Chancery Chambers
Level 4
2 Chancery Street
Auckland City 1010
New Zealand
PO Box 58
1010 Auckland
DX CP24001
09 303 5270
thelawassociation.nz

2 November 2023

Review of the Search and Surveillance Act 2012
Law Commission
By email: **ss1@lawcom.govt.nz**

Te Arotake Tuatoru i te Evidence Act 2006 | The Third Review of the Evidence Act

The Law Association Incorporated ("TLA") is a membership organisation representing over 5000 lawyers nationwide. The TLA Technology & Law ("Committee") have consulted on the ***Te Arotake Tuatoru i te Evidence Act 2006, The Third Review of the Evidence Act 2023 Issues Paper***. The Committee thanks the Law Commissioner for the extension of time in which to file these submissions in anticipation of the final report to be finalised on 24 February 2024.

Introduction

1. This is a commentary upon Chapter 6 of the Law Commission Issues Paper on the Third Review of the Evidence Act. It is designed to provide a basis for further discussion. It is not a comprehensive analysis of Chapter 6 but highlights some issues that the Committee regard as significant around searches and seizure of digital data.

2. Chapter 6 is directed towards searches of and for digital data and addresses the following issues:

    (a) a comparison between physical and digital searches;

    (b) irrelevant and privileged material;

    (c) remote access searches; and

    (d) the provision of assistance to computer and devices.

3. The approach of the Commission is to examine the law in practice since the enactment of the Act in 2006, identify any problems or shortcomings, propose a number of possible options and finally pose questions to answer. This response draws on some of the issues raised that had been raised in the Committee's submissions to the Commissioner in respect of the *Search and Surveillance Act 2012 review*.

Physical vs digital

4. There is a fundamental difference between searches in the physical realm and the digital realm. While initially it was thought that it was best to treat the two as the same, the extraordinary developments between 2006 and 2023 suggest that it is time to revisit the assumptions underlying the search provisions in the Act.

5. The Committee welcomes further opportunities to engage with the Law Commission on these broader points in the New Year.

Section 30 reform

6. There is a broader overall point with deficiencies in the search process which is that defence lawyers are left to rely on section 30 to deal with any issues. The Issues Paper notes that the Commission is currently reviewing section 30 of the *Evidence Act* as part of the review of the *Evidence Act* and it is therefore not considered in any detail in this issues paper.

7. Challenges to unlawful searches after the fact are a very limited form of accountability on enforcement agencies. This is a good opportunity to reform the law so that it promotes best practice for law enforcement agencies and encourages pro-active steps to protect rights in addition to the safeguards such as section 30.

Physical and Digital Searches

8. When the Commission examined searches relating to digital material in 2007 it concluded 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*."

9. That approach was adopted by the Act and upon an application for a search warrant there is no distinction made between whether the material is likely to be found in physical or digital form. The rules are effectively "technology neutral" although there are some specific criteria set out in relation to certain electronic searches.

10. The Law Commission observes that there "seems to be no debate that the legal threshold for searching electronic material should be the same as for physical material." However, it observes that there are some practical difficulties when it comes to issues such as:

    - the inadvertent capture of irrelevant or privileged material; and
    - determining how the rules relating to remote access searches are to apply.

11. The legal threshold for the issue of a search warrant should apply equally to physical and digital searches. However, the way in which those searches take place and the manner by which digital data is acquired and managed upon the execution of a search – either with or without a warrant – need to be clarified.

12. There is good reason for this. It lies in the fact that information or data in digital form is paradigmatically different from physical items or information recorded on paper in what

is described as “kinetic space”. It is not just a matter of tangible versus intangible. It lies in the fact that in the kinetic space information is generally fixed and static whereas in the digital space it is volatile and dynamic. Kinetic information is not corrupted when handled. Digital information may be transformed. The content of kinetic information is generally apparent on the face of it. Digital information requires the intermediation of software and hardware to be comprehensible. The relevance of kinetic information is generally apparent at the time it is located. Digital information often requires forensic analysis. Kinetic information may be read without corrupting or changing associated information. Digital information or its associated data may be corrupted or changed if directly accessed upon a computer, laptop, tablet or mobile phone. With kinetic information essentially “what you see is what you get”. With digital information there is inevitably metadata that underlies the *ex facie* information.

