

“Whatcha gonna do when they
come for you?”

***New Zealand Network
Operators and the
Telecommunications
(Interception Capabilities) Act
2004.***

Dean Pemberton

Who are you?

"Dean Pemberton" <dean@deanpemberton.com>

What do you know about Lawful Interception?

Responsible for LI at a telco.

I've worked with agencies to take that telco
from non-compliance to compliance

I've executed intercept warrants on behalf
of multiple agencies

I've spoken to the agencies involved in LI
regarding this presentation and the
information they would like presented.

Some Acronyms before we begin

All geeks love acronyms.

IANAL TINLA

I Am Not A Lawyer (and even if I was, I'm not YOUR lawyer.)

This Is Not Legal Advice.

You should take everything in this presentation seriously but seek independent legal advice before deciding to act or not to act upon any of it.

GET A LAWYER. Do not rely on what I tell you.

IANAPBFPWTLIW

I Am Not A Punching Bag For People Who
Think That Lawful Intercept Is Wrong.

It's the law, if you'd like to change it,
parliament is that way ----->

As Network Operators, we have to comply.

Don't use me as a punching bag, I punch
back =)

GALoPIS

Get A Lawyer or Play It Safe.

There are going to be parts of this which aren't clear cut. I'd suggest Playing it safe and doing what the Act says. That way if someone does stump up, then you're covered.

If you don't want to do this, then I'd suggest getting a lawyer and some legal advice.

What's the issue here

- Back in 2004 there was a bill passed into law. Telecommunications (Interception Capability) Act 2004
- This act requires that all network operators have the capability to intercept communications on their networks.
- The majority of NZ Network Operators are unaware of the act, wrongly believe they are complying with it, or are ignoring it.

Act? Which act?

Telecommunications (Interception
Capability) Act 2004

Available on <http://www.legislation.govt.nz/>

When was I told about this?

That's not how legislation works. The Act received royal ascent on the 5th of April 2004

How long do I have

That depends. The answer is either 5th
April 2009 or NOW.

The sections of the Act which deal with this
are tricky, GALoPIS

What do I need to do

Comply.

We'll get onto this.

What if I don't

Why wouldn't you want to?

\$500,000 and \$50,000 per day

Pecuniary penalty for contravention of compliance order

- (1) If the High Court is satisfied, on the application of a surveillance agency, that a person has acted in contravention of a compliance order, the Court may order the person to pay to the Crown any pecuniary penalty that the Court determines to be appropriate.
- (2) The amount of any pecuniary penalty under subsection (1) must not exceed \$500,000.
- (3) In the case of a continuing contravention of a compliance order, the Court may, in addition to any pecuniary penalty ordered to be paid under subsection (1), impose a further penalty of \$50,000 for each day or part of a day during which the contravention continues.

And the big thing here.....

Most of you don't comply.

Not even slightly.

Not even a little bit.

It shouldn't ever come to that

Without exception everyone from the agencies I've ever worked with has been great.

They are not interested in being heavy handed or throwing their weight around.

They are much happier working WITH people than against them.

Having said that, they have a job to do and are 100% focused on getting it done.

It's much better to help them out than get in the way.

Ok – Where to from here.

Well lets have a look at that actually happens

- Someone comes to you with an Intercept Warrant
- You have to provide them with a copy of the data covered by the warrant
 - Without
 - impacting other peoples traffic
 - giving them anyone else's traffic
 - letting the party of interest know

Ok – Where to from here - cont.

- You have to collect this data, package it up and ship it off in a format usable by the party issuing the warrant. Not just any format you're happy with.
- This is usually done by a purpose built interception system.

Who will come to me

- A law enforcement agency
- An intelligence and security agency

Which in reality means one of three agencies.

So I have to have this
capability set up and waiting?

Well it depends if you're a Network
Operator or a Service Provider.

Lets have a look at those terms.

Network Operator means

- a person who owns, controls, or operates a public telecommunications network; or
- a person who supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service

Service Provider means

- any person who provides a telecommunications service to an end-user (whether or not as part of a business undertaking and regardless of the nature of that business undertaking); but
- does not include a network operator

Network Operators Must. Service Providers Can

If you're a Network Operator then you must provide this capability, if you're a Service Provider, then the agencies may work with you to help you achieve it on an as needed basis.

Just being a Service Provider doesn't exempt you from the Act, it just makes your obligation a bit easier.

Do Not Play Fast And Loose With These Definitions

Everyone here is thinking:

“ I know, I'll just SAY I'm a Service Provider and I won't have to do this.”

Agencies take this very seriously. Time is of the essence to them. If you try and get wise then you'll end up in the High Court within hours trying to defend your point of view. If you have a network then this is just a cost of doing business. Don't be a fool. GALoPIS

Which one am I (NP vs. SP)

GALoPIS

Discuss this with one of the agencies concerned.

Drop me a line and I'll see if I can help you.

Wooooo Hoooo I'm a Service Provider

Good on ya – it's pretty easy then.

What you should do is make sure that you are able to do port mirroring on your Ethernet switch of choice. Buy a lockable 19" cabinet (half height should be more than enough, just make sure that you don't have to many keys)

If someone serves you with a warrant, you let them put whatever gear they want in the cabinet and give them the port mirror.

Ok Ok Ok, I'm a Network Operator, now what.

Well unfortunately the onus to have all the kit installed and working is on YOU.

But technically you don't have to DO anything right now.

It's all about capability.

Smart people get it in place before they need it. I can't tell you how to run your business, but \$50,000 a day is a lot of money.

