Chapter 6 – Searching digital data

INTRODUCTION

6.1 Since the enactment of the Search and Surveillance Act 2012 (the Act) there has been an exponential growth in the storage of information in an electronic form. Much of daily life involves electronic devices of one sort or another – from reading books on devices, to driving cars fitted with GPS navigation systems, to monitoring our fitness with electronic wrist bands.¹ We communicate via text message, email and Skype. We keep up-to-date through social media and online news websites.

6.2 In addition, much data is generated in the background of our lives that we usually know little about. Cell phone towers track our movements, EFTPOS transactions track our spending habits and smart-meters track our electricity usage.

6.3 The storage of digital information is growing at exponential rates:

- Google now processes over 40,000 search queries every second on average, which translates to 3.5 billion searches per day and 1.2 trillion searches per year worldwide (up from nearly 800 billion searches in 2009);²
- a report prepared in 2014 for the United Nations Secretary-General on the data revolution noted that 90 per cent of data in the world had been created in the previous two years alone;³
- in New Zealand, the number of uncapped broadband data plans nationwide quadrupled from 2014 to 2015, while fibre-based Internet connections more than doubled;⁴
- in 2015, there were 117.7 wireless mobile broadband subscriptions per 100 New Zealanders;⁵

¹ In this Paper we have used the term “electronic devices” in a broad sense to refer to all devices that operate with components such as microchips and transistors that control and direct electric currents. This includes but is not limited to computers, tablets and mobile phones.


⁴ From 115,000 to 628,000 and from 46,000 to 100,000+ respectively: Statistics New Zealand “Internet Service Provider Survey: 2015” (14 October 2015) <www.stats.govt.nz>.
• electricity smart meters have been installed in 1.2 million New Zealand homes, outnumbering traditional analogue systems.\(^6\)

### 6.4 The rise in the use of mobile devices and remote data storage since 2012 has raised significant questions about the way the Act is operating. For example:

- Does the Act deal adequately with the risk of electronic searches capturing irrelevant or privileged material?
- Does the Act provide appropriate guidance in relation to remote access searching?
- Is the maximum penalty for failing to comply with a request to provide assistance to access a mobile device adequate?

### 6.5 This chapter discusses the similarities and differences between digital and physical searching, before considering each of these questions in turn. While we deal with issues that relate to privilege generally in Chapter 8, we have discussed privilege as it relates to the capturing of digital material in this chapter because some of the options for reform are shared with options to address the potential problem of seeing irrelevant material. It should also be noted that, in Chapter 7, we discuss whether New Zealand Police should be able to search electronic devices under warrantless powers.

### COMPARING PHYSICAL AND DIGITAL SEARCHES

### 6.6 The differences between digital and physical methods of data storage go further than merely the quantity of data stored on a digital device. There are also qualitative differences. For example, a smart phone can reveal the user’s internet search history and where the user has physically been. If the owner of the phone is using some of the more common applications, their phone can reveal who their friends are, what they cooked for dinner, how much exercise they are doing, and how well they slept the previous night.

### 6.7 The nature and quantity of data about individuals now stored in electronic form presents opportunities for enforcement agencies but also challenges for the protection of human rights. Those challenges were recognised in the Law Commission’s 2007


The Commission considered whether computer searches have a potentially larger impact on privacy interests and require a more stringent search regime. It was thought that a person may be more concerned about a search of their computer than of their physical premises because of the large amount of personal information that may be present on the computer (rather than being dispersed around their premises in physical form). Also of concern was the potential for law enforcement investigators to see a large amount of material on a computer that is unrelated to the subject of the search.

6.8 However, the Commission also considered that law enforcement investigators may not know in advance of executing a warrant whether the material sought is in electronic or physical form, meaning that a more stringent regime for computer searches may create an incentive for criminal organisations to use an electronic medium to conduct criminal activity. Ultimately, the Commission concluded that:

... the fact that information is stored in intangible form should not confer any greater protection from search and seizure than information that exists in tangible form; on balance, a different regime for the search and seizure of intangible material is not justified.

6.9 This approach was largely adopted by the Act. The threshold for applying for and issuing a search warrant makes no distinction between whether the material is likely to be found in physical or electronic form. Also, while the Act provides some specific provisions in relation to electronic searches, many of the rules in the Act for the execution of warrants do not distinguish between electronic and physical search. That means that rules originally formulated in respect of physical searches must be applied by analogy to electronic searches.

---

8 At [7.14].
9 At [7.16].
10 At [7.19].
11 Search and Surveillance Act 2012, s 6. This provision reads: “An issuing officer may issue a search warrant, in relation to a place, vehicle, or other thing, on application by a constable if the issuing officer is satisfied that there are reasonable grounds—(a) to suspect that an offence specified in the application and punishable by imprisonment has been committed, or is being committed, or will be committed; and (b) to believe that the search will find evidential material in respect of the offence in or on the place, vehicle, or other thing specified in the application”.
12 For example, more restrictive criteria for remote access searches and a duty on persons with knowledge of a computer to assist access to that system.
6.10 In many respects this approach is operating effectively. There seems to be no debate that the legal threshold for searching electronic material should be the same as for physical material. There are, however, some concerns around the practical application of the rules when a digital search is involved. This includes difficulties associated with:

• the increased likelihood of inadvertently capturing irrelevant or privileged material; and

• determining when and how the rules relating to remote access searches apply.

6.11 We discuss each of these concerns in this chapter. We also discuss a concern that has arisen as to the penalty for failing to provide assistance to access a computer.

**IRRELEVANT AND PRIVILEGED MATERIAL**

**Digital searching methods**

6.12 There is a range of ways of capturing electronic material. At one end of the spectrum, a portable electronic device can be connected to a terminal designed to screen the contents of the device for certain material. The New Zealand Customs Service uses this method to screen some devices for prohibited items or illegal activities at the border. If the screening process does not detect any relevant material (for example, illegal pornography), the device is returned to the owner. No information from the device is copied or retained. This method involves a relatively low level of privacy invasion because most material on the device is not actually seen by a person and no data is retained.

6.13 In contrast, the content of a mobile phone carried by a person arrested or detained for an offence may be searched without a warrant if the arresting officer has reasonable grounds to believe that the phone contains evidential material related to the offence. This may involve the officer manually searching the phone. The search should be targeted to finding the particular information sought. A broad, untargeted search may

---


14 Search and Surveillance Act 2012, ss 88 and 125(1)(l).

15 However, Police tell us that manual searches are not generally recommended and that extraction devices, which capture all the data on a device, are provided in many centres.
be considered unreasonable by a court under section 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).\footnote{Section 21 of the New Zealand Bill of Rights Act 1990 reads: “[e]veryone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.”}

6.14 Searches of computers and devices located at businesses and private homes, however, are generally conducted in a systematic manner involving two stages – first, capturing the data, and second, searching the captured data.

**Capturing the data**

6.15 At the first stage, investigators will capture all the data stored on a targeted computer or device by making a forensic image of it. The images are either made on-site by downloading all the data onto a separate storage device; or off-site when the computers, devices or hard drives are seized and removed. The images include all the data on a computer or device, including deleted and hidden data. Investigators often use a write-blocking device to prevent the original material from being modified. Both the forensic image and the original data can be “hashed” using an algorithm. This means that the values assigned by the algorithm through the hashing process to the original data and to the forensic image can be compared to ensure that the image is accurate.