13. Although the Act recognises these paradigmatic differences in sections 110(i) and 125(m) there is a significant difference in the way in which searches may be carried out between those where a warrant is required and those where it is not.

14. The methodology of search is discussed at paragraphs 6.12 and 6.14. Briefly stated, the search of a device on private property normally will require a warrant. In contrast, and the Law Commission notes this at para 6.13, 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 a manual search of the phone (refer sections 88 and 125(l)).

15. The only justification for a warrantless search of a device under section 125(l) is that data may be deleted or destroyed in the time that it takes to get a warrant from an issuing officer.

16. That justification is without foundation. The integrity of data may be maintained if the device is *seized* at the time of apprehension and access to its storage or memory disabled pending a warrant to examine the device being obtained. The evidential material is retained but the officer does not have the power, without a warrant, to trawl through its contents seeking relevant information. Given the nature of mobile phones as set out in *Riley* v *California*, a warrant should be obtained.

Capturing the Data

17. The Commission deals with this at paras 6.15 – 6.16. It is our view that this should only be done pursuant to a warrant.

Searching the Data

18. It is in this area that there is potential for invasion of privacy, the acquisition of irrelevant information or breaches of privilege. The Commission observes that where information acquisition or examination is carried out by a Digital Forensic Unit there is less likelihood of these problems arising. The Commission points out the detail that may be required where a search warrant is granted including possible restrictions on how a search of electronic material must be conducted to minimise the risk of investigators seeing

irrelevant or privileged material. It also points out that similar restrictions do not apply to warrantless searches. This emphasises the need for a warrantless "search" to be limited to seizure in the case of digital data.

19. The qualities of digital information mean that there are tools available that will, if not eliminate the discovery of irrelevant or privileged material, restrict or limit its discovery. Although it is unlikely, given the absence of sophisticated technological knowledge by issuing officers, conditions involving the use of what are termed "e-discovery tools" such as keyword searches, concept searching, de-duplication and the like could be deployed. A further alternative is that suggested by Baragwanath J in Chief Executive of the *Ministry of Fisheries* v *United Fisheries* – the employment of a neutral third party to isolate privileged or irrelevant material.

Plain View

20. Dr David Harvey has commented elsewhere as to the applicability of the "plain view" doctrine and section 123. The Law Commission acknowledges that the plain view doctrine 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.

21. We find it odd for the Commission to then suggest that this is not seen as a problem with the plain view rule itself. The Committee disagrees. The plain view doctrine developed in the kinetic space and depends upon the limits of perception. The deployment of digital forensic tools may make a search more "targeted" as suggested but the "plain view" doctrine can be invoked if items "of interest" are found. Our view is that if a search is authorised for one purpose, evidence unassociated with that purpose should not be admissible.

Too Much Information?

22. In paragraphs 6.31 – 6.33 the scope of searches is considered, noting that digital searches capture more data than evidential material sought, and that in searching digital material, those searches must be targeted. The problem arises in that the potential to "see" irrelevant material is much higher in a digital search.

23. We refer to our earlier suggestion about conditions on search warrants. The deployment of e-discovery tools, designed to reduce volume and disclose only relevant material, will resolve this difficulty.

Privileged Material (Paras 6.35 – 6.40)

24. The procedures for invoking privilege in the *Search and Surveillance Act* (Sections 140 – 147) are premised upon material in the kinetic rather than the digital space. Furthermore the invocation of privilege is somewhat retrospective. A more proactive approach is required.

25. The paper describes the process that is used by the IRD (6.37 – 6.38) which are interesting and perhaps go part of the way towards addressing the problem. A more rigorous

approach, which builds upon the decision of Baragwanath J in *United Fisheries*, may be found in *US* v *Comprehensive Drug Testing*. In that case the Ninth Circuit Court of Appeals placed the responsibility for privilege protection squarely in the lap of the person issuing the search warrant and requires the imposition of conditions upon the search process. The power to order conditions is present in the *Search and Surveillance Act* section 103(3) and (4)(i). The use of this power received lukewarm mention from the Supreme Court in *Dotcom* v *AG* and there was certainly no enthusiasm for the imposition of conditions.

