to s 103 which deals with the form and content of the search warrant. The search warrant must contain, in reasonable detail, certain particulars that are listed in s 103(4).

Section 103(4)(k) refers to a remote access search. If the warrant is intended to authorise a remote access search[27] the search warrant must contain the access information that identifies the thing to be searched remotely. This returns us to the definition of 'access information.' It will be remembered that this includes codes, passwords and encryption keys as well as related information enabling access to the computer system or any other data storage device. It could conceivably be said that 'code' could include a uniform resource locator or URL, a profile, a mail box or e-mail address or an account name which would then identify the 'location'[28] of the information sought.

The examples given in the definition of 'thing' are somewhat confusing because *eiusdem generis*[29] has a limiting and restrictive effect rather than an expansive one. The definition of 'thing' in s 97 gives examples of an e-mail address or access information to an internet data storage facility. This may limit the possibility of an internet data storage facility being a 'thing.' But in s 103(4)(k) the search of the 'thing' is exemplified as an internet data storage facility not situated at a physical location. Whilst it is applauded that the scope of the definition of 'thing' is widened in s 103(4)(k) it is perhaps unfortunate that in the definition section the exemplification has a limiting effect.

Search warrants and remote access – criteria

Interestingly the criteria for the issue of a search warrant authorising a remote access search are contained, not in the material that must be placed before the issuing officer in an application for search warrant under s 98, but in s 103(6). This states:

23 *[2004] 3 NZLR 748 at [110].*
24 *Marshall McLuhan, Understanding Media: The Extensions of Man (McGraw Hill, NY 1964).*
25 *Search and Surveillance Act 2012, s 98.*
26 *Search and Surveillance Act 2012, s 98(1)(d) and (e).*
27 *For example, a search of thing such as an internet data storage facility that is not situated at a physical location.*
28 *The server holding the information.*
29 *Meaning ' of the same kinds, class, or nature' .*

> 'An issuing officer may not issue a search warrant authorising the remote access search of a thing unless he or she is satisfied that the thing is not located at a physical address that a person can enter and search.'

This means that the application for the search warrant must contain sufficient information about the intangible information to establish that a remote access search is necessary. This is because of the *absence* of the intangible information at the physical address the subject of the search. A remote access search would not be authorised, for example, in respect of data held on a home computer because the home computer and the intangible data held upon it is present at a place, namely the home address. Similarly, data held on an office server located in business premises may be searched at the business address. The issue becomes more complicated if the business or home users are using Cloud computing, or data is located off site or in several servers located in one or more countries.

Before issuing a search warrant, the issuing officer would have to be satisfied that the data is *not located* at the physical address. This might mean, for example, that an earlier search has located information that the user of the computer has data located in the Cloud or on a remote server. This information would have to be put before an issuing officer to provide the basis for a remote access search. Alternatively, there would have to be some information or evidence obtained by the investigators to satisfy the issuing officer:

(a) that a remote access search was necessary; and

(b) that there was access information to enable the remote access search to be carried out.

Cyber search powers – local and remote data

I now turn to a consideration of the powers that are authorised in carrying out a search. These are contained in s 110. Interestingly, the search powers in respect of a document that may be lawfully seized in s 110(g) immediately precede the search powers in respect of access to a computer system or intangible material contained in s 110(h) – (i). One wonders whether or not it is coincidence that information based searches of different paradigms should be so closely located in the statutory structure.

Section 110(h) authorises a person exercising the search power to use any reasonable means to obtain access to a computer system or other data storage device located in whole or in part at the place, vehicle, or other thing if any intangible material that is the subject of the search may be in that computer system or other device.

It is important to note that s 110(h) deals with locally located data within the particular device. Section 110(i) enables the copying of material by means of previewing, cloning or other forensic methods for examination either before or after removal. Thus cyber-search powers set out in s 110 are directed towards data contained in a device that is located in a physical place and enables the retrieval or copying of that material.

Section 111 deals specifically with the remote access search of a thing authorised by a warrant and states:

> 'Every person executing a search warrant authorising a remote access search may:
>
> (a) use reasonable measures to gain access to the thing to be searched and
>
> (b) if any intangible material in the thing is the subject of the search or may otherwise be lawfully seized copy that material (including by means of previewing, cloning or other forensic methods)'.

The use of the words 'in the thing' suggests that whatever it is that retains the data is in the nature of a 'container.' This demonstrates the difficulty in attempting to conceptualise locatable electronic data which may in fact be spread across a number of servers or hard drives.[30]

Whether or not cloning would be a proper means of retrieving data located in a remote server in the Cloud is debatable. An additional problem arises as to the nature of the data in its raw form, and the combination of software and hardware that will be necessary to render it into meaningful information. It seems that the cyber-search provisions of the Search and Seizure Act are premised upon an assumption of the availability of proper interpreter or rendering hardware and software which may make the data intelligible. As I have earlier observed, the data in of itself means nothing unless one is able to interpret binary language.

Section 112 authorises the removal of items for examination or analysis in certain circumstances. It provides as follows:

> 'If a person exercising a search power is uncertain

30 *For a consideration of analogies for a computer as a storage device see Chief Executive Ministry of Fisheries v United Fisheries [2010] NZCA 356, [2011] NZAR 54 and Faisaltex Ltd v Preston Crown Court [2008] EWHC 2382 (Admin), [2009] 1 WLR 1987 (DC) discussed below.*

whether any item found may lawfully be seized, and it is not reasonably practicable to determine whether that item can be seized at the place or vehicle where the search takes place, the person exercising the search power may remove the item for the purpose of examination or analysis to determine whether it may be lawfully seized'.

This raises the prospect of seizure of an item to determine whether or not it may be lawfully seized, and could well apply within the context of a computer or computer data prior to cloning. As will be discussed later, the effect of the decision of the Court of Appeal in *Chief Executive Ministry of Fisheries v United Fisheries Limited*[31] will be relevant, along with a consideration of the 'plain view' provisions of the Search and Surveillance Act.[32]

Cyber search specialist assistance and expertise

There will be occasions in the course of a computer search where specialist expertise will be required. Section 113 allows for people to be called upon to assist a person exercising a search power. The person assisting may:

'use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place, vehicle, or other thing if any intangible material that is the subject of the search may be in that computer system or other device.'[33]

Where any intangible material accessed under paragraph (h) which is the subject of the search or may otherwise be lawfully seized, the person assisting may copy that material.[34] Section 114 specifically addresses powers of persons called to assist in remote access search. These powers are similar to those of the person executing the search warrant under s 111.

Section 114 provides that every person called on to assist a person executing a search warrant authorising *a remote access* search may:

'(a) use reasonable measures to gain access to the thing to be searched; and

(b) if any intangible material in the thing is the subject of the search or may otherwise be lawfully seized, copy that material (including by means of previewing, cloning, or other forensic methods).'

Obtaining access to computer systems or to remote access sites may have additional layers of difficulty arising from the need to know login names, passwords and encryption particulars. Section 130[35] provides that a person exercising a search power in respect of data held in a computer system or other data storage may require a 'specified person' to provide access information and other information or assistance that is reasonable and necessary to allow the person exercising the search power to obtain access to the data. The definition of a 'specified person' is contained in s 130(5).[36] The specified person may be:

'(a) the user of a computer system or other data storage device or internet site who has relevant knowledge of that system device or site or

(b) a person who provides an internet service or maintains an internet site and who holds access information.'