6.16 Enforcement agencies that undertake a large amount of digital searches often have digital forensic units (DFUs) with specialist computer forensic staff. These units exist independently from their organisation’s investigating teams. Their functions are to capture the relevant computer data, search it for the specific information requested and send only the relevant material to the investigators. A key advantage of DFUs is that any irrelevant or privileged material inadvertently seen in the course of searching for the targeted material is not seen by the people actually conducting the investigation.

**Searching the data**

6.17 At the second stage, the forensic image is searched for relevant material. Searches of digital material can be akin to searching for needles in very large haystacks and a variety of methods may be used to find the information sought under a warrant or when exercising a relevant search power. The process has been described to us as involving a combination of in-depth systematic search together with intuition and
experience. A forensic specialist will usually use specialist forensic software and search terms to find either the particular material targeted or to find material that is irrelevant and can be filtered out of the search.

6.18 Where the search is conducted by a DFU, any documents that appear to contain evidential material will be transferred to another storage device and sent to the investigating officers. Sometimes there will be a to-and-fro process between the investigators and DFU staff to clarify exactly what type of material is required for the investigation. Often a record of the search will be made, which includes the types of software and search terms used to isolate the evidential material.

**The statutory requirements**

6.19 There are various ways in which the Act currently manages the risk of irrelevant or privileged material being seen by investigators undertaking digital searches.

**Specification of details in warrants**

6.20 Reflecting the common law rule that warrants cannot be issued for “fishing expeditions”, there are a number of provisions in the Act that require the object of a search to be specifically described. This limits the amount of irrelevant material that will be seen. The application for a search warrant must provide certain particulars in “reasonable detail”, including:

(d) the address or other description of the place, vehicle, or other thing proposed to be entered, or entered and searched, inspected, or examined:

(e) a description of the item or items or other evidential material believed to be in or on the place, vehicle, or other thing that are sought by the applicant:

6.21 The particulars that must be described in the warrant itself include:

(f) the address or description of the place, vehicle, or other thing that may be entered, or entered and searched, inspected, or examined:

(g) a description of what may be seized:

(h) the period during which the warrant may be executed, being—

(i) a period specified by the issuing officer not exceeding 14 days from the date of issue; or

---

19. Section 103(4).
(ii) if the issuing officer is satisfied that a period of longer than 14 days is necessary for execution, a period specified by the issuing officer not exceeding 30 days from the date of issue:

(i) any conditions specified by the issuing officer under subsection (3)(b):

(j) if the warrant may be executed on more than 1 occasion, the number of times that the warrant may be executed:

(k) if the warrant is intended to authorise a remote access search (for example, a search of a thing such as an Internet data storage facility that is not situated at a physical location) the access information that identifies the thing to be searched remotely:

(l) an explanation of the availability of relevant privileges and an outline of how any of those privileges may be claimed (where applicable):

…

6.22 The issuing officer may impose any conditions that are considered reasonable. Those conditions could, in theory, include restrictions on how a search of electronic material must be conducted to minimise the risk of investigators seeing irrelevant or privileged material.

6.23 We note that there is no equivalent requirement for specification in relation to warrantless powers (as they are exercised without pre-authorisation by an issuing officer). Digital searches under warrantless powers are limited by the particular threshold for the exercise of each power and by the terms of section 110, which describes other powers that a person executing a search warrant or a warrantless search has.

The procedure for dealing with privileged material

6.24 The law has long held that certain types of information are subject to heightened privacy interests and has granted them special status as privileged material. The Act provides a framework for dealing with claims of privilege in respect of information that may be obtained under search or surveillance device warrants or other search powers. The purpose of that framework is to minimise the risk of investigators inadvertently seeing privileged material. In Chapter 8 we describe in more detail the procedure in the Act for dealing with privilege.

---

20 Search and Surveillance Act 2012, s 103(3)(b).
21 Law Commission Search and Surveillance Powers (NZLC R97, 2007) at [122].
The rules governing seizure

6.25 Prior to the Act, there was doubt surrounding the amount of data that could be captured in the first step of a search of digital material. However, it is now clear that:

- the whole computer or device may be seized if it is not reasonably practicable to determine whether particular items on the computer or device are able to be seized;
- reasonable measures may be used to access a computer system or other data storage device if intangible material that is the subject of the search may be on the computer or device; and
- intangible material that can be seized can also be copied.

6.26 Those rules reflect the fact that it can be difficult to know in advance exactly where on a computer or device the targeted material will be stored.

6.27 The Act provides no guidance on how forensic investigators must search the captured data for relevant material while minimising the risk of seeing privileged or irrelevant material. However, there are rules applicable to all searches around what material may be seized that must be applied by analogy to digital searches. Generally, only items that are the subject of the search may be seized. However, there has always been an exception for items related to criminal offending that are in “plain view”, but are not covered by the warrant. The plain view rule was included (and extended) in the Act:

An enforcement officer to whom this section applies may seize any item or items that he or she, or any person assisting him or her, finds in the course of carrying out the search or as a result of observations at the place or in or on the vehicle, if the enforcement officer has reasonable grounds to believe that he or she could have seized the item or items under—

23 Search and Surveillance Act 2012, s 112.
24 Section 110(h).
25 Section 110(i). That would include copying the entire hard drive that was seized under s 112 because it was not reasonably practicable to determine on-site what items on the computer may be seized.
26 The Act lists some powers that are relevant to conducting electronic searches, such as the powers to request any person to assist with a search, to use equipment to help carry out a search and to use reasonable measures to access a computer system or other data storage device (s 110(b), (e) and (h)), but they do not restrict or guide how the search may be conducted.
27 Section 110(d).
28 Section 123(2).
(a) any search warrant that could have been obtained by him or her under this Act or any other enactment; or
(b) any other search power exercisable by him or her under this Act or any other enactment.

6.28 The plain view rule does not affect the scope of the search itself; rather, it dictates what items found during a search can be seized. In effect, section 123 means that enforcement officers may seize items that come to light incidentally during the course of a search that are relevant to a different offence. However, no further searching can be undertaken to find further related items or to determine whether found items constitute evidential material (unless a different search power applies or a new search warrant is obtained).29

6.29 As we have discussed above, electronic devices can contain large amounts of information. Because of this, the “plain view” rule has the potential to operate more broadly in the electronic sphere than in respect of physical searches. There is a greater amount of material that an enforcement officer may “find” in the course of carrying out an electronic search and be able to seize under the plain view rule.

6.30 We do not see this as a problem with the plain view rule itself. It simply underscores the importance of ensuring that electronic searches are carried out in the most targeted way possible, to minimise the amount of irrelevant material that is seen.

**Does the Act permit enforcement agencies to see too much digital material?**

6.31 There seems to be a concern, touched on in the Law Commission’s 2007 Report,30 that the sheer volume of information stored on a computer inevitably makes computer searches very intrusive. This concern equates the data captured to the data searched. However, a computer search is not inherently intrusive – it depends on how the search is conducted. If the evidential material sought is very specific and the search is well targeted for that material, it may be found with very little irrelevant material being seen, perhaps on par with a targeted search of physical premises.31

6.32 However, the nature of digital searches means that investigators can potentially see much more irrelevant material in the course of even a highly targeted search than would be usual for a physical search. Evidential material can be hidden, deleted or in

---

29 See Simon France (ed) Adams on Criminal Law - Rights and Powers (online looseleaf ed, Thomson Reuters) at [SS123.03].
31 In fact, it could be argued that a well targeted search is less intrusive than a physical search of (for example) a home, which may include the bedroom and bathroom and is perhaps witnessed by the neighbours.
an unusual format, which means that investigators must sometimes search in areas of the hard drive that are not the most obvious places to find the material. For example, some businesses store documents as scanned photos or PDF files without converting them into text with optical character recognition. In that situation, an investigator may need to search the photos on a computer to find the required evidence.

