The New Zealand Crimes Amendment Act: A legal white elephant?

Peter Taylor, Chapman Tripp

Peter Taylor is a solicitor with the Wellington office of Chapman Tripp in New Zealand. He practices commercial law, specialising in the acquisition and supply of information technology solutions.

Until the recent passing of the *Crimes Amendment Act* (the *Act*), New Zealand did not have laws directly aimed at addressing computer crime or of an electronic technology nature. While existing laws were applicable in some situations, other types of computer-based activity were slipping through the cracks. This article briefly addresses the New Zealand position prior to the introduction of the Act, summarises the effect of the new provisions, and in doing so refutes one of the main criticisms which has been leveled against it.

The position prior to the Act

Before the Act was passed, New Zealand was reliant upon general law to cover computer-based crime, and in many cases, the general law was adequate. One example is the decision in *R v Misic* [2001] 3 NZLR 1 (CA). The court there upheld a conviction on three counts relating to the fraudulent use of a computer program to evade international telephone call bills. Anderson J approved the words of Lord Hoffman in *Birmingham City Council v Oakley* [2001] 1 All ER 385 at 396, that "when a statute employs a concept which may change in content with advancing knowledge, technology or social standards, it should be interpreted as it would be currently understood. The content may change, but the concept remains the same".

Unfortunately, existing laws are not always so pliable. In *R v Wilkinson* [1999] 1 NZLR 403, a full bench of the Court of Appeal considered the legal definition of "theft" in relation to an elaborate electronic transfer of funds. In overturning the conviction, the court held that the simple electronic transfer of funds from one account to another did not amount to theft. The crux of the court's reasoning was that the electronic funds were not a thing "capable of being stolen", as electronic funds are not a tangible thing, being merely an acknowledgement of a debt owed by a bank to the account holder.

The aim of the Crimes Amendment Act

Clearly, existing law could not always cope with an electronic age environment. Therefore, the aim of the *Crimes Amendment Act* was simple – to make criminal law more clear and certain in respect of computer-based crime.

The *Crimes Amendment Act* became law on 7 July 2003, but has so far received a mixed reception. While some commentators have characterised it as "a smart piece of drafting",[1] others have called it a "lesson in how not to draft laws".[2] The remainder of this article explains this criticism, and, by summarising some of the Act's other new provisions, illustrates that such criticism may be misplaced – due both to the other provisions of the Act, the law in general, and measures individual companies can take for themselves.

The centre of the criticism: unauthorised access of a computer system

One of the provisions which has attracted most attention is section 252. Section 252 provides that:

> *252 Accessing computer system without authorisation*
>
> (1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.
>
> (2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

While section 252(1) appears sensible, the controversy has arisen because of the proviso contained in section 252(2). Subsection 2 effectively provides that a person is not liable if authorised to access a computer system for one purpose, but accesses it for a different one instead. It has therefore been argued that while subsection 1 is a prudent provision, subsection 2 unreasonably dilutes its effect, and that this dilution should be eliminated (particularly given that insider hacking is generally reported as being a much more serious problem than external hacking).

However, these criticisms assume that because section 252 does not criminalise something, that the law condones it. This ignores the fact that while insider hacking might not always be a breach of section 252, it would probably be an offence under either the criminal law generally, or one of the other computer based-laws in the Act.

Other relevant offences

Computer crime offences

One such provision is section 249. Section 249 provides that it is an offence to access a computer system and dishonestly obtain any pecuniary advantage or benefit, or cause a loss to any other person. It is also an offence to merely intend to do this. Furthermore, section 250 makes it an

offence to intentionally damage or modify any data or software in any computer system, or cause any computer system to fail or deny service to any authorised users.

While these are clearly important provisions in their own right, they would also make up for nearly all the diluting effects of section 252(2). For example, if an employee who was authorised to access a computer system for one purpose actually accessed it for another, then in order to escape liability that employee would have to exit from the system, taking no advantage for themselves, and causing no loss to anyone else. A loss, in particular, might occur very easily – a lost opportunity, a lost advantage, or perhaps even by something as simple as crashing the system or using system resources.

Other general criminal offences

As well as these computer-specific offences, as always there are criminal offences of a more general nature which could also apply. For example, the Act introduces a new "theft of trade secrets" offence in section 230. Section 230 makes it an offence to obtain or copy a trade secret, with intent to cause loss or obtain a financial advantage. A "trade secret" is any information that is (or could be) used industrially or commercially, is not generally available, has potential economic value, and is the subject of "all reasonable efforts" to preserve its secrecy.

Civil liability

Furthermore, not only could an errant employee thus be liable under the Act, but there is also the possibility of civil liability. Many prudently worded employment agreements require employees to keep certain information confidential, stipulate that certain intellectual property will be and will remain the property of the employer, and state that certain actions are not permitted.

By contract, an employee has thus agreed not to access certain information – and can be sued for it if they do, without the need to involve the criminal law. Therefore for this reason also, criticism of section 252 is misplaced. Not only does the criminal law provide a remedy, but individual companies can also protect themselves by contract. As always, some measure of responsibility lies with individuals to protect their interests. A generally expressed criminal law cannot always do so.

Furthermore, having such a *contract* in place would actually make it easier for the employee to be *criminally* liable. Because a "trade secret" is something which must be "the subject of all reasonable efforts to preserve its secrecy", a carefully worded employment agreement (along with suitable technological measures) can help establish that an employer has made a reasonable effort to protect its secrecy. In this way a breach of contract can help support criminal charges.

Conclusion

For these reasons, the *Crimes Amendment Act* has gone a long way towards filling the cracks in New Zealand's general criminal laws in respect of computer based crime. The new provisions, in conjunction with the general criminal law and contractual protection, should provide a satisfactory level of protection for most companies in a wide range of situations.

---

1 See comments in an article by Stephen Bell, "Just what is this thing called computer", www.idg.net.nz, 21 July 2003

2 Chris Barton, "Clumsy law for a different world", www.nzherald.co.nz, 8 July 2003.