26. Nevertheless, conditions about dealing with digital data upon seizure to ensure privilege is properly protected, along with focussing the search upon relevant material should provide strong protections in addition to those provided in sections 141(a) and 147(a).

27. The difficulty with coming to grips with such problems and the reluctance to adopt an exceptionalist approach to digital material is understandable. A consistent approach across all media is to be preferred. What the drafters of the statute and the appellate Court have failed to understand is the paradigmatically different nature of information in the digital space and that it has additional underlying qualities that simply are not present for search targets in the kinetic space. The ease of retrieval of digital material, its location often on a single medium (be it a hard drive, a USB stick or in the Cloud) and the ability to copy the entire volume of the medium together with the ability to carry out a search through that material create both an advantage and a disadvantage. The advantage is that information may be located easily. The disadvantage is that relevant information is located amongst information possessed of a number of different qualities, be it irrelevant, personal and private, as well as privileged. The "scattergun" way in which information is retained on storage media means that investigators have the ability to look at all the information that is there. Yet within both those advantages and disadvantages lies the answer – as Charles Clark said in another context "the answer to the machine lies in the machine". We have already referred to software or e-discovery tools that can reduce volume and separate out material that is relevant. The deployment of these tools, possibly by a neutral party as suggested in *United Fisheries* or *Comprehensive Drug Testing*, provides an acceptable solution.

Options for Reform (Paras 6.41 – 6.56)

28. The options for reform that are suggested are, regrettably, limited. The focus is primarily upon privilege protections.

29. As will be apparent from the above discussion there need to be other protections in place. Documenting search procedures (para 6.42 – 6.44) certainly is necessary to ensure the integrity of the examination process. But protections must be in place earlier than that.

30. There should be provision for seizure of a digital device in the case of a warrantless search but a search of the content of the device requires a warrant with conditions as to the manner of the search to ensure location of relevant material and to protect privacy, privilege and irrelevant material. This may require issuing officers to upskill so that they may craft meaningful search conditions and for requesting investigators to specify the information sought with some accuracy and detail so that proper search terms can be crafted.

31. These protections are suggested at para 6.45 relating to privileged material, but as suggested the protections should not be limited to that area alone. The temptation for investigators to indiscriminately trawl through data rather than identify with precision what is required must be resisted.

32. The concerns expressed in para 6.49 about unduly restrictive conditions can be alleviated by the ability for the investigator to increase the scope of the search with a fresh application. The concerns expressed about conditions limiting the parts of a machine which may be searched clearly demonstrate a misunderstanding of the way in which search software and e-discovery tools may be deployed. The search process implied in bullet point 2 of para 6.50 is that of "manual review" – a very slow, intrusive and time consuming process. Software tools are available which would expedite this sort of search.

33. A further step suggested is the imposition of a statutory duty to minimise access to privileged and irrelevant material similar to section 140(2)(a). Para 6.54 proposes a solution but my suggestion is that software tools should be deployed to assist in privilege and privacy protections, but rather than have a statutory provision mandating the use of software tools, which puts the "power" in the hands of the investigator, the utilisation of such tools should be defined by the issuing officer who the provides a supervisory power over the process.

Remote Access Searches

34. The statutory provisions relating to remote access searches are, to say the least, opaque. We have always envisaged those provisions as either:

    (i) authorising access to and search of a seized digital device at a site other than that of the physical search, although the cloning provisions of section 110(i) suggests otherwise; or

    (ii) authorising access to a digital device or data storage facility (referred to as a "thing") without a specified or identifiable physical location by means of a network or the Internet.

35. The latter option seems to be more logical but there are problems with the language used and clear confusion about the way in which networks operate. For example the provisions of section 132 are premised upon the ability to send an email message advising of the remote access search. This may reflect the level of understanding (or lack of it) of the nature of remote searches or communications protocols that are available on the Internet.

36. The various problems with remote access searching are clearly identified in the Law Commission paper – para 6.57 and following.

37. Our view is that there must be a provision for the ability to search a data storage system by means of network or wireless links. However, the extraordinarily opaque language surrounding remote access searches needs to be addressed. The use of the word "thing" is simply absurd. Device would make things very clear.