6.33 An understanding of the nature of digital forensic searches brings some perspective to this risk. Our research for this review and discussions with digital forensic specialists has led us to the following tentative conclusions:

- Digital searches generally capture much more data than the evidential material sought, but only a fraction of the captured data is actually seen.
- Searches of digital material are usually highly targeted to the evidential material sought. There is a legal requirement for the search to be targeted, but also the volume of data captured and pressures of time and resources generally make that a necessity.
- Just as in a physical search, investigators undertaking digital searches will see irrelevant material in the course of their search. In some cases, the potential to see irrelevant material is much greater in a digital search than in a physical search.

6.34 These are, however, preliminary conclusions and we would be interested to hear from those who conduct digital searches and those who have had their digital devices searched, as to whether our discussion in this chapter reflects their experience.

**Does the Act adequately protect privileged material during digital searches?**

6.35 While the Act has gone a long way towards clarifying how issues of privilege must be dealt with when executing physical searches, it says nothing specific in relation to digital searches.

6.36 If a person claims privilege, the Act states that they must provide a particularised list of the things in respect of which the privilege is claimed. A variety of practices have developed across the different enforcement agencies for dealing with this in respect of digital material. Often, the person executing the search will discuss the issue with the

---

32 Optical character recognition (often known as OCR) is the mechanical or electronic conversion of images of typed, handwritten or printed text into machine-encoded text.

33 Search and Surveillance Act 2012, ss 141(a) and 147(a).
person claiming the privilege and come up with a customised plan for identifying and then isolating the privileged documents. That plan may include:

- the owner of the material providing a list of search terms designed to identify privileged documents;
- a lawyer for either the person claiming privilege or for the enforcement agency trawling through the documents to identify legally privileged documents; or
- the appointment of an independent person to identify privileged material.

6.37 We note that the Inland Revenue Department (IRD) has established standard operating procedures for the use of its search powers, including dealing with privilege in digital searches. 34 Those procedures provide that: 35

- electronically stored documents that are potentially subject to privilege will be copied or imaged, sealed and removed (or the device containing the document will be removed for imaging off-site);
- the copy or image will remain in the custody of IRD’s DFU and not be released to investigators until after the privilege process is completed; and
- the owner of the documents can provide a list of keywords to the DFU staff, who will use them to identify documents to which the privileges apply.

6.38 We are told that the identified documents are then transferred to a separate storage device and offered to the owner to specify any documents for which they wish to claim privilege. Documents in respect of which privilege is claimed are permanently removed from the captured data.

6.39 These procedures and those described in paragraph 6.36 are particularly relevant where the entire contents of a hard drive of a computer or several computers are captured and searched, and more generally where there is no urgency. We would be interested to know how issues of privilege are dealt with in other circumstances, for example in relation to the search under a warrantless power of a single mobile device.

6.40 Finally, we note that some enforcement agencies have expressed frustration at the lack of legislative guidance on how to deal with privilege in digital searches, but also

---

34 Inland Revenue Department Operational Statement: The Commissioner of Inland Revenue’s Search Powers (OS 13/01, September 2013).
35 As above at [136].
concede that any requirements need to be flexible enough to cater to different types of digital material and differing claims of privilege. Some agencies have also commented that privilege claims over digital material can cause significant delay in investigations.

Options for reform

6.41 If it is concluded that the Act currently permits enforcement officers to see privileged material or more material than is necessary during digital searches, then there are numerous ways in which the Act could be amended to address that problem. We discuss three options for reform below.

Documenting search procedures

6.42 One option for reducing the amount of irrelevant material that is seen during digital searches would be for the Act to require a person undertaking a search of a computer or other data storage device to produce a record of their search procedure. That record would then be available on request to the owner of the computer or device searched.

6.43 This option has three advantages. First, it would ensure that the person conducting the search is accountable for each step taken in the process. Knowing that someone may check up on the procedure followed should help ensure that the search is conducted within lawful limits. Second, it would provide a defendant in subsequent criminal proceedings with the means of checking whether or not evidence from the search used against him or her was lawfully obtained. Third, even if criminal proceedings did not eventuate, it would enable the person who owned the computer or device to know the extent to which his or her privacy had been interfered with and make a complaint to the Privacy Commissioner, where appropriate.\[36\]

6.44 This type of record is already part of the standard practice of DFUs within enforcement agencies and is provided as part of litigation disclosure to the defendant. We do not know the extent to which records are kept when computers or devices are searched by enforcement agencies without DFUs.

---

\[36\] Privacy Act 1993, s 67. Under this section, a person may make a complaint to the Commissioner alleging that any action is or appears to be an interference with the privacy of an individual. Under s 66 of that Act, an action is an interference with privacy if the action breaches an information privacy principle and, in the opinion of the Commissioner or Tribunal, the action caused loss, detriment, damage, or injury to the individual; adversely affected the rights, benefits, privileges, obligations, or interests of that individual; or resulted in significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.
Specifying example warrant conditions

6.45 One option for both limiting the amount of irrelevant material that is seen and for preventing investigators from seeing privileged material would be for the Act to require the issuing officer to consider imposing conditions on the warrant that are specifically designed to address these risks.

6.46 As we have mentioned, issuing officers already have the power to impose any conditions on search warrants they consider reasonable. The Act provides two optional conditions as examples. Further optional conditions could be added to that list in relation to digital searches (together with a requirement for the issuing officer to consider imposing such a condition), for example:

• requiring an electronic device that will be searched to be switched to “flight mode” as soon as it is seized;
• permitting only specified parts of the computer, data storage device, or data captured to be searched;
• permitting only specific search terms to be used to identify the information sought; or
• requiring the search to be supervised by an independent third party.

6.47 In relation to privilege, the issuing officer could be required to consider conditions covering how digital material should be handled to identify and separate out privileged material, along the lines of IRD’s standard operating procedures.

6.48 The advantage of this option is that an independent person (the issuing officer) considers the risks of the digital search before the search is conducted – before privacy is invaded or the privileged material is seen. Requiring issuing officers to consider imposing specified conditions would help to balance the risks associated with search warrant applications being determined ex parte (meaning the issuing officer does not have the benefit of opposing submissions on what conditions are appropriate).

6.49 However, most issuing officers are not trained in the technical requirements for digital searches, which may limit the value of such an approach. There is a risk that these types of conditions could be imposed without a full understanding of their technical

37 Search and Surveillance Act 2012, s 103(3)(b). The two optional conditions relate to restricting the time of execution and requiring assistance to be provided by the occupier or person in charge of a place searched.
impact, which could unreasonably reduce the flexibility available to investigating officers.

6.50 Also, each of the conditions relating to the risk of seeing irrelevant material in paragraph 6.46 may be of limited benefit:

- Switching a device to “flight mode” would prevent information accessible from the device via the Internet from being seen during the search. It would also ensure the information is preserved in the same form as when it was seized: if a device remains connected to the Internet, the data on it may automatically update or be over-written. However, we have been told that Police already recommend that officers switch mobile devices to flight mode to ensure the data cannot be remotely wiped or updated after it comes into police possession.