The scope of the definition of a specified person in s 130(5)(b) is quite wide and could include an internet service provider who holds access information, or a person who maintains a particular site for data storage purposes and who may also have access information. This could cast an obligation upon an ISP or data storage organisation, both of whom may hold access information on their files, to provide that information to enable a remote access search or a search of a computer system.

The mere provision of access should not amount to self incrimination,[37] but must be read subject to sub Part 5 of Part 4 which relates to privilege and confidentiality.

Although the term is not used in s 130, s 130(5) defines a 'user':

'"user", in relation to a computer system or other data storage device or an Internet site, means a person who—

(a) owns, leases, possesses, or controls the system, device, or site; or

(b) is entitled, by reason of an account or other arrangement, to access data on an Internet site; or

(c) is an employee of a person described in

31 *[2010] NZCA 356, [2011] NZAR 54.*
32 *Search and Surveillance Act 2012, s 123.*
33 *Search and Surveillance Act 2012, s 113(2)(h).*
34 *Search and Surveillance Act 2012, s 113(2)(i). Including by means of previewing, cloning, or other forensic methods either before or after removal for examination.*
35 *Which, as I have earlier observed, replicates in substance Summary Proceedings Act, s 198B.*
36 *A term or definition that was not present in section 198B.*
37 *Search and Surveillance Act 2012, s 130(2) – (3). See also Summary Proceedings Act 1957, s 198B.*

paragraph (a) or (b).'

The definition is wide although it is limited to s 130 because it is prefaced with the words 'in this section.'

Section 198B of the Summary Proceedings Act contained an offence for failing to assist in providing knowledge of a computer or network to assist access. A similar offence is provided in the Search and Surveillance Act 2012 in respect of a breach of s 130 and that offence is contained in s 178. It is an offence to fail, without reasonable excuse, to assist a person exercising a search power when requested to do so under s 30(1).

Notice of a remote access search

Notice of the fact of a remote access search will not be apparent to a person whose data may be the target of the search unless that person is present when the remote access search is carried out. The provisions of s 132 are designed to ensure that the target of a remote access search has been notified that a search has been carried out. The person conducting a remote access search must, when the search has been completed, send an electronic message to the e-mail address of the 'thing' being searched and attach a copy of the search warrant and provide certain particulars:

> '(i) the date and time of the commencement and completion of this search;
>
> (ii) name and unique identifier of the person who had overall responsibility for that search;
>
> (iii) the address of the office to which enquiries should be made.'[38]

If the electronic message cannot be delivered or is returned undelivered, the person conducting the search has to take all reasonable steps to identify the user of the thing searched and send the information to that person.

The language of s 132(1) is confusing because it is based upon a number of assumptions. It refers to the 'thing' being searched. This may be the data storage facility which is the subject of the remote search. It is highly unlikely that a Cloud based server, for example, would have an e-mail address. It will have an IP address. That does not automatically mean that such IP address will be associated with an e-mail account or an e-mail server. There may be an e-mail address associated with the account of the person who is using the Cloud based service. However, in some cases the provisions of the subsection may be impossible of performance because the thing searched may not have an e-mail address. In addition, notice to a 'thing' presumably is conflated with notice to a person since it will be a person who will be taking any action following upon a remote access search.

It would have been preferable to eliminate the confusion caused by the default position. Given that the intention of the notice is to bring the fact of a remote search to a person associated with the target of the remote access search, the requirement to ascertain that person, and give notice would have been a preferable default position.

Remote access searches and extraterritorial issues

Remote access searching gives rise to jurisdictional issues in the case of data stored in servers situated in another jurisdiction. Cloud computing makes this almost inevitable. Some data in the Cloud may be held across a number of jurisdictions.

An extra territorial or cross-border search occurs when an enforcement agency from New Zealand obtains access to a computer or an address that is in another country to obtain evidential material in executing a domestic search warrant. The Law Commission suggests that jurisdictional issues arising as to the access to data are likely to be the biggest obstacle to effective remote access searches. The matter is further complicated by virtue of the fact that New Zealand is not a signatory to the Convention on Cyber Crime 2001 which allows for cross border assistance in criminal matters.[39]

However New Zealand has enacted the Mutual Assistance in Criminal Matters Act 1992 which is designed to facilitate New Zealand providing and obtaining international assistance in criminal matters. This includes obtaining evidence and executing requests for search and seizure. However mutual assistance would require that a search would have to be carried out pursuant to the laws of the assisting state rather than in accordance with the Search and Surveillance Act.

The Law Commission suggested that remote cross border searches should be allowed where the search is to open source or publicly available data regardless of where it is stored geographically. This presumably would not have privacy or information 'ownership' implications. In such a case, if data is available to the public it would not require a search warrant.

Cross border searching could be conducted in

38 Section 132(1)(b).
39 The Convention on Cybercrime, ETS no 185, Budapest 23 November 2011.

accordance with mutual assistance arrangements as has already been suggested. The third suggestion offered by the Law Commission suggested that cross border searches could be specifically authorised under a search warrant. In my view that raises some very real difficulties, especially where there are no mutual assistance arrangements in place. The remote access search may well constitute an unlawful act under the laws of the other state. Alternatively there may be other criteria that have to be fulfilled before a search may be lawful. For example, the United States of America has a developed jurisprudence based upon Fourth Amendment considerations which differ from those in New Zealand.

A further difficulty involves unlawful access to computer systems contained in provisions similar to s 252 of the Crimes Act 1961. Many countries have enacted, or are likely to enact, legislative provisions prohibiting such access within their borders and a remote access search would therefore be unlawful. A lawfully issued search warrant may not fulfil authorisation requirements that would allow access in the 'hosting' state.

The Law Commission acknowledged that while principles of territorial sovereignty should be recognised to the maximum extent possible, observation of such principles may be impossible where the identity of the relevant jurisdiction is unknown.

To further complicate the matter, unlawful cross border searches run the risk of censure by a foreign government and the risk that the evidential material derived from the search may be rendered inadmissible on the basis of foreign unlawfulness.

The Law Commission considered whether the approval of the Attorney General should be sought for a remote cross border search but submissions did not favour such precondition on the basis of uncertainty and potential delay and does not appear in the Act.

The suggestion that search warrant authorisation would cure jurisdictional problems arising in a remote cross border search does not, in my view, solve the problem. The Law Commission suggested that if a remote cross border search was sought a warrant application:

> (a) would require disclosure of that fact,
>
> (b) that the search was or would likely to be a cross border search,
>
> (c) together with the nature of any mutual assistance arrangements with the relevant country if the identity of that country was known.

Where a warrant was issued without specific authorisation for a cross border search, the enforcement agency would have to return to the issuing officer for further authorisation for a cross border search. Such a situation might become apparent in the course of executing the initial search warrant. This is the preferred option for the Law Commission given the inconclusive state of international law.

