REMOTE SEARCHING: TRAWLING IN THE CLOUD

CHRIS PATTERSON*

The Search and Surveillance Act 2012 (SSA) allows the Police and other enforcement agencies to perform remote searches of data. All searches are, however, subject to the overriding but not absolute principles of the New Zealand Bill of Rights Act 1990 (the BORA), in particular s 21. The application of the BORA should provide a balance between the acts of an enforcement agency carrying out its investigative role and an individual's right not to be subjected to unreasonable search and seizure. Such a right should extend to the protection of an individual's privacy in respect to data stored on internet cloud based servers, requiring enforcement agencies to obtain a warrant in order to search that data. However increasingly, data is stored offshore which gives rise to a number of jurisdictional issues.

The few co-operative arrangements that exist between states are at present considered necessary in order to prevent reciprocated aggressive searches.[1] *Any search undertaken pursuant to these arrangements, and in accordance with the SSA, will in most cases be considered a lawful search. However, if a search is undertaken of a target computer from which the location is unknown or authority has not been granted by the governing territory, should the search be considered unlawful?*

This article will argue that any Court faced with a remote cross border search will need to consider the implications and application of the BORA as well as whether or not the SSA has an extra territorial effect. This article will also argue that data obtained via remote searching is likely to be considered unlawful in terms of the minimum rights prescribed by the BORA. The article concludes with the proposition that legislative amendments are necessary to provide better guidance and clarity as to the scope of remote searching.

I. INTRODUCTION — THE NEXT PHASE OF THE DIGITAL REVOLUTION — CLOUD COMPUTING

The significant advancements during the last 30 years in information communication technologies (ICT), has heralded an unprecedented and exponential increase in the creation and storage of information. It is arguable

* LLB\BCom (Hons), admitted as a barrister and solicitor of the High Court of New Zealand, admitted as a barrister in the High Court of Australia, Supreme Court of New South Wales and Supreme Court of Queensland. Acknowledges and is grateful for the review comments provided by Nicola Hartwell, Laura Cole and anonymous reviewers. All URL references were accurate as of 2 July 2016.

[1] See the Convention on Cybercrime CETS 185 (opened for signature 23 November 2001, entered into force 1 July 2004). Note, despite Recommendation 7.13 of the Law Commission *Search and Surveillance Powers* (NZLC R79, 2007) at 229, New Zealand has not sought to become a party to the Convention. For a discussion and commentary on the convention see: Alana Maurushat "Australia's Accession to the 'Cybercrime Convention': Is The 'Convention' Still Relevant in Combating Cybercrime in the ERA of Botnets and Obfuscation Crime Tools?" (2010) 33 UNSWLJ 431.

that smartphones can be described as mobile portable computers given they share a number of characteristics, including having a processor. The average smartphone user spends more time on their device using the internet or a wide range of applications for communication, work and/or entertainment, than making phone calls. A standard smartphone has more computing power and storage capability than many commercial mainframe computers of the 1980s. Whilst denied, some have attributed Bill Gates as saying that "64 kbps is more memory than most computer users will ever need". Whether or not this statement was in fact made, advances in technology have established that significantly more is required to drive modern technology. Now most New Zealanders have an ability to obtain and create what would have been unimaginable 20, or even 10, years ago in terms of receiving, creating, sharing and storing vast volumes of data.

Large quantities of the data created by individuals is personal in nature. The proliferation of personal data gives rise to a number of serious privacy and freedom from unreasonable search issues. The drafters of the New Zealand Bill of Rights Act 1990 (the BORA) would likely not have considered, or even contemplated, the implications that it would have on the creation and collection of personal data stored on personal electronic devices. They certainly would not have appreciated the impact that cloud computing would have on the day-to-day lives of many New Zealanders.

The digital landfill each individual creates on a daily basis includes, at one end, information that could be described as digital waste, such as a deleted application and its associated files, and at the other, highly personal and sensitive information such as bank account details. There may be, and often is, more than one location in which an individual's digital files are stored, especially if he or she uses more than one device.

Physical devices are not the only data storage technology used by individuals. Increasingly we are utilising the cloud to store files.[2] Storage of personal information in the cloud has become, in many cases, completely seamless. An example is the automatic uploading of photographs taken on smart phones to a cloud storage application such as Dropbox or iCloud. So what exactly is the cloud? The United States Department of Commerce National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[3]

[2] Louis Columbus "Roundup of Cloud Computing Forecasts and Market Estimates, 2016" *Forbes* (online ed, United States of America, 13 March 2016).
[3] Peter Mell and Timothy Grance "The NIST Definition of Cloud Computing" Special Publication 800-145 (28 September 2011) NIST <http://www.nist.gov/> at 2.