It's just like redundant links and backups.

It's like Russian Roulette. You don't HAVE to do anything until you get an Intercept Warrant, but then you HAVE to have the capability to comply with it.

Some people don't have backup systems.

Some people don't have redundant core links

Some people don't have resilient networks.

Some people find out that not having these things costs them a whole lot of money when things go wrong.

This is the same thing.

Examples

Lets look at some examples

Dark Fibre

You're a company with a whole lot of Dark Fibre in the ground. You sell this to anyone who stumps up with the cash and you don't care (or participate in what they put over it).

Uh Oh.

Dark Fibre – cont

Ok – So who are we kidding – you're a Network Operator for sure.

And the LEA is not going to be able to go to **ANYONE** else to get this data if they have a warrant.

So not complying, or trying to blame someone else is **NOT** an option for you. It's the law.

Dark Fibre – cont

So what do you need to do. You need to be able to give any agency a copy of the data going across that fibre in a format that they are happy with. And you need to do this without causing service interruption to other parties or letting the party of interest know.

The smart thing would be to invest in optical taps from the outset and factor this into the cost of doing business.

Then have a way to plum these into a system which bundles the data up and ships it off in a format suitable to the agencies.

LLU DSL

Woooo Hooo finally Telecom unbundles!!!!

You race out and buy some DSLAMS and
offer DSL all over the place.

Uh Oh

LLU DSL - cont

You're a Network Provider.

You're going to need to be able to provide a copy of any of that traffic to agencies. And you also need to make sure that it's as close to the edge as possible so you don't miss user to user communication. Warrants are for all communication from a person, not just whatever crosses your upstream border router.

Smart thing would be to make sure that Interception Capability is present in your BRAS and roll it out with your new network. Make sure that the format is suitable to all the agencies.

But TCPDUMP is ok right?

Not really. Some agencies have indicated that it MIGHT be ok for a short term solution. These same agencies have said that if you are a Network Provider putting an interception mechanism into production, that they won't be accepting a laptop with tcpdump and a pcap file.

TCPDUMP/PCAP just isn't what the agencies need. It doesn't help them do their jobs. It just doesn't comply enough with the chain of evidence to be of any use to them. If you think you fall into the Network Operator category you NEED to be talking to someone about this.

But TCPDUMP is ok right? - cont

The other reason that TCPDUMP is not acceptable long term is the speed at which the agencies require the data.

They want it as close to real time as possible.

Having someone come around once a week (or even once a day) to sneaker-net a drive just won't work.

Most purpose built interception systems package and deliver files on a minute by minute basis.

UBS

That's a hard one. It's hard to know if you're a Network Provider or not.

But here is a possible scenario for you.

UBS – cont.

You're a company. You resell some DSL connection from a major national telecom company. You also have a VoIP toll bypass offering.

You assume that your obligation to intercept the data on the DSL is handled by your DSL wholesaler.

Uh Oh

UBS – cont.

Get that in writing!!!

It would be all too easy for your wholesaler to say..

“Hang on a sec. Here is a 'competitor' of ours in the voice space claiming that he's not a Network Operator when he clearly operates a network. I'm sorry Mr Agency-Man we're not doing his job for him”

Then you're going to have a very grumpy agency taking you to court for non-compliance (and probably getting the data from your upstream anyway)

GET IT IN WRITING!

While I'm on the subject of VoIP.

Make sure that if you're doing VoIP that you have some way to intercept and pass on all calls and call data.

But you were doing this anyway right?

Encryption and what you need to do

Yeah this is a problem you **NEED** to be
aware of.

Here is a part of the act:

Encryption – cont

Section 8

- (3) A network operator must, in order to comply with subsection (1)(c), decrypt a telecommunication on that operator's public telecommunications network or telecommunications service if—
- (a) the content of that telecommunication has been encrypted; and
 - (b) the network operator intercepting the telecommunication has provided that encryption.
- (4) However, subsection (3) does not require a network operator to—
- (a) decrypt any telecommunication on that operator's public telecommunications network or telecommunications service if the encryption has been provided by means of a product that is—
 - (i) supplied by a person other than the operator and is available on retail sale to the public; or
 - (ii) supplied by the operator as an agent for that product; and
 - (b) ensure that a surveillance agency has the ability to decrypt any telecommunication.

Encryption – cont

It's hard to know what your obligations are if you provide a managed VPN service for a customer.

In providing the hardware and support, do you have an obligation to provide an unencrypted copy?

How does this change if you use OpenSSL on a *nix box vs. IPSec on a router?

There may be some wiggle room in the “agent for that product” area, but GALoPIS

What are they interested in?

Communications. They want to know what parties of interest are saying/doing.

Chat protocols

Web Surfing

IM protocols

Games

Not so interested in the 50G of Movies someone is downloading

FTP depends on what it is.

As you can see it's not cut and dried.

Work and Home

“I'm a business only NSP, they only want to intercept home lines right?”

In this case warrants cover a party of interest, not a particular location.

This means that if they are Chatting/IM-ing/VoIP-ing/Skype-ing etc from work, then that's covered too.

Most of the time agencies don't want to approach businesses themselves because they don't know if they can trust the bosses.

Who do I talk to?

There isn't a special “Network Operator Liaison” person at the agencies. They are too busy with their day jobs.

I'm a pretty good first contact (and no one else wanted their name on public slides).

If you want to talk through your obligations with agency people, get in touch with me and we'll sort it out.

Who are you again?

"Dean Pemberton" <dean@deanpemberton.com>