38. The adoption of the *Crimes Act* definition of "computer system" is problematic. That definition potentially may extend to the internet – para 6.93 – although there is some difference of opinion on the part of commentators suggesting a local area network is what was intended. (Para 6.97). I favour the latter interpretation. The definition of a computer system was settled in 1999 when the computer crimes provisions of the *Crimes Act* were introduced. The Internet was then in its infancy. When the legislation was enacted (2003) the definition was not reworked to clarify the scope of the definition. There were a number of other drafting anomalies as well. But by 2003 the internet was well established and its potential was becoming clear. In a discussion that Dr David Harvey has had with Dr Warren Young, he expressed favour with a more expansive definition.

39. The problem that the wider interpretation creates is that a remote access search has extra-territorial application. Although the Court of Appeal has recognised this – see *R* v *Stevenson* – and has covered itself by suggesting that such a warrant would be unenforceable, basic principles of international law relating to sovereignty as illustrated in the *Microsoft Ireland Case* make it clear that such searches can only take place within the domestic jurisdiction. The activities of the NSA as described in the Snowden revelation make it clear that cross-border remote access searching is possible, but "because we can" is a proposition that runs up against Rule of Law principles.

40. Thus, any changes to remote access searching would have to make it clear that such searches are limited to devices located within the domestic jurisdiction and cannot extend off-shore unless it is with the consent of a person authorised to access those devices or has control of access to such devices. The definition of a computer system would have to be revisited both in the *Search and Surveillance Act* and in the *Crimes Act.*

41. The Issues Paper makes it clear that there are alternative ways of ensuring access to off-shore data. International co-operation per medium the provisions of the Budapest (Cybercrime) Convention or via MACMA arrangements are two examples. The Law Commission suggests (para 6.127) that consideration of such matters is beyond the scope of the review, but in our view they must be considered if meaningful and lawful methods of conducting off-shore digital searches are going to take place.

Section 125(1)(l)

The Argument Outlined

42. If the provisions of section 125(1)(l) and (m) allow a warrantless search of data, the scope of the search power is significantly wider than that authorised by section 110(h) and (i) which require a warrant.

43. This being so there is an advantage to invoking a section 88 search power and obtain without a warrant evidence of information that would otherwise require an application for a warrant and the obligation to satisfy the issuing officer of grounds.

44. The result is that the intrusiveness of a search under section 125(1)(l) is significantly greater and requires virtually no threshold to engage it other than section 88. This has significant implications for the citizen's privacy interests and tilts the tension between

State interest and individual interest markedly in favour of the State and significantly against the individual.

45. There are reasons why a warrant is necessary to access a computer system pursuant to section 110(h) not the least of which is the issue of privacy of personal data.

46. A section 88 arrest engaging a search power under section 125 especially of a cell phone has significant privacy implications that should be protected by a warrant. This is confirmed when one looks at the progressively intrusive scope of the search powers commencing at section 125(1)(i) and following.

47. A nuanced approach to the scope of the search power under section 125(1)(l) should be adopted so that the power is restricted to seizure of the cell phone with a requirement that data access would require a warrant to be consistent with the approach under section 110.

The Argument Developed

Section 125(l) wider than section 110(h) and (i)

48. The starting point in this argument is the privacy interests of the citizen. The privacy of the citizen in his or her dwelling is a fundamental one. In *R* v *F* the High Court observed that "the sanctity of the home and the right to privacy in a dwelling ... is a fundamental right of importance to New Zealanders."[1] In *F* v *R* the Court of Appeal noted that "a person's home has long been recognised as a special place where a person's fundamental right to privacy is protected from unauthorised interference."[2]

49. It is for this reason that a search of premises requires a warrant to be issued after proper grounds have been established.[3]

50. Once a warrant has been issued a search power may be exercised pursuant to it.[4] Included in the search powers, as long as a search of computer systems is authorised by the warrant, are the following:

> (h) 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:
>
> (i) if any intangible material accessed under paragraph (h) is the subject of the search or may otherwise be lawfully seized, to copy that material (including by means of previewing, cloning, or other forensic methods either before or after removal for examination).[5]

51. It should be noted that section 110 addresses search powers which means a search warrant issued under the *Search and Surveillance Act 2012* and any enactment that is set

---

[1] *R* v *F* [2013] NZHC 1686 at [41].
[2] *F* v *R* [2014] NZCA 313 at [23].
[3] *Search and Surveillance Act 2012* sections 98 - 100.
[4] *Search and Surveillance Act 2012* Section 110.
[5] *Search and Surveillance Act 2012* section 110 (h) and (i).

out in column 2 of the of the Schedule which contains powers in other enactments to which Part 4 of the *Search and Surveillance Act* applies. Search powers also extend to powers conferred under the *Search and Surveillance Act* or the enactments in the Schedule involving the entry and search, inspection or examination without a warrant, any place, vehicle or other thing or to search a person.