In the absence of syncing their local computer and cloud account, if a Dropbox user wishes to access their files in Dropbox, as with any other cloud based service, they can only do so by remote means. The user has to login to the relevant cloud service using their account details. A user can then conduct as many remote searches of the files that are contained within their account as they like. However, what if that person is not the account holder? What if that person is a member of an investigating authority which has been issued with a warrant to remotely search a specific user's account? What are the key legal issues that arise and would they justify one or more amendments to the SSA?

II. From the Physical to the Purely Intangible

The case law in respect to computer searches both here in New Zealand and overseas has focused on the search and seizure of physical equipment, documentation, or information obtained at a specific location. The search and seizure of computer equipment is usually authorised by way of a warrant that prevents those executing the warrant from being otherwise liable in either trespass and/or conversion. Warrants are required to provide sufficient particulars so as to enable those subjected to the execution of a warrant to ascertain the scope and bounds of the authority granted to those who are executing the warrant. It is a long-standing rule that a general warrant is invalid.[4]

Striking an appropriate balance to ensure that an individual is free from being subjected to an unnecessary search and seizure and ensuring his or her right to privacy is protected, can and should be provided for by way of conditions contained in the warrant as stipulated by the issuing officer. The conditions applicable to computer searches can be separated into two groups or categories. These are items that can be seized and then searched, and items which are seized after the initial seizure and search. In relation to the latter, it is not uncommon to utilise forensic tools to search for relevant data. To varying degrees, forensic technology is used to remain within the scope of the warrant by filtering and separating the data which is relevant from that which is irrelevant or subject to legal privilege. This point, however, is unsettled.

On one hand, authorities have suggested that the police are able to use forensic technology to identify privileged material.[5] Equally, the courts have also suggested an independent examiner locate the privileged material instead.[6] This latter view is consistent with the view in the United States in *United States v Comprehensive Drug Testing*.[7] It is the author's opinion if a balance is to be struck in a manner to protect legal privilege, the approach taken in the United States in *United States v Comprehensive Drug Testing* is to be followed.

[4] *Dotcom & Ors v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745, (2014) 27 CRNZ 537, minority at [32] and majority at [71].
[5] At [204].
[6] *Chief Executive of the Ministry of Fisheries v United Fisheries Ltd* [2010] NZCA 356, [2011] NZAR 54 at [59] per Baragwanath J dissenting in part.
[7] *United States v Comprehensive Drug Testing* 579 F 3d 989 (9th Cir 2009) at 1006.

Otherwise, it is leaving material in the hands of the organisations in charge of prosecution to protect the interests of the accused.

III. The Purpose of a Remote Search

Investigative authorities undertaking a remote search are doing so because either the account user is unwilling or unable to provide, or is likely to attempt to destroy or conceal, relevant evidence if advised that the account is of interest to the investigative authority. A remote search gives the investigative authority access to a remote device, application or email account which then enables the investigator to copy, pursuant to any warrant conditions, the data contained within the remote device. An example could be all of the emails stored in a specific Hotmail email account. An investigator will in most, if not all, cases want to copy the data contained in the account for subsequent forensic analysis.

Criminal enterprise has been quick to adopt and use, whether intentionally or otherwise, new technologies to evade the authorities and conceal evidence of criminal activity. The risk of digital evidence being erased is a common concern for investigators. Investigators will, at a minimum, seek to preserve relevant or potentially relevant evidence before it can be erased or moved elsewhere for concealment. The challenge for law enforcement agencies is the same across a number of nations. As Brenner has noted:[8]

> Law enforcement officers from various countries are grappling with the conflict that currently exists between the need to deploy "computer intrusion techniques that exist in a legal gray area" if they are to battle cybercrime effectively and the need to preserve individual privacy.

IV. Legislative Framework

A. New Zealand Bill of Rights Act 1990

Section 21 of the BORA codifies the common law principle that individuals have a right to be free from unreasonable search and seizure. The codification of the rights set out in s 21 is consistent with New Zealand's international commitment to arts 17.1 and 17.2 of the International Covenant on Civil and Political Rights, by ensuring that all persons within New Zealand are not subjected to "arbitrary or unlawful interference with [their] privacy, family, home or correspondence ..." and that each person has the "right to the protection of law against such interference or attacks".[9]

[8] Susan Brenner "Law, Dissonance, and Remote Computer Searches" (2012) 14 NCJL & Tech 43 at 91-92 quoting Ryan Gallagher "US and Other Western Nations Met with Germany over Shady Computer-Surveillance Tactics" *Slate* (United States of America, 3 April 2012).