- Conditions limiting which parts of a computer or device can be searched or which search terms can be used may be very difficult to apply in practice, because it may not be known in advance how evidential material is stored on that computer or device. Also, data is sometimes deliberately stored in unusual formats to hide it from potential investigations. For example, the phone number of an associate could be in the contacts list on a phone, but could equally be in a word document stored on an email, in a photo or screenshot, or in an unrelated application. A suspect could use an abbreviation or nickname for an associate to make it harder for investigators to find material when using search terms.

- Supervision by an independent third party could be expensive and time-consuming. We have been told of instances where third parties have supervised digital searches, but only for the purpose of identifying privileged material. We suspect that, while the presence of a third party may provide reassurance to the owner of the material searched, it is not likely to have much impact on the amount of irrelevant material seen by investigators. In addition, it may pose a significant impediment to investigations.

6.51 While they are not completely independent, DFUs located within enforcement agencies offer a sort of compromise. As described above, they capture the data, search for relevant documents and send only those to investigators. While the forensic specialist may see significant amounts of irrelevant material, the actual investigators do not. However, there may be little point in a condition on a warrant requiring the search to be conducted by a DFU (where one exists within an enforcement agency), because we are advised that where that option exists it will be taken.
6.52 A further option would be to impose a statutory duty on enforcement officers to take all reasonable steps to minimise access to privileged or irrelevant material. The Act currently places a similar duty in relation to privilege on any person who is undertaking surveillance under the Act. That person must: 38

... take all reasonable steps to prevent the interception of any communication or information to which a privilege recognised by this subpart would apply if the communication or information were sought to be disclosed in a proceeding.

6.53 We have no specific indication of the legislative intention behind the inclusion of this duty in relation to surveillance. However, we speculate that it was considered very difficult to enact specific procedures to protect privileged material in relation to surveillance, given that surveillance is an ongoing process that generally occurs without the subject’s knowledge (and who is therefore unable to make a claim of privilege at the time it is occurring). By placing the onus on the person undertaking the surveillance to consider the issue in advance, some protection is provided and the flexibility that is required to undertake the surveillance is maintained.

6.54 In relation to searches of digital material, and merely for discussion purposes, a duty could be phrased as follows:

Any person who undertakes a search of digital material must take all reasonable steps to avoid seeing:

- material that is not evidential material to which the search power applies; and
- any communication or information to which a privilege recognised by this subpart would apply if the communication or information were sought to be disclosed in a proceeding.

6.55 Such a duty would require the person undertaking the search to consider the two identified risks before undertaking the search and to implement procedures to avoid them. The advantages of this duty are that:

- it provides some assurance to the owners of the information searched that their privacy will not be unnecessarily invaded and that the risk of seeing privileged material is reduced;
- it recognises that the risks cannot be completely eliminated but that there is a public interest in officers taking steps to reduce the risk; and

38 Search and Surveillance Act 2012, s 140(2)(a).
• the steps taken to mitigate the risks could be determined on a case-by-case basis, without prescriptive rules that might limit the flexibility required for a search.

6.56 We suspect that this duty would have little impact on large scale searches of digital material by DFUs of enforcement agencies. From what we are told, DFUs already take steps to address these risks in every case. We are less sure of the impact that it might have on one-off searches of digital devices by officers who are not forensic specialists. We envisage that “all reasonable steps” would require the officer to show that the search was planned and that it was targeted to the material sought under the warrant or search power.

Q23 Is there potential under the Act for enforcement officers or assistants searching digital material to see more material than is necessary for the purpose of the search (irrelevant material)?

Q24 Does the Act adequately protect privileged material from being seen by enforcement agencies during digital searches?

Q25 Are any amendments to the Act necessary or desirable to limit the amount of privileged or irrelevant material seen during electronic searches? For example, the Act could be amended to include:

(a) a requirement to document the search procedures followed and provide it to the owner of the material searched if requested;
(b) a requirement that the issuing officer consider the imposition of specified conditions designed to reduce the risk of seeing privileged or irrelevant material; and/or
(c) a duty on the person undertaking a search of digital material to take all reasonable steps to avoid seeing privileged or irrelevant material.

REMOTE ACCESS SEARCHES

6.57 Prior to 2012, it was unclear whether a search warrant for computer information provided authority to access that information remotely. The Act sought to address this by creating special rules for “remote access searches”. A remote access search is defined in the Act 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.

---

39 Law Commission Search and Surveillance Powers (NZLC R97, 2007) at [7.74].
40 Search and Surveillance Act 2012, s 3 (definition of “remote access search”).
6.58 We discuss some issues with this definition below.\textsuperscript{41} In practical terms, we have treated a remote access search as a search of material that is not stored on the computer or device being searched or on the same computer system as that computer or device.

6.59 The Law Commission’s 2007 Report said that it was one of the most difficult issues it dealt with. It listed the Privacy Commissioner’s concerns with the remote accessing of computer information as including:\textsuperscript{42}

\begin{itemize}
  \item the owner of the data is unable to be present during the search;
  \item the evidence obtained through a covert search of a computer is of questionable value unless the search is undertaken under carefully controlled conditions to ensure reliability and admissibility of evidence; and
  \item search warrants can be granted by people without the professional, legal and judicial experience required to craft appropriate conditions to protect the privacy of third parties.
\end{itemize}

6.60 The Commission cautiously concluded that the power to execute computer searches remotely “is not recommended as a general law enforcement tool”.\textsuperscript{43} However, it recommended there should be a power to access network computer data where it is accessible from a computer found at the place being searched; and to conduct remote access searches when there is no identifiable physical location where the data is stored.\textsuperscript{44} These recommendations were generally implemented in the Act.

6.61 Since the enactment of the Act, the use of internet-based data storage facilities has grown exponentially. Both at home and in the office, web-based applications for business and conducting our private lives are in very common use. Some of the most common examples are Google Drive, Apple iCloud, Dropbox, Pinterest, and Xero accounting software. However, information is also stored on the Internet in ways we do not necessarily think of as “storage”: for example, in email accounts, blogs, social media and many applications providing entertainment or services from our computers and devices.

\textsuperscript{41} See paragraphs [6.104]-[6.105].

\textsuperscript{42} Law Commission Search and Surveillance Powers (NZLC R97, 2007) at [7.106].

\textsuperscript{43} At 24.

\textsuperscript{44} At 24.
6.62 This increase means that it has also become much more common for evidential material required for law enforcement purposes to be stored on internet-based facilities. That raises a general question for this review as to whether the Act is clear enough about when searches of this Internet data require prior authorisation (or specific authorisation).

**The statutory provisions**

6.63 The Act establishes separate rules for digital searches that are conducted remotely. However, the provisions tend to deal with remote searches in an indirect manner, making them somewhat difficult to understand. To start with, rather than defining “remote access search” directly, the Act defines the concept by reference to the condition for authorising it (it does not have a physical address that a person can enter and search).  

6.64 Just as the Act does not state when a search warrant is required, neither does it directly state when a warrant is required for a remote access search. However, it does say that:

- an issuing officer must 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; and
- if the warrant is intended to authorise a remote access search, it must contain the access information that identifies the thing to be searched remotely in reasonable detail.

6.65 Strangely, those requirements are found in the section concerned with the form and content of a search warrant, rather than in the sections concerned with the contents of an application for a search warrant and with the conditions for issuing a warrant. In effect, they mean that if a search to be conducted under a warrant is intended to

---

45 Search and Surveillance Act 2012, s 3 (definition of “remote access search”: “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”).