52. The specific powers granted under section 110 (h) and (i) recognise that computer and data storage systems present unique challenges for investigating officers.

53. This was recognised by the Law Commission in 2007 when it stated:

> *"We have considered the potential impact of computer searches on human rights values such as privacy, outlined in Chapter 2. The computer is a powerful repository of private information that has no exact equivalent in tangible terms. A person subjected to a search may be more concerned about law enforcement agencies accessing their computer than their premises, because of the complete picture that may be revealed about them. This is due to the range of information that may be present on a computer, such as personal correspondence, appointment diary, personal diary, business dealings, financial, banking and tax records and medical information. This information may also exist in tangible form, but tangible information is more likely to be dispersed throughout the premises and the specificity of the warrant is likely to preclude access to all of that information. In searching a person's computer, the concern is that a large amount of information of many different types, unrelated to the basis for the search, is potentially accessible."*[6]

54. The development of information and communication technologies has advanced since 2007 especially in the development of the mobile phone and the smart phone. As submitted above, these devices are computers and are certainly data storage devices. The privacy interests in these devices has been remarked upon by the Supreme Court in *Dotcom* v *Attorney General*[7] where it was stated:

> "[191] … *searches of computers (including smart phones) raise special privacy concerns, because of the nature and extent of information that they hold, and which searchers must examine, if a search is to be effective. This may include information that users believe has been deleted from their files or information which they may be unaware was ever created. The potential for invasion of privacy in searches of computers is high, particularly with searches of computers located in private homes, because information of a personal nature may be stored on them even if they are also used for business purposes. These are interests of the kind that s 21 of the Bill of Rights Act was intended to protect from unreasonable intrusion*.
>
> [192] *Accordingly, for a search of any computer to be reasonable, a [warrant] must give specific authorisation for the computer to be searched in order to identify and seize the data that it is believed is evidence of commission of an*

[6] Law Commission *Search and Surveillance Powers – Report 97* (Law Commission, Wellington 2007) para 7.14 p. 197.
[7] [2014] NZSC 199.

offence. For a warrant to include such authority there must have been must have been sufficient sworn grounds in the application to support its issue in that form."

55. In saying this the Supreme acknowledged the observations of the Supreme Court of the United States in *Riley* v *California*[8] and of the Supreme Court of Canada in *R* v *Fearon.*[9]

56. In *Riley* the Court made the following observations about cell phones and their unique characteristics:

> *Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term ''cell phone'' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*
>
> *One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J.L. & Pub. Pol'y 403, 404–405 (2013). Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick, supra, rather than a container the size of the cigarette package…..*
>
> *But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. See Kerr, supra, at 404….*
>
> *Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.*
>
> *The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information— an address, a note, a prescription, a bank statement, a video— that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back*

[8] 134 S. Ct 2473 (2014).
[9] [2014] SCC 77.

> *to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.*
>
> *Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013). A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. See, e.g., United States v Frankenberry, 387 F.2d 337 (C.A.2 1967) (per curiam). But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. See Ontario v Quon, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."*[10]

57. In *Riley* the United States Supreme Court held that a warrant was needed before the contents of a mobile phone could be examined.

58. The case of *R* v *Fearon*[11] recognised the potential for a more significant invasion of privacy than the typical search incident to an arrest. However, the Court found that the common law power to search incident to an arrest permitted the search of cell phones and similar devices, although privacy interests meant that modification of the common law framework was necessary.