[9] International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 Dec 1966, entered into force 23 March 1976).

Section 21 provides:

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

There is a large volume of case law relating to the application of s 21.[10] In the context of seizure and search of data pursuant to a warrant, the Supreme Court in *Dotcom & Ors v Attorney-General*[11] (*Dotcom*) affirmed the Court of Appeal's acknowledgement in *Tranz Rail Ltd v Wellington District Court*[12] that general warrants are invalid and in breach of s 21 of the BORA.

The Supreme Court in the *Dotcom* case held:[13]

> 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.

The threshold issue in which the Courts interpret statutory provisions authorising searches is beyond the scope of this article and will not be traversed.

B. Search and Surveillance Act 2012

The warrant issued in the *Dotcom* case was granted by the District Court at Auckland pursuant to the Mutual Assistance in Criminal Matters Act 1992 less than three months before the commencement of the equivalent empowering section contained in pt 4 of the SSA. The passing and commencement of the SSA does not diminish the underlying principles of s 21 of the BORA. The Law Commission has stated that:[14]

> … section 21 will remain as an important statement of general principle that will guide the interpretation and application of the search and seizure provisions that we propose, just as it is currently.

The relevant empowering sections of the SSA relating to remote searches are s 103, which sets out the form and content of search warrants, and s 111 which provides:

> Remote access search of thing authorised by warrant
> Every person executing a search warrant authorising a remote access search may —

[10] See also s 5 of the BORA which enables the Courts to apply s 21 to statutory searches. See also *Hamed & Ors v R* [2012] 2 NZLR 305 which, in the context of a surveillance, confirms at [11] that "the values protected by s 21 are not simply property-based, as were the common law protections which preceded it. Rather, they provide security against unreasonable intrusion by State agencies into the personal space within which freedom to be private is recognised as an aspect of human dignity."

[11] *Dotcom & Ors v Attorney-General*, above n 4, minority at [32] and majority at [71].

[12] *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [38] and [41].

[13] *Dotcom & Ors v Attorney-General*, above n 4, at [191].

[14] Law Commission, above n 1, at 2.49.

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

"Remote access" is defined as "a search of a thing such as an internet data storage facility that does not have a physical address that a person can enter and search".[15]

"Internet data storage facility" is not defined in the Act. Most, if not all, cloud apps and remote email accounts, including Hotmail,[16] Gmail,[17] Google Drive[18] and Dropbox[19] being the type of material that will be of interest to an investigative authority, are all internet data storage facilities as they are all accessed via the internet and they store data. However, cloud apps and remote email accounts also store data on computer servers. The applicable computer servers are located at specific addresses or physical locations. It would be fair to assume that the respective addresses where each server is located is a physical address that a person can enter and search given that a person, such as an employee or contractor engaged by the cloud service provider, would have had to enter the address in order to install and maintain the server.

A "person" is not defined in the SSA, although the ordinary meaning of person can likely be assumed.[20] "Search" is also not defined, however this is likely for consistency with s 21 of the BORA in which a definition for "search" is also omitted. Blanchard J, when considering what constitutes a s 21 "search" in *Hamed v R,* adopted the view of the Supreme Court of Canada in *R v Wise*[21] when he stated "if the police activity invades a reasonable expectation of privacy, then the activity is a search."[22] In a cloud app context, a remote search would be considered a search in terms of the *Hamed v R* guidelines as a person would have a reasonable expectation that law enforcement agencies do not trawl through his or her accounts, particularly given the majority of accounts are protected by passwords. It could also be interpreted by reference to its common usage in computing i.e. the act or process of electronically viewing data. However, a good reason to omit providing a statutory, or indeed judicial, definition of the term is to keep it technologically neutral given the advancement in techniques used to perform a search, and an individual's expectation of privacy, may change over time.

---

[15] Search and Surveillance Act 2012 (SSA), s 3.
[16] <http://www.hotmail.com/>.
[17] <http://www.gmail.com/>.
[18] <http://www.google.com/drive>.
[19] <http://www.dropbox.com/>.
[20] Interpretation Act 1999, s 29.
[21] *R v Wise* [1992] 1 SCR 527.
[22] *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305, (2011) 25 CRNZ 326 at [163].