In the case of *Stevenson v R*,[40] the police applied for a search warrant addressed to Microsoft for records that were kept in the USA. The request was directed to Microsoft in New Zealand who forwarded it to the American parent. The appellant challenged the issue of the warrant. The court held as follows:

> 'Fourth, Mr Haskett submits that the warrant issued against Microsoft should be ruled invalid and the evidence obtained from that source excluded. He relies on the same grounds advanced in support of the challenge to the search warrant, which we have rejected. Additionally, however, he submits that the warrant for Microsoft was invalid because it purported to authorise search in the United States of America. The answer to that submission is, as Mr Ebersohn points out, that the Summary Proceedings Act does not require a warrant to be limited to the New Zealand jurisdiction although of course it could not be practically enforced outside of New Zealand.'[41]

Could this approach – without any developed reasoning – be applied under the Search and Surveillance Act and particularly to remote access searches? The determinative language of the court would suggest it does. A remote access warrant, like a warrant under the Summary Proceedings Act, is not limited to the New Zealand jurisdiction. But the issue of practical enforcement off-shore encounters a technology that enables the act of searching without the formal execution of the warrant. Technically, a remote access search can be carried out. The technology allows an enforcement officer to obtain access to a server off-shore and obtain the data sought. In a situation where a warrant had not been issued authorising such a search, such an action would constitute unauthorised access to a computer system. In such a case, because an action necessary to the commission of the offence had taken place in New Zealand, this would expose the person accessing to an offence against s 252 of the Crimes Act 1961. Thus, the issue of a remote access warrant would protect

40 [2012] NZCA 189.
41 [2012] NZCA 189 at [57].

the enforcement officer from any potential liability in New Zealand. The warrant would make lawful an act of 'hacking' that would otherwise be unlawful and punishable under domestic law. In addition, the provisions of s 132 would allow retrospective notice of the search to be given to the user of the thing searched. But does that mean that there are no implications as far as the 'hosting' state is concerned? There certainly are, and the recipient of a s 132 notice could well raise the issue with the enforcement authorities in the hosting state.

These conclusions suggest that the comment in *Stevenson* needs to be revisited. The first point to note is that *Stevenson* did not deal with a remote access search and was directed to an entity that had a physical domestic presence. Secondly, the information sought may have been digital in nature, but would have to be retrieved by human intervention. A remote access search, by its nature does not require action on the part of the 'thing' in respect of which the search is authorised. Arising from that the third point is that the technology allows complex enforcement issues to be circumvented. The remote access search can be effected by use of the technology.

But just because the technology allows it, should this be permitted to happen? Should the issue of a search warrant allow an extraterritorial remote access search, and should the fruits thereof be admissible? A strict 'crime control' approach would suggest an affirmative response. On the other hand a principled approach that recognises the broader issues of the Rule of Law must recognise that there is a customary international law prohibition on conducting investigations in the territory of another state.[42] Remote access searches violate territorial integrity and, whatever the constitutional constraints that exist within the searching country, such searches are prohibited as violations of international law. Notwithstanding the utopian vision of a separate jurisdiction for cyberspace, the reality is that data has a physical location within the territorial jurisdiction of a state.

Some states have asserted that they possess a broad power to conduct remote cross-border searches, that is, to use computers within their territory to obtain access to and examine data physically stored outside of their territory, so long as the data is relevant to an investigation of conduct over which they have jurisdiction and their own law authorises the search.[43] On the other hand, states applying a stricter interpretation of customary international law to remote cross-border searches need to use various legal assistance mechanisms to conduct the search, such as mutual legal assistance treaties or co-operation at police level. Some steps have been taken toward developing international instruments that facilitate international co-operation and mutual assistance and the recognition of a limited power to conduct cross-border searches.[44]

There are compelling reasons of international comity, adherence to mutual assistance arrangements and to obligations at international law that demand that New Zealand take a principled approach to prohibiting off-shore remote access searches where no reciprocal arrangements are in place. Mutual assistance procedures, where they exist, should continue to apply. Where cross-border searches are permitted within the scope of those arrangements, they should be permitted. A problem arises in situations where mutual assistance arrangements exist but are inadequate to cover cross-border searches; where no mutual assistance arrangements are in place; or it is entirely unclear which jurisdiction remotely accessible data is held in. The Law Commission suggests as follows:

> 'Where there are no mutual assistance arrangements in place between New Zealand and the jurisdiction in which the data is held, cross-border searches should be permitted, provided that the search is not unlawful in the jurisdiction in which the data is held. It would be undesirable for New Zealand law to authorise an action that may constitute an unlawful act under the laws of another country. Enforcement agencies would therefore need to investigate any local legal restrictions on the accessing and searching of data and ensure that any remote cross-border search is conducted in compliance with any such restrictions. Where an agency concludes that a search would not be unlawful in the relevant jurisdiction, any other possible consequences should be considered, bearing in mind the seriousness of the offending under investigation and the likely attitude of the country in which the data is held. However, any such authority to conduct cross-border searches would be of somewhat limited scope, given that many countries have enacted or are likely to enact legislative provisions prohibiting such access to computer systems within their borders.'[45]

What of the situation where it is unclear in which jurisdiction data may be held? The Law Commission was

42 *Michael A. Sussman, 'The Critical Challenges from International High-tech and Computer-related Crime at the Millennium' Duke Journal of Comparative & International Law Volume 9, Number 2 (Spring 1999), 451 – 489.*

43 *Patricia L. Bellia, 'Chasing Bits Across Borders' (2001) University of Chicago Legal Forum, 35 – 101, 39.*

44 *For example, article 19(2) of the Convention on Cybercrime recommends only permitting remote searches within a country's territory.*

45 *Search and Surveillance Powers: Report para 7.122.*

of the view that there may be circumstances where law enforcement agencies should be permitted to conduct a search. It stated:

> 'While principles of territorial sovereignty should be recognised to the maximum extent possible, this becomes impossible to observe where the identity of the relevant jurisdiction is unknown. To prevent law enforcement from investigating alleged offending solely because data is held in an unknown jurisdiction would also create an obvious incentive to hide data in offshore storage facilities. However, it is difficult to find workable parameters for cross-border searches in unknown jurisdictions.We considered whether authority should be contingent on there being no reason to believe that the search would constitute an offence under the laws of any particular jurisdiction. However, with the growing numbers of countries enacting prohibitions on the unauthorised accessing of computer systems this is likely to be unworkable in practice. We considered, alternatively, whether New Zealand law could be used as a benchmark. However, this is also unworkable in practice as a search of data held in New Zealand by foreign law enforcement is unlikely to be lawful under s 252 of the Crimes Act 1961.'[46]

The question of a remote access cross border search is fraught with difficulty and in my view is one where judges issuing search warrants should tread with extreme care. It may well be that the concept of 'cyber space' as a separate place confuses the issue, but the fact of the matter is that the data the subject of the search is located on a server in a foreign jurisdiction. That the data may be accessed remotely by an enforcement authority has 'physical world' ramifications. Differing standards and thresholds for search together with differing approaches towards privacy and data security mean that there is no easy answer to whether a cross-border remote access search would be lawful and therefore whether or not the evidence would be admissible. There would have to be very clear disclosure of all issues at search warrant stage so that if it were found that the search was unlawful, the curative powers of s 30 of the Evidence Act 2006 could be brought into play. Otherwise the issue of a remote access cross border search warrant might be seen as an egregious act of unlawfulness that could not be cured by the balancing test. In closing on this topic I can only endorse the Law Commission recommendation that New Zealand accede to the Convention of Cybercrime so that cross-border remote access searches could be carried out more effectively and solidly grounded in international law.

