

counsel

Business practices made illegal?

The Crimes Amendment Act 2003 is taking a hard line on on-line crimes. Indeed, it goes further than that. It makes crimes of some previously legitimate and standard business practices (on-line or otherwise). Computer cookies might now be illegal. Monitoring employees' emails and Internet use might now be illegal. Some standard negotiation tactics might now be illegal.

The amendments have a broader reach than may have been intended. Businesses need to be aware of these developments, and to take steps to minimise their risks.

- *The impact of the Crimes Amendment Act 2003 on the IT and corporate sectors*
- *As expected: new weapons against virus writers and hackers*
- *Unexpected consequences of the new law*
- *What should businesses do?*

The impact of the Crimes Amendment Act 2003 on the IT and corporate sectors

The Crimes Amendment Act takes effect from 1 October 2003. Styled during its early stages as the "Anti-Hacking Bill", it is in fact far more wide-ranging, and affects all businesses - not just the IT sector.

On the one hand, and as expected, it creates several specific computer misuse crimes. But it also appears to:

- blur the line between tough negotiating and blackmail
- turn disclosure of trade secrets into a crime, and
- criminalise many existing innocent business practices, especially in the IT sector, such as -
 - the use of internet cookies
 - monitoring employee emails and Internet use without consent

Businesses can minimise their risk by:

- understanding the new law and its implications
- obtaining consent from all affected people before accessing IT systems or communications in any way (including by way of cookies)
- not disclosing, using or copying others' intellectual property without consent, and
- being careful what pressure they bring to bear during negotiations and what statements they make during business dealings.

- performing routine computer maintenance without specific authorisation, and
- providing information about computer crime techniques.

Employees and officers of a company convicted of committing, aiding or abetting these crimes face prison sentences of 2 to 14 years. But there are some practical steps businesses can take to minimise risk.

As expected: new weapons against virus writers and hackers

There are four new computer offences. Broadly speaking, it will now be an offence to do any of the following things *without authorisation*:

- accessing a computer system for a dishonest purpose
- damaging or interfering with a computer system
- making, selling, distributing or possessing software for committing a crime, or
- accessing a computer system (this will cover "pure hacking" where an unauthorised user

simply accesses a system without doing anything else).

These new crimes plug some historical gaps in our criminal law. For example, although Courts had previously managed to apply other Crimes Act offences to dishonest use of computers (fraud, forgery and criminal damage), those offences did not clearly cover "pure hacking". Also, theft provisions did not cover unauthorised transfers of electronic bank funds - as electronic funds were considered to be merely an acknowledgement of a debt owed by the bank, rather than a tangible thing "capable of being stolen".

The new crimes also make it very clear that in many cases computer misuse can be prosecuted as a criminal offence. Those provisions will be important tools to protect IT systems from intruders and abuse.

Unexpected consequences of the new law

Loophole for employees accessing system for unauthorised purpose

The "pure hacking" offence does not apply to people who are authorised for one purpose, but access a computer system for a

different purpose. For example, an employee who is allowed to access a computer system for work purposes could use it for personal purposes instead without breaching the "pure hacking" provision. Although the employee may well have breached one of the other computer crimes (for example, if he or she had a dishonest purpose or caused damage), businesses should still use their employment and other contracts to protect themselves against this loophole.

Some legitimate business practices are criminalised

Another big problem is that some commonly accepted business practices are illegal under the new law. The computer crimes are drafted so widely, in an effort to be technology-neutral, that they catch many everyday IT business practices. And the Act's effect extends beyond IT-related practices. The Act's changes also catch many non-IT practices. For example, as discussed below, the trade secrets and blackmail provisions are also wider than expected.

Computer website cookies may be illegal

A huge number of business websites, including all e-

Businesses should guard against the risk of criminal liability by advising their employees (whether in their employment contracts or otherwise) that network activities may be monitored either directly or through contractors.

commerce websites and all websites with user log-ins, use internet “cookies”. Cookies are small data files that the website host computer sends to a website user’s computer. They allow the host computer to recognise repeat website users, and to store and regularly update useful information about them, such as shopping history, the contents of “shopping carts”, and user preferences. They serve a useful purpose for both website user and host.

The trouble is that the cookies are usually sent and updated without any deliberate act or consent on the user’s part – and this could be interpreted as “intentionally ... without authorisation ... modifying or interfering with any data in a computer system” or as “accessing ... any computer system without authorisation, knowing or being reckless as to whether there is authorisation”. Both are breaches of the new law.