C. Check and Balance – Issuing Officer Approval

The requirement that a remote search must be authorised by a warrant is the one and only check and balance provided for under the SSA. The issuing officer will be reliant on the enforcement agency applying for the warrant to provide them with "full information to allow him or her to assess"[23] the appropriateness and necessary specifics of a warrant.

An obvious difficulty in achieving an effective balance in the context of a remote search is the issuing officer's dependence on the enforcement agency providing sufficient information to enable the issuing officer to make an informed decision. Issuing officers are not currently required by law to have sufficient, or even any, knowledge of the technical and legal issues associated with a remote search.[24] The Court of Appeal in *A Firm of Solicitors v District Court at Auckland* in the context of a computer search by the Serious Fraud Office suggested that:[25]

> … the jurisprudence that has developed in relation to [civil search][26] orders in the civil jurisdiction of the High Court could provide useful guidance in the development of appropriate procedures in cases [involving privilege].

A key aspect of civil search orders is proportionality. The scope of a civil search order should be no greater than is necessary to ensure that relevant evidence is located and secured. The obligation rests on the applying party to make full material disclosure so that the judge considering the application can balance the competing interests of both sides. It is perhaps too much to expect an enforcement agency will always adhere to the strict requirements of the High Court Rules and general jurisprudence relating to search orders. However, to enable the appropriate balance to be struck it has to be recognised that not all, if any, issuing officers will necessarily have the specific technical and legal experience required to be able to fully consider an application for a warrant to authorise a remote search. It would go some way forward to improving the likelihood that the correct balance will be struck if the application followed a process similar to a civil search order. As an example, the application should include an affidavit from a forensic information technology expert setting out, in everyday language, what the scope of the warrant sought will entail, what processes will be followed to minimise or eliminate access to irrelevant material, and what steps will be taken to avoid and protect inadvertent access to personal information.

---

[23] *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 at [76].
[24] David Harvey *Internet.law.nz* (4th ed, revised, LexisNexis, Wellington, 2016) at [8.369 - 8.374].
[25] *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 at [140].
[26] The Court of Appeal referred to an Anton Piller order. A number of safeguard conditions arising out of the Anton Piller jurisprudence are found in pt 33 of High Court Rules which came into effect on 1 February 2009. See also, for a general commentary of the search order jurisprudence, RA McGechan (ed) *McGechan on Procedure* (looseleaf ed, Brookers) at [HRPt 33].

D. Possible Fine Tuning (s 357)

Section 357 of the SSA requires the Minister of Justice to call for a joint review of the operation of the SSA by the Law Commission and Ministry of Justice. The joint review must be completed by the delivery of a report to the Minster of Justice within one year i.e. by 30 June 2017. On 28 June 2016 the Minster of Justice, pursuant to s 357, referred a review to the Law Commission.[27] One of the three terms of reference is "whether any amendments to the Act [the SSA] are necessary or desirable".[28] On 28 June 2016 the Law Commission issued a media release that contained the following Q&A:[29]

> Will the impact of new technology be considered in the review? Yes. For example, since the Act was enacted in 2012 there has been a significant increase in the use of smart phones and "the cloud" to store information. Also, technology presents Police and enforcement officers with new ways to investigate crime that were not envisaged in 2012. The review will examine whether the provisions of the Act provide adequate powers and protections in light of these changes.

Given the purpose of remote searches as discussed above, the definition of "remote search" and s 111 should both, or at least one, be amended to meet the objective of creating "greater consistency and transparency in the way in which such [remote] search … powers [are] carried out".[30] I suggest that a number of amendments relating to remote searches should be considered. These include:

- The definition of "Remote Access Search" in s 3 should either remove the words "that does not have a physical address that a person can enter and search" or, alternatively, a reasonable practicality exception should be included. The wording could be amended to "that has a physical address that a person cannot reasonably, for practical purposes, be expected to enter and search". Such an amendment would reduce any arguments that a server hosting a cloud app that is the subject of a warrant is located at a physical address. It is accepted that the amendment proposed would keep the door open to more cross border searches. It is only a question of striking an appropriate balance.