46 Although we note that a remote access search without a warrant may be an offence under s 252 of the Crimes Act 1961 (accessing a computer system without authorisation).

47 Section 103(6). Some people interpret this section as indicating a preference for physical searches.

48 Sections 103(4)(k) and s 3 (definition of “access information”: “includes codes, passwords, and encryption keys, and any related information that enables access to a computer system or any other data storage device”).

49 Sections 98 and 6.
include accessing material remotely, that remote access must be specifically authorised in the warrant. The Act says nothing about whether data can be searched remotely under a warrantless search power.

6.66 The Act states that any person executing a search warrant authorising a remote access search and any person called on to assist, may use reasonable measures to gain access to the thing and to copy any material found that is the subject of the search. These powers replicate those provided in a standard search warrant.

6.67 The only other provision in the Act that specifically deals with remote access searches relates to providing notice of the search. The person conducting a remote access search must provide notice of the search when it is completed by sending an electronic message to “the email address of the thing searched” providing specific details of the search and attaching a copy of the search warrant. If that electronic message is unable to be delivered, the person who conducted the search must take all reasonable steps to identify the user of the thing searched and to send the information to that person.

6.68 Finally, it should also be noted that one of the standard powers of a person exercising a search power may enable some forms of remote access searching without requiring specific authorisation. Section 110(h) states that a person executing a search power has the power to use “any reasonable measures to access a computer system … located at the place” searched. The ambit of the term “computer system” (which is defined in section 3 of the Act) is fairly vague. However, to the extent that the computer system includes any data stored via an Internet facility, section 110(h) arguably enables remote access searching without requiring specific authorisation in a warrant. We discuss the meaning of “computer system” further below.

6.69 Our research and consultation to date raises three issues relating to remote access searches:

- whether there continues to be justification for separate rules for remote access searches, and if so:
  - whether the provisions in the Act should be amended to make the rules and their application clearer; and

---

50 Search and Surveillance Act 2012, ss 111 and 114.
51 Sections 110(h) and 113(2)(h).
52 Section 132.
• whether notice of a remote access search should be able to be deferred.

**The justification for separate rules is questionable**

6.70 The principle underlying the special rules for remote access searches is a preference for physical searches, expressed as a requirement that an issuing officer may not authorise a remote access search unless there is no physical address that can be entered and searched. It appears that the purpose of this restriction is to allay any public concern over the apparent lack of protections around remote access searches: ⁵³

\[ \text{... we expect that empowering enforcement agencies to conduct computer searches remotely would prompt widespread concern about authorised state hacking into the lives of private citizens (albeit under search powers) and that there would not be sufficient public confidence that privacy interests would be adequately protected.} \]

6.71 Therefore, a key question for this review is whether public concern about access to remotely stored information remains high or whether it is thought that those concerns can be adequately dealt with procedurally – for example, by adequate particularisation of the database to be searched and notification requirements. Put another way, does a determination that the data sought is not located at a physical address that can be entered and searched mean that it should be subject to greater protection?

6.72 The Law Commission’s original intention was for the legislation to indicate a preference for a physical search: ⁵⁴

\[ \text{... where there are physical premises capable of being identified and searched, the presumption that a search power be exercised on those premises is to be preserved.} \]

6.73 Therefore, if the subject of a search uses a dedicated computer to access an Internet data storage facility, a search of the internet-based data via that dedicated computer could be carried out when conducting a search (under a warrant or search power) of the physical premises where the computer is located. The search of the internet-based data would not need a separate, specific authority. However, where the search subject does not possess or use a dedicated computer to access the facility, and instead accesses the facility from any computer with Internet access: ⁵⁵

\[ \text{... there is no specific physical location that can practicably be searched to locate a device that can then be subject to a computer search.} \]

---

⁵³ Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [7.82].
⁵⁴ At [7.83].
⁵⁵ At [7.94].
6.74 The current problem is that since that policy was articulated in 2007, there has been a significant increase in the use of web-based applications for many purposes, both private and in business. That means that:

• the use of a dedicated computer to access internet-based applications has declined;
• a greater percentage of evidential material is found on internet-based data storage facilities;
• people are often unaware (and unconcerned about) where their data is stored; and
• the distinction between data stored locally and data stored remotely may not be clear to a law enforcement investigator.

6.75 Perhaps the key issue here is whether the location of the data should matter. Assuming data is located within New Zealand, should there be different rules for internet-based data that is not accessed from a dedicated computer (specific authorisation required) than for internet-based data that is accessed via a dedicated computer (specific authorisation is not required)? With the advent of cloud computing, does the location of the data stored become an artificial distinction?

Option for reform

6.76 If it were thought that there should no longer be special rules for remote access searches, the Act could be amended to remove the requirement that an issuing officer may only issue a warrant for a remote access search if the thing to be searched is not located at a physical address that a person can enter and search. In other words, specific authorisation for a remote access search would not be required. Rather, applications for searches of remotely stored data would be governed by section 6 of the Act. That would mean that applications for search warrants relating to remotely stored data would not need to specify the access information for the thing to be searched.

6.77 The original intention behind the latter requirement was to prevent “fishing expeditions” by ensuring that remote access searches are confined to only what is justified for the investigation. However, arguably the requirements to adequately detail the scope of other types of searches would also provide sufficient protection for remote access searches. Applications for other searches must specify:  

---

56 Search and Surveillance Act 2012, s 98(1)(d)–(e).
• the address or other description of the place, vehicle, or other thing proposed to be entered, or entered and searched, inspected or examined; and

• a description of the item or items or other evidential material believed to be in or on the place, vehicle or other thing that are sought by the applicant.

6.78 Under these requirements, instead of specifying the access information (for example, Google email; email address – joe.bloggs@gmail.com; password – 1234) the application for a search warrant would describe the thing to be searched and the evidential material believed to be in that thing (for example, “any emails to or from Joe Bloggs relating to the supply of illegal drugs on any ISP”).

6.79 The current requirement to specify the access information can amount to a “catch-22” situation for enforcement officers: to get the access information, the officer needs to do a search, but in order to do the search, the officer needs the access information. Sometimes the officer is able to obtain access information from prior voluntary disclosure by a person, by using a production order, or from a prior unrelated search.

6.80 Relying on descriptions of the remote data sought, rather than on the access information for that data would remove a significant hurdle for criminal investigations. However, if the special rules for remote access searches are retained, there is scope to clarify the regime, as we discuss next.

Q26 Should the Act continue to treat data stored remotely differently from data stored at a physical location that can be entered and searched?

The rules controlling remote access search are not clear

6.81 We have encountered some confusion as to when remotely stored data can be searched without specific authority and when a remote access search warrant needs to be issued by an issuing officer. This has resulted in a variety of practices amongst enforcement agencies:

• some agencies never do remote access searches because they are unsure about the meaning of “physical address”;

• some agencies will access data stored remotely only from computers that are already open and logged on to the relevant database;

• sometimes any data that can be accessed from a computer located in premises that are being searched will be accessed (whether or not it is remotely located) if it falls within the terms of the search warrant; and
some agencies restrict remote access searches to only those circumstances in which they can get a search warrant, making it unavailable to them in respect of warrantless powers (including search powers in other statutes).

6.82 This lack of clarity has been caused by several inter-related factors. We discuss each of these below and outline options that may help to address them.

