Submission

Search & Surveillance Bill

3rd September 2010

Tech Liberty

http://techliberty.org.nz

PO Box 5641
Lambton Quay
Wellington

Introduction

Thank you for the opportunity to make a submission on the revamped Search & Surveillance Bill.

About this submission

This submission is split into two sections:

1. General comments about the Bill
2. A more in-depth look at the issues around computer searching.

Request to speak

We understand that the Committee is not intending to conduct further public hearings, but we would appreciate the chance to make a submission in person if possible.

About the submitter

Tech Liberty is dedicated to protecting people's rights in the areas of the Internet and technology. We make submissions on public policy, help to educate people about their rights, and defend those whose rights are being infringed.

Contact us

Enquiries can be directed to Tech Liberty's spokesperson, Thomas Beagle, on 021-80-50-40, thomas@techliberty.org.nz or at PO Box 5641, Lambton Quay, Wellington.

1. General comments about the S&S Bill

While we appreciate the proposed changes to the Bill, we still hold grave concerns about the general thrust of the Bill towards increased powers for search and surveillance.

We have the following comments on some of the issues raised by the Summary Departmental Report.

Enforcement and Regulatory Agencies

The report talks about the scale and complexity of the Bill and how this makes it hard to understand, something that has not been improved in the latest version.

We believe that a significant part of the confusion around the Search and Surveillance Bill is caused by the way that it tries to cater for the requirements of both enforcement and regulatory agencies. This makes the Bill very hard to follow as it is hard to tell which parts apply to which types of agencies.

The conflation of these two types of agencies has also contributed to the "take a power given to one agency and give it to all of them" which has led to absurdities such as allowing city councils to apply for warrants for covert video surveillance.

We recommend that the Bill be split into two, with one bill for enforcement agencies and another for regulatory agencies. This would be similar to the way that the Official Information Act has two versions, one for central government and one for local government. We believe that this would substantially improve the clarity of the law and allow for more flexibility in drafting.

Safeguards and the principle of notification

The report shows that a significant number of submissions have raised concerns about the safeguards for civil liberties in the Bill.

There is also a discussion of notification in the section about production orders, with the Privacy Commissioner recommending that people should be notified when a production order has been issued against them (possibly after the investigation is complete to ensure that it is not compromised).

In response, the report notes in comment 118 that there are no notification requirements for a search warrant and that therefore it would be anomalous to add them for a production order. We accept the inconsistency but suggest that the wrong conclusion has been drawn in response.

We recommend that the Bill establish the principle that the targets of search & surveillance powers must be notified that this has happened at such a time when this will not compromise the investigation. This recommendation is built upon the following principles:

- Our society is built upon open and accountable government.
- It is impossible for someone to challenge the actions of a government agency if they do not know that those actions have occurred.
- There is no legitimate interest in keeping searches or surveillance secret after the completion of the investigation.

This notification regime will provide an important safeguard against abuse of search & surveillance powers by allowing people to respond to and challenge the exercise of those powers used against them.

Examination Orders

In comment 52, the report details that Examination Orders are necessary because people who may wish to help the Police will be prevented from doing so by professional ethics (the example of an accountant is given). However, the Bill does not attempt to address this, but rather provides a means to force people to testify and thereby erodes the right to silence.

We recommend that this section be substantially rewritten to maintain the right to silence, but provide protections to enable people such as accountants to be able to assist the Police with the investigation of serious crimes if they choose to.

Recommendations

1. Split the Search & Surveillance Bill into two, with one for enforcement agencies and the other for regulatory agencies.
2. All targets of search and surveillance activity should have a right to be notified of this at such a time when it will not compromise the investigation.
3. Change examination orders to retain the right to silence but provide protections for people who wish to assist Police with their investigations of serious crimes.

2. Computer Searching

The bill contains a number of provisions around the searching of computer systems. The submissions and comments in response discuss issues around:

- The wide-ranging scope of data held on personal computers
- How to define what is to be searched
- What "plain view" means on a computer
- The issue of "trawling" through computers

Our response

The bill ignores the reality of how computers are currently seized and searched, and therefore contains assumptions about warrant specificity, trawling and plain view that don't make sense. (This section was prepared in consultation with an experienced computer forensics examiner.)

Copying/Imaging and Analysing Computers

The first thing typically done when a search warrant is exercised is that the computer systems are seized and a copy (an image) of the entire system is taken. This allows the investigator to preserve the integrity of the evidence and also has the advantage of allowing seized equipment to be returned sooner.

Secondly, investigators then use sophisticated tools to read the entire contents of the copied computer to create an index of what is stored on it. Once this indexing process is completed, the contents of the copied computer can be searched quickly and with very little effort.