  Reasonable practicality could be determined in terms of a balancing exercise. Putting aside the jurisdictional implications which are addressed later in this article, reasonable practicality may include a risk that data could be destroyed or concealed during the passage of time, or in circumstances where it is unreasonable to expect an investigating authority to travel to far flung locations to physically undertake a search of a server, such as when it is known the relevant server is located elsewhere, for example, travel to Singapore in order to physically undertake a search of a server.[31]

---

[27] Law Commission "Search and Surveillance Act 2012" (28 June 2016) Law Commission <http://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012>.
[28] Law Commission "Terms of Reference for the Statutory Review of the Search and Surveillance Act 2012" (28 June 2016) <http://www.lawcom.govt.nz/>.
[29] Law Commission "Law Commission Begins Joint Review of the Search and Surveillance Act 2012" (press release, 28 June 2016) <http://www.lawcom.govt.nz/>.
[30] Law Commission "Law Commission Begins Joint Review of the Search and Surveillance Act 2012" (press release, 28 June 2016) <http://www.lawcom.govt.nz/>.
[31] As an example Microsoft Inc has its cloud computing Microsoft Office 365 servers which are accessed by New Zealand customers located in datacenters in Singapore: "New Office 365 Datacentres" (8 February 2015) <http://imageframe.co.uk/new-office-365-datacentres/>.

- Another section that would be desirable to amend is s 111(b). It is difficult to comprehend a remote search that did not include "any intangible material". All remote searches by their very nature involve "intangible material". Data is merely electronic information, which by its very nature is therefore "intangible material".[32] As tangible material can only be searched via direct means, by its very nature it needs to be located somewhere physical. Therefore, a person (such as an investigator) could physically enter the address of where the tangible material is located and undertake the search in person. The simple amendment is to delete from s 111(b) the words "if any intangible material in the thing is the subject of the search or may otherwise be lawfully seized".

V. Jurisdiction – The Problem of Remote Cross Border Searches

The issue of jurisdiction does not arise when an investigator searches and seizes, for subsequent examination, a device located in New Zealand. Likewise, putting aside the issues identified above in relation to the current wording of the legislation, a remote search undertaken in respect to a server located in New Zealand is unlikely to raise any jurisdictional issues. If, however, a data centre is located outside New Zealand, as is the case for a large majority of data centres, an issue as to jurisdiction will arise. The former Solicitor-General, Michael Herron QC, has commented that: "This jurisdictional point is likely to be the biggest obstacle to using remote access searches effectively."[33] In some jurisdictions, such as Germany, the use of remote searches are prohibited on constitutional grounds,[34] and in others are indefensible.[35]

Recognising and respecting territorial sovereignty is an important obligation of every responsible nation. Michael Sussmann[36] makes it clear that customary international law prohibits conducting an investigation in the territory of another state. He suggests that "[g]overnments have three potential solutions". These are to either:

1. Forego the development of principles, allowing for each country to decide for itself whether trans border searches constitute an acceptable law enforcement practice;
2. Limit trans-border searches to cases where production of the data could otherwise be compelled though [domestic] legal processes; or
3. Creating principles permitting law enforcement agencies to conduct trans-border searches under clearly defined circumstances.

---

[32] Data is defined as quantities, symbols and characters that are transmitted or stored via electrical signals on, or through, a computer: English Oxford Living Dictionary <https://en.oxforddictionaries.com/definition/data>.

[33] Michael Heron and Dale La Hood *Search and Surveillance Act 2011 – New Powers* (New Zealand Law Society, 2012) at 32.

[34] Steven Bellovin, Matt Blaze and Susan Landau "Comments on Proposed Remote Search Rules" Computer Science at Columbia University <http://www.cs.columbia.edu/> and Alana Maurushat "Australia's Accession to the Cybercrime Convention: Is The Convention Still Relevant In Combating Cybercrime in the ERA of Botnets and Obfuscation Crime Tools?" (2010) 33(2) UNSWLJ 431.

[35] *Microsoft Corporation v United States of America* 829 F 3d 197 (2nd Cir 2016).

[36] Michael Sussmann "The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium" (1999) 9 Duke J Comp & Int'l L 451 at 471–472.

As will be evident above, New Zealand has adopted, in s 111, Sussmann's third solution but without any "clearly defined circumstances". The absence of specificity in s 111 is, in my view, a serious matter that needs to be addressed. Legislation is presumed to only have domestic application (i.e. no extra-territorial application) unless the wording of the legislation explicitly or implicitly creates extra-territorial effect.[37] Otherwise, the aim of striking the appropriate balance between effective criminal investigation and the protection of individual privacy cannot be met.