Disposal of forensic copies

Section 161 is the final section to be considered in this discussion of the cyber search powers contained in the Act. It deals with the disposal of forensic copies. If a forensic copy of data held on a computer system or other data storage device does not contain any evidential material, the person making the forensic copy must ensure that the copy and any other copies made from it are deleted, erased or otherwise destroyed in a manner which prevents the retrieval of the copy or copies by any method.

If the examination of the data shows it contains a *mixture* of data that is evidential material and data that is not, the forensic copy of the data and any copies made of that copy may be retained in their entirety. The forensic copy and any other copies may continue to be searched if such a search was authorised by the search power under which the data was seized and copied.

Handling data retrieved

The Act does not address how forensic data, data retrieved as the result of a search warrant or a remote access search, should be handled.

The difficulty arises because computer systems, be they local or remote, rarely contain a single class of data. They may well contain a large mixture of data some of which may be personal, some of which may be professional, some of which may be confidential, some of which may be protected by privilege and a fraction of which may be of evidential significance. The cloning of a hard drive or the copying of a subscribers 'space' on a remote server will result in a retrieval of a mixture of such information. That much is recognised by s 161(2). The question is how the data should be handled after the search has been carried out, the data recovered and the investigative process is undertaken.

The nature of a computer in the context of search and seizure was considered in the case of *Faisaltex Limited v Preston Crown Court*.[47] In that case Keane LJ held that an item could be the subject of a search warrant that may contain irrelevant as well as relevant material. In an effort to draw an analogy, a filing cabinet was offered as the example of a container although the court considered that a computer was a single thing and drew an analogy

46 *Search and Surveillance Powers: Report para 7.123.*

47 *[2008] EWHC 2382 (Admin), [2009] 1 WLR 1987 (DC).*

with a diary. With the greatest of respect, it is unwise to attempt to draw analogies with paradigmatically different concepts. Perhaps much of the difficulty that we have with computer technology is that pre-digital paradigm terms appropriate, say, to the print technology such as 'document' and 'web page' are used for convenience in the new paradigm as we struggle to develop language that properly reflects the new concept.

The *Faisaltex* approach was followed by the New Zealand Court of Appeal in *Chief Executive Ministry of Fisheries v United Fisheries*.[48] This involved the execution of a search without warrant. The fruits of the search included some computers. Baragwanath J expressed concern that the wholesale cloning of the computer hard drives could harvest privileged information as well as non-privileged information and a system for searching should protect that information. He stated, at [60]:

> 'Because the evidence establishes that the computer did contain information that was conceivably privileged, I respectfully dissent from the conclusion of the other members of the court that it was lawful to clone this computer without adoption of a procedure to protect the privileged interest. Parliament has not conferred carte blanche upon fisheries officers but is left to the court the task of specifying how to balance the public interest in the enforcement of the law against the competing public interest in the preservation of the privilege. I would therefore impute to the legislature an intention that such protection is a condition precedent to a lawful cloning.'

The majority of the Court of Appeal concluded otherwise and took a more generous view of the nature of the computer and the information contained thereon. The starting point was based on the evidence of a forensic accountant who stated that computer forensic best practice involved preserving the electronic data contained within the computer from alteration or deletion by forensic copying or cloning.

Because of the volatile nature of electronic evidence this best practice step is necessary to fix the nature of the electronic data at a point in time. Because of the way in which the computer operates, important evidence such as date and time stamps associated with every file on the computer, as well as the very existence of files, could be altered. The cloning process provides an integrity check that the data cloned is identical to that which existed on the hard drive in the computer being examined.[49] The court took its lead from the *Faisaltex* case and held that it follows, as with a diary or a ship's log, that the *computer itself* is evidence and the relevance is not just in the diary entries but also their position in the diary or log. In this respect the majority seemed to be concerned with as much with the container as with the contents. If this approach is followed, and using unfortunate analogies which must arise from the use of the language of the court, it would be legitimate to take an entire filing cabinet or copy its entire contents before determining relevance. The majority did recognise and agreed with the problems created by legally privileged material and recognised the difficulties identified by Baragwanath J where legally privileged material was involved. A reasonable exercise of the search power, it was suggested, would entail taking steps to protect such material and an appointment of an independent barrister and computer expert[50] were ways of meeting such concerns the majority observed:

> 'We leave open the more complicated question of how the competing interests are to be resolved where the privacy issues are those of a particular person investigated or employees'.[51]

As Baragwanath J observed:

> 'Computers can be used to store a wide range of material including very personal information. There is, though, some force in the argument that many searches, for example those by the police, will involve perusal of both relevant and irrelevant material to find the relevant if the relevant matters likely to be found in a place where irrelevant material is stored. Where a computer is used for ordinary work purposes that is likely to militate against any requirement for precautions to protect the irrelevant'.[52]

The way in which the examination should be carried out was left to the High Court Judge following the decision of the Court of Appeal.

The handling of retrieved data inevitably involves a consideration of the 'plain view' doctrine. Although the matter was not specifically addressed in *United Fisheries*, it is suggested that the approach of Baragwanath J and the involvement of third party scrutiny of recovered data apply to seizure of all recovered electronic data. It is to the issue of 'plain view' searches that I shall now turn.

48 *[2010] NZCA 356, [2011] NZAR 54.*
49 *Cloning, however, is just the first step in the evidence recovery process.*
50 *It would be ideal if both skill sets could reside in the one person.*
51 *[2010] NZCA 356, [2011] NZAR 54 at [82].*
52 *[2010] NZCA 356, [2011] NZAR 54 at [82].*

Cyber searches and 'plain view'

In theory a cybersearch can be carried out like any other search. The search is limited to information that is specified in the search warrant. Officers may seize evidential material outside the scope of the search warrant if it is in plain view. The same rule applies to digital data. The problem lies in the way in which mixed and largely irrelevant data may be stored on a computer along with material within the scope of the search warrant. At present the evaluation of such material is left to the investigating officer or those called upon to assist. These investigating officers may uncover evidence of other offending beyond the scope of the warrant. It could be argued that because the data is accessible and available (unless it is password protected or encrypted) it is in plain view. The issue that arises in such circumstances is whether or not the 'first view' of the recovered electronic data or the cloned hard drive should be reserved to the investigating officer or be conducted by a third party.

This section argues that the 'plain view' doctrine cannot and should not apply to electronic data, and that prior to a consideration by investigating officers, seized electronic data should be evaluated by an independent third party.

A cloned copy of a hard drive preserves information at a point in time. A difficulty lies in the way in which the examination of that information to locate items of relevance to the inquiry should be carried out. Evidence of matters that are not relevant to the particular inquiry, but that may disclose other information of interest to investigative bodies, may well be uncovered within the 'filing cabinet.' The *United Fisheries* use of the 'filing cabinet' analogy provides a context, but as the discussion continues it will become apparent that the analogy fails when confronted with technical reality.

The 'plain view' doctrine is the subject of s 123 of the Search and Surveillance Act 2012.