**Placement of the rules within the Act is confusing**

6.83 As noted above, the placement within the Act of the provisions controlling remote access searches is confusing. The key provisions are found in the section concerned with the form and content of a search warrant, rather than those concerned with the content of the application and with the conditions for issuing the warrant. This raises questions without clear answers about why these rules were separated out. What was Parliament’s intention and does that different treatment have an impact on the interpretation of the provisions? We suggest that the placement of these rules creates unnecessary uncertainty as to their meaning.

**The warrant regime is permissive not mandatory**

6.84 The Act provides rules for when an issuing officer may issue a search warrant authorising remote access search. It says nothing directly about when a remote access search may be undertaken. However, enforcement agencies look to these provisions for indications of Parliament’s intention as to when remote access search is permitted. It may be clearer and enhance the protection of privacy if Parliament’s intention in this regard is stated more directly in the Act.

**Option for reform**

6.85 To resolve this uncertainty, a new provision could be inserted into the Act that clearly specifies when a remote access search warrant is required. For example, it could be required if the thing to be searched is “any data not stored on the computer or device being searched nor on any computer connected to it”.

6.86 Obviously, this raises the question of what is “connected” to the computer being searched. We discuss options for clarifying that concept in our discussion on

---

57 Search and Surveillance Act 2012, s 103(6).
There may also be other ways of describing the type of remote data for which a remote access search warrant is required.

6.87 We note that this issue is related to our discussion in Chapters 2 and 9 about whether the Act should be clearer about what types of search activity and requests for information from third parties should require a warrant or other authorisation. Any recommendation to provide greater clarity on those matters should be consistent with the approach taken in relation to remote access searches.

**The meaning of “computer system” is unclear**

6.88 Section 110(h) of the Act states that a search power authorises the person exercising it:

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

6.89 This provision could be interpreted as authorising, without requiring further specific authority, access to data stored remotely, to the extent that data is part of the “computer system”. This power applies to both searches under a search warrant or under a warrantless power of search.

6.90 The key issue here is whether data stored via an internet-based storage facility is part of the “computer system” and, if so, whether that extends to Internet facilities that are public or controlled by an external person or organisation. One example of externally-controlled data stored remotely is Xero accounting software. Xero is a subscription-based accounting software tool for small to medium-sized businesses. In this system, all financial data is stored in the cloud and so can be accessed from any location and any computer. Does the storage of its financial data via an externally controlled Internet facility mean that it is not part of the “computer system” that the computer being searched is part of?

6.91 Unfortunately, the ambit of “computer system” is not clear. This is a problem because it means that it is also not clear what is authorised by the Act, what might be an

---

58 Emphasis added.
59 When a computer or device is searched under a warrantless power, data that is accessed remotely from that computer or device could be accessed without requiring further authority if it is part of the computer system to which that computer or device is connected. The warrantless search power does not authorise a search beyond that system.
unreasonable search under section 21 of NZBORA and what may be an offence under section 252 of the Crimes Act 1961 (accessing a computer system without authorisation).

6.92 The definition of “computer system” in the Act is borrowed directly from the Crimes Act:\(^{60}\)

\begin{verbatim}
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.
\end{verbatim}

6.93 The authors of *Adams on Criminal Law – Rights and Powers* consider that “computer system” extends to data on the Internet that is accessible from the computer being searched. The authors state:\(^{61}\)

A search of a computer network of a business, even though the server is at premises other than those being searched, is clearly contemplated by the definition. However, the definition would appear to be much broader and allow access to any web-based material that is accessible from a computer that is being lawfully searched. On this interpretation, a search of a Google account held by the owner of a computer in the premises being searched is permitted, whether or not the computer is logged on to Gmail at the time of the search and whether or not a password is required in order to access it.

6.94 Interestingly, the *Adams* commentary on the same definition in the Crimes Act (which is provided for the purpose of defining the ambit of certain computer crimes) dissects the definition and reaches slightly different conclusions on its ambit.\(^{62}\) In relation to the phrase “interconnected computer”, the authors suggest that there are two possible meanings, which depend on whether “interconnected” is measured by reference to the computer user or by reference to the operator or controller.

6.95 The first meaning is very broad. Under it, all the millions of computers that a user can access through the communication links of the Internet would be part of the computer

---

\(^{60}\) Crimes Act 1961, s 248; Search and Surveillance Act 2012, s 3.

\(^{61}\) *Adams on Criminal Law - Rights and Powers*, above n 29, at [SS3.09.01].

\(^{62}\) Simon France (ed) *Adams on Criminal Law - Offences and Defences* (online looseleaf ed, Thomson Reuters) at [CA248.03].
system, despite them being owned by diverse users, in different countries and operating to different technical specifications. The second meaning is much narrower. Under it, only the computers that are connected by the ability of a single person with appropriate authority within the system to determine how they operate would be part of the computer system. An example of this second meaning is a “local area network” of linked computers, which together provide computer services for a company, government agency or educational institution.

6.96 The authors of Adams suggest that the second, narrower meaning is more appropriate. This is because its focus on authorisation within the system ties into the lack of authorisation contemplated by the offences in the Crimes Act (such as the offence of unauthorised access to a computer system in section 252). Also, the broader meaning would make the concept of “communication links” used later in the definition redundant.

6.97 This raises a question about whether a broader or narrower interpretation of “communication links” is more appropriate in the context of the Act. If a wide meaning was adopted, that would capture the transfer of data to a cloud-based storage facility and would permit the searching of data remotely under section 110(h). If a narrower meaning was adopted, only data stored on other computers or devices able to be controlled by one authorised person (say within a local area network) could be accessed remotely under section 110(h). It would not cover data stored on the cloud.

6.98 This discussion demonstrates that at the very least, there is uncertainty about the ambit of “computer system”, what sort of remote searching would be permitted under section 110(h), and what would amount to an unauthorised search in terms of section 252 of the Crimes Act.

Options for reform

6.99 There is a variety of ways in which the Act could define the scope of remotely accessed data falling within the definition of “computer system”. First, in theory, it could rule out all data not stored on the computer being searched. If that is the case, the person executing the search would have to first disconnect the computer from any Internet connection and then make an image of its hard drive. Any data accessible from that computer but not stored on it would not be accessible under the power in section 110(h). However, it would be open to the enforcement officer to apply for a
remote access search warrant. This option has the advantage of being very clear. However, it also introduces significant impediments to the investigation of offences.

6.100 Second, the definition of “computer system” could distinguish between data that is stored on an Internet storage facility that is internally controlled or externally controlled. For example, if an organisation stores some of its data via an internet-based facility that is controlled by it and solely for its own internal use, that data would be part of the “computer system”. But data stored on an externally controlled internet-based facility (such as Xero) would not be part of that “computer system”.

6.101 The appeal of this distinction between internally and externally controlled Internet data storage facilities is that the available data is clearly within the network of the computer being searched. However, it may also be thought to be a rather arbitrary distinction. The decisions as to whether an organisation uses an internally or externally controlled Internet system are likely to have little to do with how much control the organisation wishes to have over the information. It is likely to regard both types of data as being within its organisational system.

6.102 Third, the definition could distinguish remote data based on factors such as whether:

- the computer was currently logged on to that Internet facility at the time it was searched; or
- the Internet data storage facility is always only accessed from the computer being searched.

6.103 However, the first factor also provides only an arbitrary link to the computer being searched and it could be very difficult for the second factor to be determined by the person executing the search.