It is expected the New Zealand public would be concerned if a foreign power started undertaking remote searches on computer systems based in New Zealand, and which contained personal information relating to New Zealand citizens and/or residents. However, what is good for the goose should also be good for the gander. The use of reciprocal assistance arrangements is one way to respect territorial sovereignty and operate within agreed bounds. Simply legislating empowering authority for New Zealand enforcement agencies to conduct, albeit with a warrant, remote cross border searches is unlikely to enhance New Zealand's reputation within the international community. There is a real risk that a New Zealand enforcement agency may commit an offence under the laws of a foreign country, such as Germany, simply by executing a remote cross border search. This should not be ignored.

The Law Commission was alive to some of the risks mentioned above but nevertheless went on to recommend that remote cross border searches be permitted subject to the search being:[38]

- limited to open-source (publically available) data; or
- conducted in accordance with mutual assistance arrangements in place between New Zealand and the relevant jurisdiction; or
- specifically authorised under a search warrant.

The first of the three conditional recommendations cannot be justified if one accepts that the harm created by a remote cross border search is not just in terms of the data obtained on an individual level, but more importantly the "intentional interference with the searched state's power to provide privacy or property protections within its territory".[39]

The Law Commission's first two conditional recommendations, on their face, do not appear to be too objectionable. However, they never made their way into s 111. Rather, it was the third condition which is reflected. A remote search, under

[37] For example, s 144A of the Crimes Act 1961. See also *LM v The Queen* [2014] NZSC 110, [2015] 1 NZLR 23 at [38] per Glazebrook and Arnold JJ as authority for extra-territorial application of party offences under s 144A despite s 6, which limits the extra-territorial application of the Act unless it is provided for in the Act or any other enactment. The case involved a situation in which the appellant was a New Zealander, but the party who committed the alleged offending was not a New Zealander, and therefore under New Zealand law did not commit an offence. Note the author was counsel for the appellant.

[38] Law Commission, above n 1, at Recommendation 7.12.

[39] Patrica L Bellia "Chasing Bits Across Borders" (2001) U Chi Legal F 35 at 74.

the SSA, must be authorised by a search warrant. This condition alone ignores the risks, legal and reputational, associated with remote cross border searches. Instead, it expressly authorises a remote cross border search provided that the authorisation has been granted, via a warrant, by an issuing officer.

The SSA does not contain any express extraterritorial authority. The Supreme Court has held, in the general context, that "the default position is that New Zealand criminal law does not apply extraterritorially".[40] Presumably, the same can be said that criminal procedure including the authority to authorise a remote search, by default, would not extend beyond New Zealand. The Law Commission has noted that "there is a customary international law prohibition on conducting investigations in the territory of another sovereign state".[41] New Zealand investigative authorities usually have to rely on mutual assistance arrangements with other jurisdictions to facilitate or carry out investigative processes outside of New Zealand that require legal authorisation, such as the obtaining and execution of a search warrant overseas.

In the absence of an express power the courts could be asked to interpret s 111 as having an implied extraterritorial effect. It is arguable that s 111 should not be read as implying a right to undertake a remote cross border search. Nothing in the wording of the section would suggest that a remote cross border search "goes without saying". Additionally, the implication of an extension of jurisdiction beyond New Zealand is not necessary to give effect to any commitments made by New Zealand in terms of its international obligations.

A review of Hansard relating to the SSA provides no insight into the intention of the legislature with respect to territorial sovereignty.[42] The Law Commission, in its final report, made a number of key recommendations relating to searches of computers including providing "statutory authorisation for law enforcement agencies, when exercising search powers to: … conduct remote cross border searches in limited specific circumstances."[43]

VI. Comparative Analysis

The scope of this article only allows a short comparative analysis of two jurisdictions - Canada and the United States. The United States is an obvious choice due to its size and influence as a first mover in respect to the ongoing development of jurisprudence relating to the internet and, therefore, cloud computing. Canadian law provides insight into this issue from a common law perspective.

[40] *LM v The Queen*, above n 37, at [16]. Note that exceptions do exist, see ss 7 and 7A of the Crimes Act 1961.
[41] Law Commission, above n 1, at 7.109.
[42] (04 August 2009) 656 NZPD 5399; (1 March 2012) 677 NZPD 761; (7 March 2012) 678 NZPD 933; (20 March 2012) 678 NZPD 1095; (22 March 2012) 678 NZPD 1245.
[43] Law Commission, above n 1, at 7.9.