59. The majority of four Judges considered that four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with section 8.

60. **First**, the arrest must be lawful. **Second**, the search must be truly incidental to the arrest. This requirement should be strictly applied to permit searches that must be done promptly upon arrest in order to effectively serve the law enforcement purposes. In this context, those purposes are protecting the police, the accused or the public; preserving evidence; and, if the investigation will be stymied or significantly hampered absent the ability to promptly conduct the search, discovering evidence. **Third**, the nature and the extent of the search must be tailored to its purpose. In practice, this will mean that only recently sent or drafted emails, texts, photos and the call log will, generally, be available; although other searches may, in some circumstances, be justified. **Finally**, the police must take detailed notes of what they have examined on the device and how they examined it. The notes should generally include the applications searched, the extent of the search,

[10] *Riley v California* above n. 11 pp 2489 – 2490.
[11] Above n. 12.

the time of the search, its purpose and its duration. The record-keeping requirement is important to the effectiveness of after-the-fact judicial review. It will also help police officers to focus on whether what they are doing in relation to the phone falls squarely within the parameters of a lawful search incident to arrest.

61. The minority of three judges placed greater weight on the privacy implications of the search of an electronic device. The minority considered that although a cell phone may be seized upon arrest the search of its contents should be pursuant to a warrant.

62. The New Zealand Supreme Court in *Dotcom* considered that its approached conformed broadly with *Riley* and *Fearon;* and indeed recognised that on occasion privacy interests might need to be protected by the imposition of conditions by the issuing officer, although as a general rule that would not be necessary.[12] A more stringent approach was adopted by the Ninth Circuit Court of Appeals in *United States* v *Comprehensive Drug Testing Inc.*[13]

63. From these cases the following general principles can be identified.

    (a) there is a high expectation of privacy in private premises;

    (b) there is a high expectation of privacy in regard to the contents of a cell phone or smart phone. This arises from the nature of the device and the technological enhancements that accompany it. Similar privacy expectations would probably not apply were the device used solely for voice communication with an associated record of calls made and call destination or origin data.

    (c) in cases where there is a high expectation of privacy a search warrant to enter, search and seize will be required. There must be an evidential foundation provided that crosses a certain threshold to justify the issue of a warrant.

    (d) the warrant must be reasonably specific in that if a search power under section 110(h) or (i) is to be exercised, the warrant will need to specify and authorise that.

64. There is an exception to the requirement for a warrant. That is provided in section 15 of the *Search and Surveillance Act*.[14] It allows a warrantless search and the exercise of search powers in serious cases where there is an element of emergency.

65. The circumstances in which a warrantless search of premises may take place are limited. There must be suspicion of serious offending (section 15(a)), and coupled with that a belief that evidential material is present in the particular place and that delay will mean that the material may be destroyed, concealed, altered or damaged.

---

[12] *Dotcom* above fn10 at [194].

[13] 621 F 3d 1162 (9th Cir 2010). Such conditions could include the involvement of an independent third party to oversee the search of data and ensure privacy and privilege protections – for a New Zealand example see the judgment of Baragwanath J in *Chief Executive of the Ministry of Fisheries* v *United Fisheries* [2010] NZCA 356; [2011] NZAR 54.

[14] For a recent example where section 15 was considered see *Kalekale* v *R* [2016] NZCA 259.

66. The language of the section envisages a limited set of circumstances that will justify a warrantless search of premises and all those circumstances must be present. This recognises the high expectation of privacy attaching to premises.

67. The privacy interests that attach to a cell phone located in a dwelling can be overridden by a search warrant or in the extreme circumstances envisaged by section 15.

68. The provisions of section 88 coupled with section 125 seem to significantly lower the threshold in regard to cell phone privacy expectations. Yet the data contained on the cell phone when present on premises and on the person of the individual on the street or arrested remains the same. There seems to be no reason why the contents of a cell phone should be treated differently based upon mere location.

69. The threshold for a warrantless search under section 88 is significantly lower than under section 15. For example, the seizure of evidential material under section 15 may take place if it relates to the offence and if entry is delayed there is a likelihood that the material may be compromised.

70. In the case of digital data such material on the device – say a cell phone - may be altered, damaged or deleted. Thus the warrantless seizure in cases of emergency under section 15 may be justified.