Section 123 and 'plain view' searches

Section 123 applies when an enforcement officer exercising a search power may seize any item or items that they or a person assisting may find in the course of carrying out the search or as the result of observations at the place or in the vehicle. The officer must have reasonable grounds to believe that they could have seized the items under a search warrant that could have been obtained under the Search and Surveillance Act or any other search power exercisable by them. If there is some uncertainty as to the legitimacy of the search or seizure pursuant to s 112 of the Act, the item may be seized to determine whether or not it may be lawfully seized. The power in s 123 is conditioned only by the pre-requisites contained in s 123(1).

There are three circumstances that are contemplated, namely where the enforcement officer:

> (a) is exercising a search power; or
>
> (b) is lawfully in any place or in or on any vehicle; or
>
> (c) is conducting a lawful search of a person.

Sections 123(1)(b) and (c) relate to physical searches. Section 123(1)(a) involves the exercise of a search power. The term 'search power' is defined in s 3 as follows:

> '"search power" in relation to any provision in this Act, means—
>
> (a) every search warrant issued under this Act or an enactment set out in column 2 of the Schedule to which that provision is applied; and
>
> (b) every power, conferred under this Act or an enactment set out in column 2 of the Schedule to which that provision is applied, to enter and search, or enter and inspect or examine (without warrant) any place, vehicle, or other thing, or to search a person.'

It could well be that the reference in s 123 to a physical location automatically limits the 'plain view' doctrine to what may be seen in the place or vehicle. However, there are two ways in which the scope of the 'plain view' doctrine may be widened. The first is that a computer may be present in the place or vehicle and may be amendable to seizure. The second thing is that the definition of 'search power' refers to 'other thing' which may be extended to data under the definition of 'thing'. It is inevitable that complications will arise from the seizure of a computer or the cloning of a hard drive. These complications are arise as a result of the nature of electronic data storage.

Seizure of computer data

The retrieval of computer data from a computer or a remote access location involves retrieval of *all* the data. Although the data in its raw form is not in 'plain view' it may be rendered into plain view in its entirety by the utilisation of hardware and software which allows for the rendering of the data into readable form. If it is

accepted that in that way computer data falls into 'plain view,' it may also be seized or utilised in that it may be capable of being obtained by a search warrant or any other search power. This 'plain view' approach runs up against the cautions that were expressed by Baragwanath J in the *United Fisheries* case and could well mean that evidence of offending other than that immediately under investigation may be uncovered and subsequently utilised. The issue becomes one of whether 'plain view' applies.

The power to seize items under s 123 constitutes an exception to the general rule that items falling outside the ambit of a search power may not be seized. The Law Commission considered that the plain view exception was justified because:

> '... no reasonable expectation of privacy is violated by the application of the rule. There can be no reasonable privacy interest in a thing that is evidence of criminal offending and is discovered during a search that is itself being lawfully undertaken.'[53]

It was accepted that law enforcement would be restricted if obvious evidence of criminal offending was precluded from seizure where no reasonable expectation of privacy existed.

Conducting a search of a physical filing cabinet pursuant to a search warrant often necessitates a close inspection of the cabinet's contents in order to determine the existence of evidence related to the alleged offending. This is particularly so if the contents of the cabinet are predominantly documents. Nevertheless if evidence of other unrelated offending is found in the cabinet pursuant to a search warrant then such evidence could be said to be in plain view only if it was visible when the cabinet drawer was opened e.g. drug paraphernalia or perhaps a document recording drug transactions placed on top of a pile of other documents. Should evidence of offending outside the scope of the warrant come to light only after all the documents within the filing cabinet have been scrutinised, then such evidence was not in plain view and therefore not able to be seized under s 123.

At a seminar on the Act the following observation was made:

> ' ... enforcement officers will have to be careful that they remain strictly within the scope of the search powers they are exercising, and only seize things that 'come to light' incidentally. As the Law Commission indicates (at [3.132]), this does not mean that 'hidden' things cannot be seized, as long as they are revealed by a search pursuant to a warrant or a warrantless power already underway; what it does mean is that no *further* searching (whether to find an item or to discern whether it is in fact evidence of criminality) can occur. For this, a warrant would need to be claimed or a warrantless power invoked.'[54]

'Plain view' and the scope of seizure

In its report the Law Commission discussed the hypothetical situation where an enforcement officer exercising specific search powers finds evidence of criminal offending outside his or her statutory jurisdiction e.g. a fisheries officer conducting a law enforcement search of a place encounters drugs or firearms.[55] The Law Commission adopted the view that specialist enforcement officers should *not* be authorised to seize items of criminal offending outside their statutory jurisdiction:

> '... The adverse consequences in seizing an item thought to be illegal when in fact it is lawfully possessed are obvious. Enforcement officers with specialist expertise or statutory jurisdiction in only a specific area of the law will generally have insufficient knowledge to make an informed assessment that, in the circumstances, an item is evidential material relating to a criminal offence of a completely different nature to that with which they generally deal. Where they do have that expertise, discovering evidential material other than that for which the power is being exercised will largely be a matter of chance that cannot be captured by a statutory test. Accordingly, with one exception, no such power is recommended.'[56]

The exception referred to concerned the seizure of objectionable publications, in terms of the Films, Videos and Publications Act Classification Act 1993, discovered in plain view by a customs officer in the course of lawfully exercising a customs search power.

The Law Commission then stated in conclusion:

> 'In any case where a person is lawfully inspecting for regulatory/compliance purposes or searching for law enforcement purposes and sees an item that may be evidential material of a type of offence in respect of which he or she has no power to inspect or search,

53 *Search and Surveillance Powers: Report para 3.134.*

54 *Michael Heron and Dale la Hood, Search and Surveillance Act 2011 – New Powers (NZLS Seminar Paper, Wellington June 2012). The title of the NZLS seminar incorrectly stated the year of the Act.*

55 *Search and Surveillance Powers: Report para 3.158.*

56 *Search and Surveillance Powers: Report para 3.159.*

there should be no authority to seize.

In such a case the person should let the police know that the item exists and where they saw it. The police will then have to determine how best to deal with the situation. The information provided may establish grounds to obtain a search warrant or may, in some circumstances, provide a basis for warrantless search.'[57]

The recommendations of the Law Commission are now reflected in the statutory scheme of s 123. Accordingly seizure of obvious evidence of criminality is restricted in s 123(2) to items that the enforcement officer has reasonable grounds to believe could be seized by him or her under a search warrant that could be obtained by him or her or a search power exercisable by him or her.

Aside from a police officer, no person exercising an inspection or law enforcement power is permitted to seize items in plain view and reasonably believed to be evidence of any criminal offending unless the person exercising that power has jurisdiction in relation to that offence.

The problem with the filing cabinet analogy

Where the search power is executed in relation to the contents of a filing cabinet, unless the evidential material was in plain view when the cabinet drawers were opened, then any evidence of an offence outside the scope of the warrant found after the cabinet's contents were removed and examined would not be able to be seized under s 123. Such evidence was not in plain view since further 'searching' of the cabinet's contents was required.