Perhaps, in the interests of common sense, the Courts will decide that anyone who does not set their browser to reject useful cookies has implicitly consented to them, and so no offence is committed. But that is not the approach that has been taken

by the European Union, where a website host must provide details of the particular cookie concerned, and obtain the website user’s informed consent, before using the cookie.

Businesses should include a “consent to cookies” term in their website terms and conditions (remembering always that the effectiveness of the terms and conditions will depend on when and how they are presented to and acknowledged by the user).

Criminal liability for monitoring employee emails and Internet use

The new law broadens existing interception of private *oral* communications offences to cover *all* private communications, including emails and faxes. It will now generally be illegal to intercept a private communication using an interception device without the employee’s consent, or to disclose any resulting information. A communication is “private” if the circumstances reasonably indicate that the sender or recipient wanted it to be kept private, unless one of them ought reasonably to have expected that it might be intercepted.

This means that business monitoring of employee emails and Internet use without employee consent may now be illegal. Although businesses *may* be able to argue that employees must expect direct monitoring of network activities by the *employer* (and therefore their communications are not “private”), it would be very difficult to argue that the employees must also expect monitoring through a third party IT contractor hired by the employer.

Businesses should guard against the risk of criminal liability by advising their employees (whether in their employment contracts or otherwise) that network activities may be monitored either directly or through contractors. Likewise, contractors should check that this has been done before they begin work.

Standard negotiation tactics may become criminal blackmail

It is not just IT practices that are affected. The new law also expands the scope of offline liability. For example, it extends the existing criminal blackmail offence. The existing offence covers threatened

The new law – especially the expansion of liability to cover reckless false statements - imposes an added duty of care on businesses to guard against making misleading statements, including innocent mistakes, in their business dealings generally. A lapse in care could lead to criminal prosecution.

disclosure of *sexual misconduct* or *criminal offending* to obtain a benefit or cause loss. The extended offence will cover *any accusation or any disclosure of anything*, unless the threat is a reasonable and proper one in the circumstances. There is no case law regarding what threats are “reasonable” or “proper” – but some currently legitimate contractual negotiating tactics (such as threatening to refer the other party’s actions to the Commerce Commission, or to disclose discreditable but not illegal behaviour) may well fall on the wrong side of the line.

Taking, obtaining or copying trade secrets as a crime

Businesses have always been able to sue people under the civil law for disclosing confidential information. Under the new law, it is now also a *criminal offence* to take, obtain or copy any information knowing it to be a trade secret, if those actions are motivated by the desire to gain monetary benefit or cause someone loss, and there is no belief that they are lawful. “Trade secret” is a very broad concept. It encompasses any valuable or potentially valuable information that:

- could be used industrially or commercially

- is not generally available in industrial or commercial use, and
- the owner has made all reasonable efforts to keep secret.

This new offence will be useful for businesses seeking to protect their confidential business processes, know-how, inventions and other intellectual property. But businesses seeking to use other people’s intellectual property should be careful not to breach the new provision.

Criminal liability for mistaken statements in business dealings

Criminal liability for any false statements, including honest mistakes, made during negotiations and other business dealings is expanded. The Crimes Act used to prohibit company or body corporate promoters, directors, managers and officers from making a false statement, with intent to acquire investment or assets from shareholders, members, creditors or security grantors, knowing the statement to be false. Now liability has been expanded to cover:

- *any person* (formerly “company or body corporate

promoters, directors, managers and officers”)

- who makes a false statement in relation to an existing or proposed body
- with intent to acquire investment or assets from (or deceive or cause loss to) *anyone* or *any body* (formerly “shareholders, members, creditors or security grantors”)
- if the person making the statement is *reckless* as to whether it is false (formerly “knowing the statement to be false”).

Of course, directors have always been liable under the Securities Act for untrue statements in a prospectus or investment statement. However, the new law – especially the expansion of liability to cover reckless false statements - imposes an added duty of care on businesses to guard against making misleading statements, including innocent mistakes, in their business dealings generally. A lapse in care could lead to criminal prosecution.

IT service providers beware

As the IT industry deals with other people’s data and computer systems every day,

Computer security consultants routinely provide information about how computer crimes are committed, and provide computer software to try to guard against IT attacks. In doing this, they often say or imply that in the wrong hands this information or software can be used for a criminal purpose. This appears to be illegal under the Amendment Act.

there are some extra pitfalls for IT professionals to watch out for.