71. Section 88 applies to the search of a person who has been arrested or detained. The search may be directed towards evidential material relating to the offence in respect of which the person is arrested or detained.15

72. The tension that exists, however, is that a personal search is seen as more intrusive than a premises search.[16]

Invoking the section 88 power

73. There is an advantage in the ability of the officer to invoke the section 88 search power.

74. That power is engaged upon arrest or detention. Arrest or detention may be based upon suspicion or cause to suspect. The threshold is less than that required to satisfy an issuing officer to issue a search warrant.

75. Once the section 88 power is invoked, the officer has available the provisions of section 125 which relate to personal searches.

---

[15] Section 88(2)(c).

[16] See *R* v *Phohretsky* [1987] 1 SCR 945 at para [5] where it was stated that "a violation of the sanctity a person's body is much more serious than that of his office or even of his home". In New Zealand it was held that "personal search is a restraint on freedom and an affront to human dignity". *R* v *Jeffries* [1994] 1 NZLR 290 at 300. See also *R* v *Williams* [2007] NZCA 52, para 113, where the Court of Appeal reaffirmed the highest expectation of privacy relates to searches of the person.

Intrusive search under section 125(l)

76. The search power rules contained in section 110 are replaced by the provisions of section 125. The provisions relating to computer or data systems in section 110(h) and (i) are replicated in section 125(1)(l) and (m).

77. Should this extend to a cell phone? Remembering that the privacy interest in the data contained on the cell phone is the same regardless of location. An expansive interpretation of the section would suggest an affirmative answer.

78. It is submitted that the privacy interest in cell phone data and contents suggests a more nuanced approach.

79. It is acknowledged that the *seizure* of a cell phone or data storage device is justified absent a warrant. This is consistent with the warrantless seizure of evidence pursuant to section 15(b)(ii) and conforms with the minority position in *Fearon.*

80. Under the expansive approach the advantage enjoyed by the State is significantly greater in the case of the application of sections 88 and 125 than in the case of a premises search.

81. This is notwithstanding the fact that the privacy interest in the data on the cell phone has not changed. Although the volume of the data may be modified whilst the individual is away from his or her premises, there seems to be little reason to ascribe a lower privacy interest in digital data.

82. Under the expansive approach the officer may scroll through the data on the cell phone without any sort of warrant and view information that, were the phone to have been located in a dwelling, would have required the authorisation of a warrant.

Reasons why a warrant is necessary to access a computer system pursuant to section 110(h)

83. Why should there be a warrant required to access a computer system or computer data?

84. Prior to the enactment of the *Search and Surveillance Act* the rules relating to searches were designed with tangible items in mind. Tangible information material is capable of being searched – see the references to documentary searches in sections 125(1)(k) and 110(g).

85. The Law Commission recognised the qualities of computer-based information, anticipating the observations of the Courts in *Riley, Fearon* and *Dotcom*. The Law Commission observed:

> "*The computer is a powerful repository of private information that has no exact equivalent in tangible terms. A person subjected to a search may be more concerned about law enforcement agencies accessing their computer than their premises, because of the complete picture that may be revealed about them. This is due to the range of information that may be present on a computer, such as personal correspondence, appointment diary, personal diary, business dealings, financial, banking and tax records and medical information. This information may also exist in tangible form, but tangible*

information is more likely to be dispersed throughout the premises and the specificity of the warrant is likely to preclude access to all of that information. In searching a person's computer, the concern is that a large amount of information of many different types, unrelated to the basis for the search, is potentially accessible." [17]

86. The Law Commission did not support the suggestion that there should be a separate search and seizure regime for computers. It observed:

> "*Accessing computer systems and seizing intangible material for law enforcement purposes constitutes such an interference with privacy rights that computer searches should be subject to and regulated by the search and seizure regime. However, 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. We recommend that computer searches should generally be regulated by the search and seizure regime that applies to tangible items (subject to any necessary modification), in preference to creating a different regime carrying more restrictive requirements*."[18]

87. The Law Commission was also alive to the issue of the seizure of irrelevant data, referring to the case of *Calver* v *District Court at Palmerston North*[19] where it was held that the search power did not authorise the seizure of irrelevant material and that any sifting process needed to be carried out at the warrant premises. The issue of removal of the computer system and taking forensic copies was further analysed and considered in *A Firm of Solicitors* v *District Court at Auckland.*[20] The recommendation of the Law Commission was to clarify the law to allow for the access and copying of material on computers or data storage devices. The taking of a forensic copy preserved the integrity of data which might be changed by the simple operation of switching a computer on or off.[21]