It is at this point that the filing cabinet analogy breaks down, the reason being that when a clone is taken, it is tantamount to copying the entire contents of the filing cabinet. Electronic data is not like paper. It does not have physical properties akin to paper. The paper document, lying in 'plain view' in a drawer of the filing cabinet has no immediate electronic parallel.

The Law Commission wished to apply a plain view doctrine to seizures of intangible data to allow evidential material to be seized unrelated to the search warrant which comes into plain view during a computer search. US courts suggested technical means to limit computer searches to data that is reasonably likely to yield evidential material such as:

(a) searching by file name, directory or sub-directory; specifying the name or recipient of e-mail to be searched;

(b) specifying particular types of files to be searched;

(c) specifying use of specific key words or phrases in a key word search;

(d) specifying file date and time of creation; and

(e) confining the search to a specific compartment such as e-mail storage.[58]

The Law Commission considered such an approach as problematic. Limiting computer searches to key words could produce an incomplete search because key word searches only operate on files containing identifiable text. Electronic discovery software could provide a solution. The Law Commission did point out that potentially incriminating data may not be stored as accessible text but stored in other formats and suggested that the non-standard nature of computer forensic processes means that controls such as search protocols would not be a practical requirement to supplement the warrant specificity requirement.[59] Given the state of e-discovery software and the various techniques that are available, this suggestion is questionable. For example the use of hashing techniques allow for the identification of non-textual electronic objectionable material.

In relation to *tangible* evidential material, the Law Commission's approach was that evidence that is not covered by search power could only be seized if it came into 'plain view' during the course of a search, and that seizure of such material does not authorise the search of a premises for additional evidence of that or similar offences unless it is authorised by a statutory provision such as s 18 of the Misuse of Drugs Act or by obtaining a further warrant.

The Law Commission recommended this approach to intangible evidential material. The 'plain view doctrine' was predicated upon visual observation. In relation to computer data where 'plain view' would apply, would depend on whether the incriminating nature of the information was *immediately* apparent to the enforcement officer without further analysis. If the enforcement officer or forensic analyst sees evidential material for an unrelated offence during access pursuant to a search power and they have jurisdiction to obtain a warrant in respect of that offence, they may seize and retain that material.

57 *Search and Surveillance Powers: Report 97 paras 3.162 – 3.163.*
58 *Search and Surveillance Powers: Report 97 para 7.57.*
59 *Search and Surveillance Powers: Report 97 para 7.57.*

But officers may not then search for further evidence of that or similar offences – by trawling through a large amount of data stored on a computer – without separate authority. Where it is necessary to scrutinise a large amount of data while executing a search, the purpose of the scrutiny should be only to identify data falling into the description authorised by the search power and such scrutiny should not be conducted at large as an intelligence gathering exercise. Orin Kerr suggests a number of steps that could be taken to limit the operation of the plain view doctrine:[60]

> (a) examining the intent of the executing officer – where the officer tries to look for evidence described by the warrant the discovered material may be seized, but where the officer ignores the warrant that material may not be seized;
>
> (b) requiring investigators to use a targeted search tool;
>
> (c) assessing the reasonableness of the search and allowing the plain view evidence to be seized if the search is considered to be reasonable, although this may be difficult to assess where only part of the forensic process is found to be unreasonable;
>
> (d) limiting the operation of the doctrine by the type of offence so that plain view evidence can only be seized for more serious offences;
>
> (e) discarding the plain view doctrine entirely for computer searches.

The Law Commission considered that the 'plain view doctrine' was necessarily limited to *superficially apparent* incriminating material which, together with the protection against unreasonable search and seizure afforded by s 21 of the Bill of Rights Act, should provide sufficient limits on its operation in the context of computer searches. Where investigators seize plain view material *outside* the scope of a search power, that material will be liable to be rendered inadmissible unless the seizure falls within the parameters of the plain view doctrine.[60]

Of relevance will be the nature of the forensic operations that located the plain view material, the nature of the scrutiny of the plain view material to ascertain evidential value and whether the forensic process used was the most targeted process available in the circumstances.

It must be remembered that the s 21 protections afforded by the New Zealand Bill of Rights Act are subject to the s 30 balancing test. Whilst one must yield diffidence to the Law Commission's evaluation of the matter, once again it does seem that paradigmatic differences do not appear to have been taken into account. The concerns that are expressed about the limitation of search parameters and the search tools that are available perhaps may have been valid in 2007 at the time when the Law Commission was carrying out its investigation. Improvements in technology and the utilisation of a wide variety of search techniques, particularly in the field of electronic discovery, suggest that it is easier today to exclude irrelevant material from a search than it may have been five years ago. Whatever the costs of new technologies may be, the hours of labour must be substantially reduced by the use of a technology which reduces the volume of material for review. Once again it would be necessary for an investigating officer to establish the applicability of the 'plain view doctrine' in the first place and in doing so would have to explain in some detail the search processes that were undertaken that indeed revealed the other incriminating material to be 'in plain view.' The defence no doubt would have access to expert evidence to establish alternative search procedures were available, or that in fact the material would not have come within the 'plain view doctrine' thus rendering the search unlawful. In a s 30 balancing analysis, the court could well revisit whether or not the method of discovery of the material was egregious and once again an examination of the technology would be necessary.

Imposing an intermediate layer

A further problem arises in the assumption that the investigating officers have direct and immediate access to the data after seizure. In this respect, the imposition of an independent layer between the action of cloning the data and its assessment by an individual officer such as that suggested in *United Fisheries* is necessary. Although there may be significant costs associated with the employment of an independent barrister or computer expert (or both) – and it would be of advantage if both requirements could be present in the same person – it must be recognised, as was made clear by the Law Commission in its 2007 report and in s 5 of the Search and Surveillance Act and especially s 5(b),[61] that new technologies challenge concepts that were developed in a different paradigm and may make such added layers necessary.

60 *Orin S. Kerr, ' Searches and Seizures in a Digital World' Harvard Law Review Volume 119, 2005, 531 – 585.*

61 *Recognising the importance of the rights and entitlements affirmed under the New Zealand Bill of Rights Act, the Privacy Act and the Evidence Act.*

US v Comprehensive Drug Testing Inc

The case of *US v Comprehensive Drug Testing Inc*[62] is instructive in its approach to the 'plain view' doctrine in the context of digital material. In short, the case holds that the 'plain view' doctrine is inapplicable in such a context. The case warrants some detailed discussion. Kozinski J defined the fundamental issue as the procedures and safeguards that Federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information.

The background to the matter was that in 2002 the Federal government commenced an investigation into the Bay Area Lab Cooperative (BALCO) which it suspected of providing steroids to professional baseball players. At the same time the Major League Baseball Players Association entered into a collective bargaining agreement with Major League Baseball providing for suspicionless drug testing of all players. Comprehensive Drug Testing Inc., (CDT) an independent business, administered the programme and collected specimens from the players. During the BALCO investigation, Federal authorities learned of 10 players who had tested positive in the CDT programme. The government secured a subpoena seeking all drug testing records and specimens pertaining to major league baseball in CDT's possession. Unsuccessful attempts were made to quash the subpoena, but the government also obtained a warrant authorising searches CDT's facilities in Long Beach. The warrant was limited to the records of 10 players in respect of whom the government had probable cause. When the warrant was executed, however, the government seized and promptly reviewed the drug testing records for hundreds of players in major league baseball.