The Canadian Federal Court (the Federal Court) in *Re X* reviewed an application for a warrant to conduct mobile phone surveillance by the Canadian Security Intelligence Service (CSIS).[44] The Federal Court's judgment, delivered by Justice Richard Mosley, affirmed the position taken by the Canadian Supreme Court in *Hape* that:[45]

> … it is a well established principle that a state cannot act to enforce its laws within the territory of another state absent either the consent of the other state or, in exceptional cases, some other basis under international law.

In *Re X* the CSIS were not seeking judicial authorisation to violate any foreign law "but acknowledged that was the likely effect of the activities for which authorization was sought".[46] The Federal Court had to consider whether it had jurisdiction to "authorize acts by the CSIS in [Canada] which entails listening to communications and collecting information abroad."[47] The Canadian Federal Court appointed, and had the benefit of, one of her Majesty's Queens Counsel as an amicus curiae to assist in determining the issue. The Federal Court appears, while not exactly clear from the judgment, to have rejected the submission of the amicus that:[48]

> … the Service could not execute a warrant obtained under s 21 [Canadian Security Intelligence Service Act RSC 1985] and exercise its information gathering powers in another country unless it had obtained the permission of the country where the targets were located or was a party to a treaty or agreement covering the use of its powers in that country.

The Federal Court noted that Canada had participated in the development of, and signed, the Convention on Cybercrime (the Convention) but had not ratified the Convention due, in part, to "the legislation required for domestic implementation of the data preservation and disclosure measures" having a "potential impact on privacy issues".[49] The Federal Court, in approving the issuance of a cross border warrant, distinguished "the norms of territorial sovereignty" from the exercise of a country's enforcement jurisdiction. The Federal Court held that the CSIS's statutory authorisation is "not subject to territorial limitation" and that there was nothing unlawful in the CSIS collecting from Canada information that was located outside of Canada.[50] With respect to the Federal Court, its analysis and reasoning lacked any reasonable level of theoretical rigor. The Federal Court took the position that, provided the CSIS was initiating its investigative processes within Canada, it mattered not that those

[44] *Re X* 2009 FC 1058, [2010] 1 FCR 460.
[45] *R v Hape* 2007 SCC 26, [2007] 2 SCR 292 at [65].
[46] *Re X*, above n 44, at [11].
[47] At [27]. The Canadian Federal Court, at [59], reframed the issue as being "whether the Court may authorize the CSIS to listen to and record the communications at a location within Canada" and then. at [64], "whether the Court may authorize such actions in Canada knowing that the collection of such information in a foreign country may violate that state's territorial sovereignty".
[48] At [11].
[49] At [71].
[50] At [75].

processes would cross borders and therefore infringe the territorial sovereignty of one or more other nations.

The first instance judgment of the United States Magistrate Judge James C Francis IV in *A Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* (*Microsoft*) commenced with a quote:[51]

> The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactory, by any current territorially based sovereign.[52]

The United States District Court (the US District Court) in *Microsoft* had to consider a challenge by Microsoft against the issuance of a warrant to search for data on one of its servers located in Dublin, Ireland.[53] Under the warrant Microsoft was directed to produce emails of one of its customers saved on its server. Microsoft unsuccessfully argued that "Federal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States."[54] The US District Court held that Microsoft's analysis was inconsistent with the legislation that authorised the issuing of the warrant. Importantly, the US District Court accepted the United States Government's argument that the warrant was a hybrid, being part warrant and part subpoena in that:[55]

> It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause … On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premise of the ISP to search its servers and seize the e-mail account in question.

On that basis the warrant, as argued by the US Government and accepted by the US District Court, did "not implicate principles of extraterritorially".[56] The US District Court also commented on the practical implication of treating the warrant as a conventional search warrant in that "it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty" which, especially if there is no treaty in place, "make it unlikely that Congress intended to treat [an] order as a warrant for the search of premises located where the data is stored".[57] The issuance of the warrant was upheld and Microsoft's motion to quash it was dismissed.

---

[51] *A Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 15 F Supp 3d 446 (SD NY 2014).
[52] David Johnson and David Post "Law and Borders — The Rise of Cyberspace" (1996) 48 Stan L Rev 1367 at 1375.
[53] Issued pursuant to s 2703(a) of the United States' Stored Communications Act (commonly known as a "SCA Warrant") which is part of the Electronic Communications Privacy Act of 1986 18 USC (US).
[54] *A Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, above n 51, at 470.
[55] At 471.
[56] At 472.
[57] At 475.