Indexes, Plain View and Trawling

Analysis tools present investigators with lists of documents, pictures, music files, etc. These lists will typically include filenames, titles, and thumbnail images of pictures or documents.

By scanning through these lists and looking for the material specified by the search warrant, investigators will also be presented with other material that is not covered by the search warrant. They might not be actively "trawling" for material not covered in the search warrant but it will be presented to them anyway. Arguably, this information is now "in plain sight" and can be seized and acted on.

This means that any search of a computer system will inevitably extend to cover all material stored by all people on the computer system. Suggesting that the specificity requirements of search warrants will provide any protection is obviously a fiction.

Copying and Privacy Issues

There are very real privacy problems that occur with copying computer systems. An officer executing a search warrant to seize business papers would never think to seize the family photo album, but the family's digital photos would be swept up along with the rest of the data on the computer.

This means that seizing a computer risks infringing the privacy of everyone who has personal data stored on the computer system, not just the target of the search warrant (who may not even be the owner of the system).

Infringing privacy in this way leads to emotional suffering – we can all understand the worried feeling someone would have when other people have access to their personal letters and photos. While this is unavoidable when searching shared computer systems (in the same way that it's unavoidable when searching a house) the law should attempt to reduce this as much as possible while not unduly hindering investigators.

We recommend that notifications around searching should include a list of what computer systems and data storage devices were taken and whether or not they have been copied. This data should be kept for as little time as possible and the further notifications should occur when it is deleted.

Interference with business and personal life

People and businesses are increasingly relying on computer systems. Businesses may not be able to function without access to their customer and product data, whereas individuals may find it difficult to maintain communications with their friends, colleagues and families.

We recommend setting a time limit for holding seized computer systems so that they can be returned to people as soon as possible. This time limit should be sufficient for the systems to be forensically copied for further analysis.

Recommendations

4. That no information from a seized computer system, other than what is specified in the search warrant, should be able to be used.
5. That the forensic computer system used to analyse and search the data should record a list of the searches (i.e. search terms) that are used and the results of those searches. This should be made available to the defence in the event that charges are filed.
6. That the notification of being searched (section 126) should include details of what computer data storage items were taken and which of these were copied.
7. That copies of computer systems must be deleted as soon as practicable (i.e. after it is decided that charges won't be filed), and that the original owner should be notified when this is done.
8. That computer systems must be returned to the original owner as soon as possible and that a reasonable time limit of one week should be set. This should easily be enough to allow them to be copied for further analysis.

Availability of computer searches

The Bill includes provisions around access to remote computers (sections 108 and 110).

Our response

We appreciate the clarification of "computer system" (submission comment 413). However, the definition still includes "the internet" as this is a connected system with interconnected computers. Judging by the comments in the report this is not the intention and therefore further clarification is necessary.

Recommendations

9. Further clarification of the meaning of "computer system" to exclude computer systems available over the Internet that are not under the control of the people being searched.

Enforced search assistance

Clause 125 of the Bill allows the searcher to require specified people to assist with retrieving data from a computer system, including the provision of passwords and decryption keys. If the specified person refuses to assist they risk fines or imprisonment.

Our response

No access to passwords and keys

One of the principles of good security design is that there should be no other way to access the secured data – no backdoors, master passwords or similar.

This means that in many cases the systems are specifically designed so that the people who control the systems cannot read information stored by the people who use the system. Computer system administrators often will not be able to provide the passwords or decrypt the data even if they want to assist.

How will the courts determine the truth when someone says that they don't have the key or cannot retrieve the password? Will they believe the system administrator who says that they have no way to read their user's files? Will the courts be prepared to jail someone who might be incapable of doing what they are ordered to do?

Significant effort

The Bill says: "may require a specified person to provide access information and other information or assistance that is reasonable and necessary to allow the person exercising the search power to access data".

We are concerned that there is no limit on the amount of time that the searchers can force the specified person to spend in doing this. Finding and retrieving data can take a significant amount of effort (many hours or even days of work). It seems unjust to force some innocent bystander to labour for free on behalf of the searching agency.

If the Police require a locksmith to access premises they pay them for their services. This should surely apply to any other third-party obliged to assist searchers in their work where the effort involved is substantial.

We note that the Telecommunications (Interception Capability) Act 2004 provides for telecommunications companies to charge for their costs in retrieving data in response to search warrants.

Recommendations

10. The law needs some way to ensure that an innocent third-party is not penalised for being unable to assist by providing access or passwords that they do not have.
11. Agencies compelling assistance from a third-party should have to pay the standard rates for the rendered service after a minimum time.