Concerns were expressed by courts reviewing the warrants as to the process that had been undertaken and, with the exception of materials pertaining to the 10 identified baseball players, the various warrants were quashed.

One of the precedents applying to the extent of searches was *US v Tamura*.[63] Tamura was decided in 1982, just preceding the dawn of the Information Age. All of the records there were on paper. The government was authorised to seize evidence of certain payments received by Tamura from among the records of Marubeni, his employer. A three step process was required to identify the materials pertaining to the payments:

> (a) examining computer printouts to identify a transaction;
>
> (b) locating the voucher to pertain to that payment; and
>
> (c) finding the cheque that corresponded to the voucher.

The government agents soon realised that this process would take a long time unless they got help from the Marubeni employees who were present. The employees refused, so the agents seized several boxes and dozens of file drawers to be sorted out in their offices at their leisure.

The court disapproved of the wholesale seizure of documents and particularly the government's failure to return the materials that were not the object of the search once they had been segregated. There was no reason to suppress the properly seized materials just because the government had taken more than was authorised by the warrant, but for the future the court recommended that in the comparatively rare instances where documents are so intermingled that they cannot be feasibly sorted on site, the government should seal and hold the documents pending approval by a magistrate of a further search in accordance with the procedures set forth in the American Law Institutes Model Code of pre-arraignment procedure. If the need for transporting the documents was known to the agents prior to the search, they could apply for specific authorisation for large scale removal of material which should be granted by the magistrate issuing the warrant only where on site sorting is not possible and no other practical alternative exists.

In response to the suggestion in *Tamura*, the government in Comprehensive Drug Testing did seek advance authorisation for sorting and segregating off site, but once the items are seized the requirement of the warrant that any seized items not covered by the warrant be first screened and segregated by computer personal was completely ignored.

In answer to the objection raised about *Tamura*, the government argued that it did comply with the procedures, and it was not required to return any data it found showing steroid use by other baseball players because that evidence was in 'plain view' once the government agents had examined the directory. The 'plain view' doctrine negated any obligations under *Tamura* to return the property.

Kozinski J emphasised that the point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizeable materials, and to avoid turning a limited search for particular information into

62 621 F.3d. 1162 (9th Cir. 2010).
63 694 F.2d 591 (9th Cir 1982).

a general search of office file systems and computer databases:

> 'If the government can't be sure whether data may be concealed, compressed, erased or booby trapped without carefully examining the contents of every file – and we have no cavil with this general proposition – then everything the government chooses to seize will, under this theory, automatically come into plain view. Since the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less: why stop at the list of all baseball players when you can seize the entire ... directory? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the zip discs under the bed in the room where the computer once might have been. See United States v Hill 322 F.Supp.2d 1081 (CD Cal 2004). Let's take everything back to the lab, have a good look around it and see what we might stumble upon. This would make a mockery of Tamura and render the carefully crafted safe guards in the Central District warrant annulity. All three Judges below rejected this construction with good reason.'[64]

To avoid a reoccurrence, the court considered that, '... magistrate judges should insist that the government forswear reliance on the plain view doctrine. They should also require the government to forswear reliance on any similar doctrine that would allow retention of data obtained only because the government was required to segregate seizable from non-seizable data.'[65] If consent to such a waiver is not forthcoming the court said that the Magistrate Judge should order that the seizable and nonseizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether.

In addition, while it is perfectly appropriate for the warrant application to acquaint the issuing judicial officer with the theoretical risks of concealment and destruction of evidence, the court noted that the government must also fairly disclose the actual degree of such risks in the case presented to the judicial officer. In *Comprehensive*, for example, the warrant application presented to one judge discussed the numerous theoretical risks that the data might be destroyed, but failed to mention that *Comprehensive Drug Testing* had agreed to keep the data intact until its motion to quash the subpoena could be ruled on by the Northern California District Court, and that the United States Attorney's office had accepted this representation. This omission created the false impression that unless the data was seized at once it would be lost.

Finally, the court held that the process of sorting, segregating, decoding and otherwise separating seizable data (as defined by the warrant) from all other data must be designed to achieve that purpose and that purpose only. Thus the government was allowed to seize information pertaining to 10 names, and the search protocol must be designed to discover data pertaining to those names only, not to others, and not to those pertaining to other illegality. The court observed that the government has sophisticated hashing tools at its disposal that allow the identification of well known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools could not be used without specific authorisation and the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium seized.[66]

The case also noted that the government failed to comply with another important procedure that was specified in the warrant – namely that computer personnel conduct the initial review of seized data and segregate materials which was not the object of a warrant for return to their owner.

The court suggested that warrant applications should normally include, or the issuing judicial officer should insert, the protocol for preventing agents involved in the investigation from examining or obtaining any data other than that for which probable cause is shown. The procedure might involve a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation and it should be made clear that only those personnel may examine and segregate the data.

Furthermore, those computer personnel should not communicate any information they learn during the segregation process without further approval of the court. But in the discretion of the issuing judicial officer, and depending upon the nature and sensitivity of the privacy interests involved, computer personnel may be government employees or independent third parties not affiliated with the government. The court suggested that the issuing judicial officer may appoint an independent expert or special master to conduct or supervise the

64 *US v Comprehensive Drug Testing 621 F.3d. 1162 (9th Cir. 2010) at 1171.*
65 *US v Comprehensive Drug Testing, 621 F.3d. 1162 (9th Cir. 2010) at 1178.*
66 *US v Comprehensive Drug Testing, 621 F.3d. 1162 (9th Cir. 2010) at 1179.*

segregation and redaction of the data. In a case such as *Comprehensive*, where the party subject to the warrant is not suspected of any crime, and where the privacy interests of numerous other parties who are not under suspicion of criminal wrong doing or implicated by the search, the presumption should be that the segregation of data would be conducted by or under the close supervision of an independent third party selected by the court.

Only when the data has been segregated and, if necessary, redacted may government agents involved in the investigation examine only the information covered by the terms of the warrant. The court suggested that any remaining copies should be destroyed or at least so long as they may be lawfully possessed by the party from whom they were seized returned along with the actual physical medium that may have been seized such as the hard drive or computer.

Kozinski J also made some useful observations about information in the digital paradigm. He said that the case well illustrates both the challenges faced by modern law enforcement in retrieving information that needs to pursue and prosecute wrong doers and the threat to the privacy of innocent parties from a vigorous criminal investigation. At the time of *Tamura*, most individuals and enterprises kept records in their filing cabinets or similar facilities. Today, the same kind of data is usually stored electronically, often far from the premises. Electronic storage facilities intermingle data, making them difficult to retrieve without a thorough understanding of the filing and classification systems used – something that can only be determined by closely analysing the data in a controlled environment. *Tamura* involved a few dozen boxes and was considered a broad seizure; but even inexpensive electronic storage media today can store the equivalent of millions of pages of information.