IT providers: whose authority is needed?

The four new computer offences apply to actions that are carried out "without authority". But whose authority is this? For example, if an IT service provider is contracted by a hosting service provider to alter or delete hosted third party information on a hard drive, does that service provider need the third party's consent? Or is the host's consent enough?

The law is unclear. Therefore, businesses involved (in whatever capacity) with computer systems in which several people have some kind of interest should always make sure that they have covered *all* possible consents. For example, hosting service providers should ensure that customers provide comprehensive consents for the host and third party IT contractors to access the customer's data.

How wide should that authority be?

IT service providers should ensure that the consents obtained cover the *full range* of computer access, data deletion

and modification, and other activities and consequences that might be involved in providing IT services - not just those contemplated when the service provider is engaged. For example, IT service providers should ensure that their authorisations expressly cover:

- accessing all relevant computer systems
- taking the computer systems off-line (thereby denying access to authorised users)
- causing a computer system to fail during servicing, and
- deleting, modifying, interfering with and impairing data and software.

Doing any of these things, no matter how innocent or well-intentioned, without the relevant authorisation could lead to criminal prosecution. That prosecution could relate not only to the crime of unauthorised computer system access or interference. It could also (in many cases) relate to the crime of possessing software that enables unauthorised computer system access.

Security consultants: disseminating information about computer crimes may become illegal

There is a final pitfall in the new law for IT security consultants. It is now an offence to supply or offer to supply any "software or other information that would enable another person to access a computer system without authorisation" if the supplier knows that the software or information's sole or principal purpose is to commit a crime, or holds out that it is useful for that purpose.

Computer security consultants routinely provide information about how computer crimes are committed, and provide computer software to try to guard against IT attacks. In doing this, they often say or imply that in the wrong hands this information or software can be used for a criminal purpose. This appears to be illegal under the Amendment Act, because, arguably, it involves "holding out" that the information or software is useful for the purposes of committing a crime.

The police may decide not to prosecute this kind of activity. But in any event, consultants should try to avoid saying or implying that any information or software could be useful in committing a crime.

Ironically, businesses which need the new law's protection are being put at risk by it.

What should businesses do?

This new law contains some useful provisions for businesses seeking to protect their IT systems and confidential information. Unfortunately, while well-intentioned, it is so vaguely and broadly drafted that it captures many other business practices as well. Just as they did before the new law, the Courts will again have to decide what the law means, and how to apply it sensibly. In the meantime, ironically, businesses which need the new law's protection are being put at risk by it.

Businesses can minimise their risk by:

- understanding the new law and its implications
- obtaining consent from all affected people before accessing IT systems or communications in any way (including by way of cookies)
- not disclosing, using or copying others' intellectual property without consent, and

- being careful what pressure they bring to bear during negotiations and what statements they make during business dealings. ●

Andrew Poole acknowledges the assistance of Helen Strachan in preparing this *Counsel*.

Our thanks to Andrew Poole for writing this edition of Counsel.



Andrew Poole
PARTNER, Auckland
64-9-357 9057
Email: andrew.poole@chapmantripp.com

AUCKLAND
23-29 Albert Street
PO Box 2206, Auckland
New Zealand
Telephone: 64-9-357 9000
Facsimile: 64-9-357 9099
Email: ctsyak@chapmantripp.com

WELLINGTON
1-13 Grey Street
PO Box 993, Wellington
New Zealand
Telephone: 64-4-499 5999
Facsimile: 64-4-472 7111
Email: ctsywn@chapmantripp.com

CHRISTCHURCH
119 Armagh Street
PO Box 2510, Christchurch
New Zealand
Telephone: 64-3-353 4130
Facsimile: 64-3-365 4587
Email: ctsyah@chapmantripp.com

www.chapmantripp.com

This Counsel highlights issues in a number of legal fields. For further information on any issues raised in this Counsel, please contact the partner or principal with whom you usually deal, or any of the following:

AUCKLAND
Paul Wilkins
Greg France

WELLINGTON
Paul Barnett
Peter Taylor

CHRISTCHURCH
Andrew Woods

Every effort has been made to ensure accuracy in this newsletter. However, the items are necessarily generalised and readers are urged to seek specific advice on particular matters and not rely solely on this text.