88. A further issue considered by the Law Commission was the specificity of the search and made the following observation:

> "*An additional specificity issue arises in the context of computer searches. Regardless of the degree of specificity of the data sought by the search, it is arguable that the nature of the storage medium gives rise to an increased risk that irrelevant material will be searched. Computer searches generally involve a great deal of irrelevant material that is intermingled with evidential material. A US commentator has argued that the particularity requirement does not impose the same restrictions on searches of computers as it does in the physical context due to the following factors:*
>
> > *the large amount of information held on computers (compared to the*

[17] Law Commission *Search and Surveillance Powers* above fn. 9 para 7.14 (footnotes omitted).
[18] Ibid. para 7.19.
[19] [2005] DCR 114.
[20] [2006] 1 NZLR 586.
[21] Law Commission *Search and Surveillance Powers* above fn. 9 para 7.3 and 7.32.

amount of potential physical evidence in a search of premises);

the fact that electronic evidence can be hidden anywhere, so that the usual rule limiting a search for tangible items to places where the evidence described in the warrant might conceivably be located does not provide the same limitation in a search for intangible items;

the thorough nature of a forensic examination of a computer compared to a physical search of premises; and

the fact that computer searches typically occur off site in the police computer laboratory and are not limited by the same time constraints as a search of premises.

The interplay of these factors gives rise to a perception that computer searches are at risk of becoming a general trawling exercise, rather than a focussed search for particular material. We have therefore considered whether there should be controls on the way that the computer search is conducted in order for the search to be sufficiently limited."[22]

89. Despite the fact that the Law Commission did not consider that a separate regime for computer searches was justified, nevertheless the observations made about computer searches make it clear that there is a recognition that computer data presents a different paradigm from a search of kinetic material.

Limitation of section 88 search

90. When a search power is invoked under section 88 the scope of the search, if it involves a cell phone, should be limited to seizure of the cell phone. The reasons for that are as follows:

- the search power is highly intrusive and is recognised as more so than a property search;
- unless the search falls within the ambit of section 15 a search of premises requires a warrant;
- that warrant must be specific enough to include computer equipment; and
- normally computer data would be forensically cloned before examination. Accessing computer data on site by turning the machine on (or off) would impact upon data integrity.

91. The anomaly arises with an arrest and the invocation of the section 88 search power.

92. Under the expansive definition of the way in which the search may be exercised employing section 125(l) an investigating officer could open, turn on and "trawl" through data on a laptop being carried by the suspect on the pretext that there may be evidential material available.

[22] Ibid. para 7.57.

93. A similar outcome could apply to a cell phone.

94. The privacy implications of data stored on a computer and on a cell phone are no different.

95. The risks of interference with data on the device are eliminated by the act of seizure and removal from the possession of the suspect.

96. The Legislature could not have intended that a more intrusive search regime should be applicable consequent upon a section 88 search of the person with associated power to access data storage devices at the time of the search than was applicable to a premises search other than in the circumstances contemplated by section 15 and which involved actually accessing the device.

Warrant to access

97. As matters stand the seizure and search of a cell phone creates an anomaly. As has been demonstrated, by adopting the expansive interpretation different rules apply to a property search involving computers and data storage devices from those attendant upon an arrest.

98. Consistency of approach, the highly intrusive nature of a personal search and privacy interests in the data stored on a cell phone or other data storage device warrant the approach that was adopted by the minority in *Fearon.*

99. The device may be seized for the purposes of preservation of the data or evidential material – if any – thereon.

100. Any subsequent search of the device utilising the forensic cloning or indeed previewing of the data should be pursuant to the authorisation of a search warrant.

The Technology & Law Committee are keen to continue to consult and dialogue on the *Search and Seizure Act* review with the Law Commission. Please feel free to contact us should you wish any clarifications or would like us to respond to any questions you may have about these submissions by liaising with the Committee Secretary, Moira McFarland at moira.mcfarland@thelawassocation.nz or 09 306 5742.

_____

Lloyd Gallagher
Convenor
The Law Association Law & Technology Committee