The court made the following final summary of its holdings:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine and digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialised personnel or an independent third party. If the segregation is to be done by government computer personnel it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial foray.
>
> 4. The government search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return nonresponsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Although the decision in *Comprehensive* has its basis in Fourth Amendment jurisprudence, the issue of the extent of material that is available in electronic storage devices and the way in which that should be dealt with in the context of a limited enquiry authorised by a search warrant is common throughout the common law world. It may well be that the 'plain view' doctrine may be of limited utility, and should be restricted to physical searches. It bears repeating that the new digital paradigm contains challenges for established processes and assumptions. The 'different' nature of digital data is recognised in *United Fisheries* and the suggestion by Baragwanath J that an independent assessor stand between the seizure of data and its examination for evidential material is mirrored in *Comprehensive*. However, the latter decisions emphasises the scrutiny that must be applied by issuing officers to applications for electronic data searches.

Some further thoughts on the cyber search regime

The technology must be understood not only in terms of developing the evidence which may arise from this search, but in terms of providing the basis for the search in the first place. The difficulties that may attend upon providing the basis for a remote access search have already be covered. It will be remembered that a search warrant authorising a remote access search cannot be issued unless the issuing officer is satisfied that the target of the search is not located at the physical address that can be entered and searched.

The following scenario may demonstrate the course of action that must be followed. Enforcement officers obtain a search warrant to search premises including computers located on the premises. A search of the computers located upon the premises may reveal evidence of data held at a remote location – say in the Cloud. This evidence

could not be uncovered at the scene of the search. Best practice dictates that officers do not use the computer itself, but rather take a forensic clone of the data. On the basis of the information contained from the search of the computer, an enforcement officer could approach an issuing officer and seek a remote access search on the basis of the evidence from the clone of the computer. Alternatively, the enforcement authorities would have to have some kind of information to suggest that data was located remotely to justify a remote access search without embarking upon the first step suggested above.

An issue is whether an application for a search warrant for premises containing computers might also include remote access application on the basis of speculation that a thing is not located at a physical address that can be entered and searched. On a rigorous interpretation of s 103(6), that could not happen. It would seem to be necessary that it would have to be established that the data is located elsewhere. This does not prevent the police from searching the computer, cell phone, iPad, or other device to establish the fact of remote location of data.

It therefore seems that it is a necessary precondition that to establish evidence of remote location of data, there be a search carried out of local physical and tangible computer systems in the first place. This will probably apply in the majority of cases.

An interesting issue might arise if a suspect uses a cell telephone to obtain access to a web based e-mail account and the police believe that the e-mail relates to an offence. The police can obtain a search warrant to search the cell telephone even if the data is stored elsewhere. It may well be that a copy of the data is located on the cell telephone. In such a case, the data would not be in a remote location and a remote access search would not be required. If it is established that it is possible to obtain access to an e-mail account through the cell telephone, but a copy of the incriminating e-mail is not located on the cell telephone itself, and is located in a web based e-mail account such as Gmail or Outlook.com (the successor to Hotmail) and access to the mail account requires a password, under s 111 the police may use reasonable measures to gain access to the remote e-mail account – presuming a remote access search – or alternatively may invoke the provisions of s 130 to obtain the password to obtain access to the account, thus circumventing the need for a remote access warrant.

If the suspect destroys the cell telephone, the police still could obtain a search warrant to obtain access to the web based e-mail account via a computer and use reasonable measures to obtain the password, as long as the URL or web e-mail address can be identified as the thing to be searched. In such a case, it is arguable that a remote access search would be necessary.

However, a further problem arises in the case of Cloud based services. Two Cloud based services that are available allow for the retention of data upon the hard drive of a local computer as well as retention of data on the Cloud based servers. It all depends on how the customer specifies the way in which the Cloud service is to operate.

One such service – Dropbox – allows for all of the files held on the Cloud servers to be 'mirrored' on any of the computers where the user may have that the Dropbox utility installed upon them. For example I have a Dropbox account with Dropbox.com where I store personal documents. I have a desk top computer in my home office that has the Dropbox utility installed upon it and is configured to update any changes to any of my documents in Dropbox located in the Cloud. I also have a desk top computer at my place of business which has the Dropbox utility installed and similarly updates any changes to documents. I have a laptop computer that has internet access and has the Dropbox utility installed upon it and is configured to update. If I change a document on my laptop computer that is in the local Dropbox folder, it will automatically update and store the document at Dropbox.com in the Cloud. When I turn on either of my desk top computers that document will automatically be updated in the Dropbox folder on that computer. It would, in those circumstances, be unnecessary to obtain a remote access search to Dropbox.com because all of the files are mirrored on both of the desk top computers and the laptop.

However, if I configure the Dropbox account in such a way that files are not mirrored on my desk top computers and my laptop, but are held only in the Dropbox account in the Cloud, it would be necessary to obtain a remote access search to obtain copies of the documents at Dropbox.com in the Cloud. An investigating officer applying for a search warrant would have to satisfy the issuing officer that my utilisation of Dropbox did not include mirroring of the files on a local computer before being able to obtain a remote access search. To obtain a remote access search upon an initial application for a search warrant would require some fairly specific evidence about my use of computers and the way in which I utilise my Dropbox account to fulfil the requirements of s 103(6).

A similar difficulty arises with the Cloud based service offered by Evernote.[67] Once again, the way in which Evernote works depends upon the way in which the

67 http://evernote.com/.

user configures it. I can hold copies of all of my Evernote documents on my desk top computer and effectively mirror everything that I have in the Cloud. Alternatively, I can hold the headers or descriptions of the documents held on the Evernote server without the content and may from time to time download onto my local computer those documents held by Evernote in the Cloud that I want to use at a particular time.

If an investigating officer were to execute a search warrant of my desk top computer and locate a reference to my use of Evernote, he may well discover the index of specific documents held by Evernote in the Cloud. The investigating officer may well be able to go further and identify from the index only the documents that are relevant to the particular inquiry and it would not be necessary for a complete download of all documents held in my Evernote account. In such a case, the investigating officer may be able to go back to the issuing officer and seek a remote access warrant in respect of those particular relevant documents. This would mean that the difficulties encountered by a complete clone of a hard drive and the concerns expressed in the *United Fisheries* case would not arise.

These are but two examples of a large number of Cloud based utilities that are available on the internet. They demonstrate the care with which investigating officers must justify and issuing officers must scrutinise applications for remote access warrants. It is my tentative view that it would be necessary for an investigating officer to provide information in some detail of the nature of the remote service the subject of the search order and particularly, if it involves Cloud based facilities, details of how the particular Cloud based service works. It should be relatively straight forward if the information is the fruit of a search of a local computer that reveals evidence of utilisation of a Cloud based or remote facility. However, it does seem at this stage that unless there is clear evidence of the way in which remote facilities are utilised, that remote access warrants will probably be consequential upon a local search rather than falling within the ambit of an initial application for a search warrant.

Conclusion

This discussion demonstrates the difficulties that arise with applying physical concepts of search to the intangible environment of the digital paradigm and the internet. It is helpful that the legislation provides guidelines within which searches take place, but it will probably become clear from this discussion that the provisions in the legislation are broad in their approach and will probably be tested over time. What is obvious is that a knowledge and understanding of the technology will be required not only of applying officers but also of those judicial officers issuing search warrants.

David J Harvey, LLB (Auckland) MJur (Waikato) PhD (Auckland) is a Judge of the District Court, New Zealand.