The meaning of “not located at a physical address” is unclear

6.104 The Act uses the phrase “not located at a physical address that a person can enter and search” to determine when an issuing officer may provide specific authorisation for a remote access search. However, the meaning of that phrase is somewhat vague. All electronic data (even that stored in “the cloud”) is located on a server (or multiple servers) somewhere in the world. In theory, that place can be entered and searched, even if, in practice, that may not be practical. It is not clear whether the condition “that

---

63 Search and Surveillance Act 2012, s 103(6).
a person can [not] enter and search” is satisfied only if it is literally impossible or whether practical concerns such as lack of time, lack of money, or the fact it is in another country or located in multiple places could make it not possible.

Option for reform

6.105 If the preference for physical searches is to remain, the Act could at least be amended to be clear that the restrictions on the issuing of a warrant for remote access searches only apply where the thing to be searched does not have a physical address that can practicably be entered and searched. The introduction of this practicality element appears to reflect the original intention of the Act.

The ability to search remotely under warrantless powers is unclear

6.106 As mentioned above, the provisions in the Act relating to remote access searches relate to search warrants only. There are no similar provisions relating to the exercise of warrantless powers. This leaves enforcement agencies unsure about whether or not they may access data remotely in those circumstances.

6.107 The main concern with the access of remotely stored data under warrantless powers is the risk of “fishing expeditions”. While it is possible to adequately particularise the scope of a remote search in a warrant application (whether by providing the access information or other descriptions), there are no such checks on the exercise of warrantless powers. However, it may be possible to provide checks in other ways, for example, by reporting on the scope of the search after it has been conducted.

6.108 Of course, all warrantless search powers are exercised without a description of the scope of the search being approved in advance. This is justified because the thresholds for the exercise of warrantless powers require urgent circumstances: in other words, there is no time to obtain a warrant. Those thresholds themselves provide the check on the scope of the search. The question here is whether there is something unique about data accessed remotely that means that extra checks (over and above the existing thresholds for warrantless powers) are required, so that a warrant must always be obtained.

Q27 Is it clear when specific authority for remote access search is required? If not, what problems have you experienced?
There is no ability to postpone notification

6.109 Currently, there is no ability to apply to a judge to postpone the notice requirements for remote access searches, as there is for searches of premises or vehicles when the owner or occupier is not present.64 In those other cases, a judge may grant a postponement if satisfied that there are reasonable grounds for believing that providing notice as required would endanger the safety of any person or prejudice ongoing investigations.65

6.110 We have been told by enforcement officers that sometimes they obtain warrants for remote access searches at a point in time when it would be prejudicial to the investigation to require them to provide notice. This may be because the remote access search indicates the existence of data that may be evidence of the offence but was not covered by the first warrant. If notice is given at that point, the person to whom the search relates will be alerted to the investigation and may destroy any relevant evidence that has not yet been obtained.

6.111 We cannot see any reason to distinguish remote access searches from other types of searches on this basis. While remote searches are different in that (without being expressly notified) the operator of the database being searched often will not know about the search, the important point is that they are notified, not the timing of that notification. The justifications for deferring that notification therefore seem to apply equally to remote access searches as for other types of search.

Option for reform

6.112 If it was thought that notification about a remote access search should be able to be deferred, that amendment could be incorporated into the existing power in section 134 to apply to a judge for a postponement of the notification obligation.

Q28 If the Act continues to treat remote access searches differently, should it permit deferral of the requirement to provide notice after a remote access search has been conducted?

Information accessed remotely is often stored overseas

6.113 Finally, there is uncertainty about the ability of enforcement officers to access information stored on servers in other jurisdictions. Much evidential material from

---

64 Search and Surveillance Act 2012, s 134.
65 Section 134(3).
internet-based facilities will be of this nature – Google email accounts and Facebook postings are just two of the more common examples. Accessing data located in a different jurisdiction is likely to violate principles of customary international law, which prohibit law enforcement agencies from conducting investigations in other jurisdictions.66

6.114 In practice, third-party providers of Internet data services often comply with New Zealand law enforcement requests for data stored on servers in other jurisdictions, particularly if the provision of that data would constitute a minimal intrusion on privacy. However, in some cases there may be legal hurdles preventing the providers from complying. For example, in the United States the Stored Communications Act restricts the ability of telecommunications companies in that country to disclose the content of stored communications, including to foreign governments.67

6.115 If, for whatever reason, a provider refuses a request from a New Zealand enforcement agency, the agency may decide to continue the investigation as best it can without the information. Alternatively, it can embark on a request for mutual legal assistance under the Mutual Assistance in Criminal Matters Act 1992. Mutual assistance is a process that can facilitate the disclosure of information between countries for the purpose of investigating and prosecuting criminal offending. However, this process can be complex as different jurisdictions have different requirements that need to be satisfied before a request for mutual assistance will be entertained, and the process can sometimes take months to complete.68

The case for reform

6.116 The general prohibition (under customary international law) on conducting investigations in the territory of another State presents challenges for law enforcement agencies that wish to access data stored on servers located in other jurisdictions. In our view, it is arguable that we need legal mechanisms both to provide law enforcement agencies with access to data stored in other jurisdictions where this is appropriate, and

67 Stored Communications Act 18 USC § 2702.
to ensure that the privacy of data stored in this country is adequately protected from requests for access from law enforcement agencies in other jurisdictions.

6.117 This issue arose in a recent high profile case in the United States. In Microsoft Corporation v United States of America, federal law enforcement officers investigating drug offences sought and received a search warrant under the Stored Communications Act for email account information about a suspect held by Microsoft. Microsoft provided some account data that was held on servers in the United States. However, it refused to supply content data that was stored on servers in Dublin, Ireland on the basis that the data was beyond the territorial control of the law of the United States.

6.118 The question for the court was whether the warrant applied extraterritorially. The United States Government argued that the warrant required Microsoft to disclose the relevant records that were under its custody or control, no matter where those documents were located. Microsoft argued that warrants have territorial limits and do not extend to things located in other jurisdictions.

6.119 The Second Circuit Court of Appeals held that there was nothing in the Stored Communications Act that indicated an intention for the warrant to operate extraterritorially; and that the conduct in question (supplying the information) would occur overseas despite the fact the information could be accessed from the United States. In holding that Microsoft could not be compelled to produce the email information stored in Dublin, it said:

> Although the Act’s focus on the customer’s privacy might suggest that the customer’s actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer’s privacy takes place under the [Act] where the customer’s protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.

6.120 In reaching this conclusion, the Court emphasised that retrieving the data will necessarily require interaction with the Dublin data centre, which is located in a foreign sovereign State. While the Court recognised that its decision would seriously impede law enforcement investigations, it said the practical considerations did not overcome the interpretation that the warrant could only reach data stored within the United States.

---

69 Microsoft Corporation v United States of America 829 F 3d 197 (2d Cir 2016).
70 At 220.
**Options for reform**

6.121 At first glance it may seem that the logical solution to the problem of New Zealand enforcement officers not being able to readily access data stored overseas would be to amend the Act to give production orders extraterritorial effect. This could be done by specifying that the obligation in section 75(1) to disclose any relevant documents that are in the person’s possession or control extends to documents located in other jurisdictions. In practice, however, this would likely be unenforceable. The service provider in the foreign country might not be obliged to disclose the information and would be subject to the law of the foreign country.