The United States Court of Appeals has subsequently overruled the decision.[58] It affirmed Microsoft's argument that Congress' characterisation of the instrument as a warrant carried traditional territorial limits.[59] Nothing in the Stored Communications Act explicitly or implicitly suggested the application of the warrant overseas.[60] Requiring Microsoft to comply with the warrant in this situation would require ignoring the Supreme Court's repeated emphasis of the presumption against extraterritoriality. The Court stated it did not have the freedom to do so.[61]

One of the issues facing remote cross border searches initiated in the United States is the Constitutional Fourth Amendment (the Fourth Amendment). The Fourth Amendment is the closest equivalent to s 21 of the BORA. The approach of courts in the United States to issuing warrants authorising remote cross border searches has been criticised for allowing the United States government to "run roughshod over territorial-based limitations" contained in the Fourth Amendment.[62]

In 2013, the United States judicial approval for remote cross border searches was firmly brought into question. In *re Warrant to Search a Target Computer at Premises Unknown*, the United States District Court declined an application by the Federal Bureau of Investigation (FBI) for a warrant to conduct a remote access search.[63] The reason given was out of a concern that Federal Rules of Criminal Procedure 41 (Rule 41) places a restriction on a judge's authority to issue only warrants within his or her district. That requirement cannot be met if the judge does not know where the computer server that is the subject of the warrant is located. To get around this issue the Department of Justice wrote to the Advisory Committee on Criminal Rules suggesting amendments to Rule 41. In response, on 28 April 2016 the United States Supreme Court issued a letter to the United States Congress advising it of a number of changes to the Federal Rules of Criminal Procedure (FRCP) including an amendment to Rule 41 authorising a magistrate judge to issue an extraterritorial remote search warrant.[64] The amendment to the FRCP will take effect on 1 December 2016 unless the United States Congress passes legislation preventing the amendment.

The amendment to Rule 41 proposes:

> Rule 41. Search and Seizure
> (b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

[58] *Microsoft Corporation v United States of America*, above n 35.
[59] *Microsoft Corporation v United States of America*, above n 35, at 5.
[60] *Microsoft Corporation v United States of America*, above n 35, at 6.
[61] *Microsoft Corporation v United States of America*, above n 35, at 6.
[62] See Jennifer Daskal "The Un-Territoriality of Data" (2015) 125 Yale LJ 326.
[63] *Re Warrant to Search a Target Computer at Premises Unknown* 958 F Supp 2d 753 (SD Tex 2013).
[64] Supreme Court of United States *Proposed Amendments to the Rules of Criminal Procedure* (28 April 2016, Supreme Court of the United States) <www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf /> at 6 – 7.

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 USC § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The amendment proposed introduces express extraterritorial effect provided the location of the computer server has been concealed, or five or more computers owned by financial organisations or the United States Government that are located in different districts have been damaged. Zack Lerner argues, amongst a number of points, that:[65]

> … the need for extraterritorial authority only extends to the acquisition of a user's most basic identifying information [and that] after collecting the user's IP or MAC address, the FBI can, and should continue its investigation as if the suspect had never concealed his or her identity in the first place.

Section 111, as enacted, contains no such condition.

VII. Conclusion

Sections 3 and 111 of the SSA require a number of general drafting amendments including refining the meaning of "remote search" and removing the reference to "intangible material".

The current joint review of the SSA by the Law Commission and the Ministry of Justice provides an opportunity to question whether s 111 strikes an appropriate balance between the legitimate need for enforcement agencies to investigate crimes and ensuring freedom from unreasonable searches or invasions of privacy. In my opinion s 111 gives enforcement agencies more authority than is necessary to identify and obtain relevant evidence. Too much reliance is then placed on the issuing officer to ensure that appropriate conditions are imposed to act as a counterbalance. Issuing officers cannot be expected to act as an effective independent safeguard given the complex and multi-layered technical and legal issues that require consideration. A possible solution may involve:

- Requiring enforcement agencies to utilise mutual assistance arrangements;
- Expressly limit remote searches to within New Zealand; and/or
- Require enforcement agencies to make full material disclosure and provide expert evidence as to the steps that will be taken to eliminate or mitigate any intrusions against individual privacy.

The circumstances where remote searches may be required will only increase with time. The fifty-nine words that make up s 111 are not sufficient to carry the

[65] Zack Lerner "A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure" (2016) 18 Yale JL & Tech 26.

weight necessary to strike the appropriate balance between the conflicting interests of the state and the individual.