6.122 An alternative solution adopted by some countries (notably Russia and Brazil) would be to enact a law that requires any company providing a service to New Zealand citizens to store all the related data in New Zealand. While the primary policy behind such a law is to protect citizens’ data from unauthorised access by foreign governments, it would also ensure that data generated by citizens is available to New Zealand’s enforcement agencies. However, data localisation policies have been criticised as being ineffective (data security is better protected by encryption than localisation) and as deterring growth and innovation due to the extra costs these policies impose on companies.

6.123 The most viable option for addressing the issue of cross-border access to data may involve international cooperation. The leading international instrument in relation to this type of cross-border assistance is the Budapest Convention. The Budapest Convention is a multilateral treaty adopted by the Council of Europe in 2001. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties. Chapter III of the Convention deals specifically with international cooperation and includes obligations relating to preservation (and limited disclosure) of stored

---

**Footnotes**


computer data, searches of stored computer data and interception of traffic (metadata) and content data.

6.124 As at October 2016, the Budapest Convention had been ratified by 49 States (including Australia, the United Kingdom, Canada and the United States) and signed by an additional six States. New Zealand is not a signatory to the Convention. However, Part V of the Commonwealth Scheme for Mutual Assistance in Criminal Matters (the Harare Scheme), of which New Zealand is a member, and the associated Model Legislation were drafted to give effect to Chapter III of the Convention. Therefore, while New Zealand is not legally bound by the Convention it has made a non-legally binding commitment to work towards compliance.

6.125 At present, New Zealand’s main mechanism for complying with Chapter III of the Convention is the Mutual Assistance in Criminal Matters Act 1992. The Law Commission recently reviewed that Act and made several recommendations designed to improve compliance with Chapter III of the Convention. This included a proposal that the Act should clarify that foreign countries may request New Zealand authorities to obtain a production order on their behalf. The Commission also proposed that there should be scope to use bilateral agreements to streamline the New Zealand process of approving and responding to such requests. If New Zealand ratified the Budapest Convention then it would have access to similar mechanisms for facilitating access to stored data that are available in other member countries.

6.126 In addition to ratifying the Budapest Convention, the United States and the United Kingdom have reportedly begun negotiations to enter an agreement to allow each of their domestic law enforcement agencies to issue warrants directly to communication

---


75 Not only is New Zealand a party to the Harare Scheme, it also developed an Action Plan to Fight Cybercrime in 2011 with the Quintet Commonwealth countries (Canada, the United Kingdom, the United States, Australia and New Zealand). The Action Plan concluded that all Quintet countries should take steps to become parties to the Budapest Convention.

76 Law Commission Extradition and Mutual Assistance in Criminal Matters (NZLC IP37, 2014) [EMA Issues Paper] at ch 17 generally and at [17.38]–[17.63]; and Law Commission Modernising New Zealand’s Extradition and Mutual Assistance Laws (NZLC R137, 2016) [EMA Report] at ch 17 (which contains a draft Bill). The Government has accepted the Commission’s recommendation that the Mutual Assistance in Criminal Matters Act 1992 should be replaced by new legislation and is currently considering the content of the draft Bill.

77 EMA Issues Paper, above n 76, at [17.38]–[17.43]; and EMA Report, above n 76, at 229 (cl 35(1)(a) of the draft Bill).

78 EMA Issues Paper, above n 76, at [17.108]; and EMA Report, above n 76, at 229 (cl 35(1)(b) of the draft Bill).
service providers in the other country to intercept communications or supply stored data for law enforcement purposes.\textsuperscript{79}

6.127 This type of agreement would bypass the request and approval process required under the Mutual Assistance in Criminal Matters Act 1992 and the need to obtain a production order under the Search and Surveillance Act. This would save time and would not present any conflict with the 1992 Act because that Act specifically states that it is not a code for international assistance in criminal matters.\textsuperscript{80} Such an agreement would, however, involve sacrificing a degree of sovereignty and control over the protection of individuals’ privacy in New Zealand. Whether that sacrifice would be warranted is a matter of international relations and is outside the scope of this review.

Q29 Should the Act be amended to facilitate access to evidential material stored overseas?

ASSISTANCE TO ACCESS COMPUTERS AND DEVICES

6.128 The Act empowers a person exercising a search power in respect of data held in a computer system or other data storage device to require a person to provide access information and other information or assistance that is reasonable and necessary to allow access to the data.\textsuperscript{81} While the section is broadly drafted, it is usually used to require people to provide passwords or encryption keys. It is an offence to fail, without reasonable excuse, to assist when requested to do so. A conviction makes a person liable to imprisonment for a term not exceeding 3 months.\textsuperscript{82}

6.129 Two issues arise in respect of this provision:

- whether the privilege against self-incrimination operates effectively in respect of this power; and
- whether the level of penalty for failing to comply with a request under this section is adequate.


\textsuperscript{80} Mutual Assistance in Criminal Matters Act 1992, s 5. The Law Commission recommended a similar provision in cl 10 of the draft Bill. See the EMA Report, above n 76, at 218.

\textsuperscript{81} Search and Surveillance Act 2012, s 130(1).

\textsuperscript{82} Section 178.
6.130 The first issue is discussed in detail in Chapter 8.

**Penalty for failure to assist**

6.131 Enforcement agencies have told us that the current penalty for failing to comply with a request under section 130 is not high enough to motivate compliance in some cases. Suspects will weigh up the possibility of a maximum term of three months’ imprisonment against the often much higher penalty they may face if the enforcement agency accesses the evidential material on their computer or electronic device. Often a rational decision is made to refuse to comply with the request for assistance.

6.132 One option is for the punishment to expressly provide for a fine as an alternative to imprisonment.\(^8^3\) It has been suggested that a fine might provide more motivation to comply with the request than a jail term. Different types of penalty will motivate different types of offenders. For some, the prospect of a short term of imprisonment may not be as intimidating as for others. This may be particularly relevant where financial crimes are being investigated and successful prosecution may lead to the offender losing significant sums of money obtained.

6.133 If the offence is amended to expressly include a fine, there is a question as to the amount of that fine. We note that the offence of resisting a search under the Serious Fraud Office Act 1990 makes a person liable on conviction to either imprisonment for a term not exceeding three months or to a fine not exceeding $5,000.\(^8^4\) Under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, the offences of obstructing an Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) supervisor and of providing false or misleading information to an AML/CFT supervisor carry penalties of up to three months’ imprisonment or a fine of up to $10,000 for an individual (or a fine of up to $50,000 for a body corporate).\(^8^5\) In line with these other statutes, it may be that a maximum fine in the range of $5,000–$10,000 is appropriate for the offence of failing to comply with a request to assist a computer search under the Act.

---

\(^8^3\) We note that, in theory, a court may already impose a fine. Section 39(1) of the Sentencing Act 2002 provides that a court may impose a fine instead of imprisonment where an enactment provides for imprisonment but does not prescribe a fine. However, we do not know how often a fine has been imposed for failing to comply with a request under section 130, if at all.

\(^8^4\) Serious Fraud Office Act 1990, s 47.

\(^8^5\) Anti-Money Laundering and Countering Financing of Terrorism Act 2009, ss 102, 103 and 105.
Of course another option would be to increase the maximum term of imprisonment. However, we do not currently favour that option because the length of imprisonment for failing to assist would not be equivalent to the level of penalty for the offence under investigation. Any increase would therefore be unlikely to provide any additional motivation to comply with the request.

Q30 Should the penalty for failing to provide access assistance be amended (for example, to explicitly provide for a fine as an alternative to imprisonment)?