Wigley & Company

BARRISTERS and SOLICITORS

Computer Security and the Law

February 2004
Wellington

10th Session:
Computer Security and the Law

P O Box 10842 • Level 7 • 11-17 Bolton Street • Wellington • New Zealand • Phone: + 64 (4) 472 3023 • Fax: + 64 (4) 471 1833

Also at Auckland • Level 9 • FAI Tower •220 Queen Street • Phone +64 (9) 307 5957

Computer security is of course important and the law goes some way to provide remedies against computer crooks and others. But there is also potential exposure for those organisations that don't set up adequate policies, security, etc. In this paper Wigley & Company address the legal aspects of computer security. We over many issues ranging from the new crimes legislation, exposure of organisations, through to employee issues, privacy concerns and international aspects.

INDEX

1 Summary

1.1 There's already some good law to prosecute computer crooks. July 2003's amendment to the Crimes Act goes a long way to strengthen criminal remedies against hackers, participants in denial of service (DOS) attacks, bent employees, and others.

1.2 It looks like some commentators haven't closely read the new law before suggesting it's of limited benefit for prosecutions of employees and other insiders. Others seem to have got it wrong when suggesting that IT security specialists could be in the gun for testing computer security as part of their work (that's likely to happen rarely). The Act does a very good job in these and other areas. It's a smart piece of drafting, particularly as:

1.2.1 it's difficult to frame legislation for computers. There's so much change going on. The new law keeps things as technologically neutral as possible;

1.2.2 it's difficult to get the balance right as between acceptable and unacceptable use of computers. Get it wrong and, in theory at

least, innocent people could be prosecuted. That's highly unlikely though in practice. Prosecutors have judicially-blessed discretion as to whether or not to prosecute in a particular case. It's very unlikely the Police will prosecute on a technicality.

1.3 Of course a criminal prosecution is just one remedy. We'll also look at civil remedies, such as damages and injunctions.

1.4 In the civil area there are 2 specific sub-categories to think about. First the laws as to privacy and confidentiality. These provide duties and remedies in the courts and also under the Privacy Act. Second, as such a high percentage of illicit computer activity is undertaken internally, there's specific employment law issues.

1.5 Proving a computer case can be hampered by problems with our evidence laws. Change is overdue. We'll touch on that aspect.

1.6 I'll deal with how organisations might be exposed legally if they fail to have adequate security and anti-virus protections in place. What happens if an organisation with inadequate security has a customer's confidential information taken from it by a hacker? Or what if a virus ends up on someone else's LAN because an organisation has inadequate anti-virus protection and the virus gets passed on? There's a real risk the organisation could be liable for damages.

1.7 Finally, we'll look at international issues.

1.8 As we go through the issues, we'll look at some legal solutions.

1.9 We're focussing only on legal aspects in this paper. It's especially important for organisations to factor in other issues when deciding what to do to protect against risk. Think about security, internal audit, employment, practical day-to-day operations and flexibility, availability of services, and so on. A holistic and balanced approach is needed. The relevant IT security standard, AS/NZS 17799, provides a useful framework.

2 Prosecutions

2.1 Computers are involved to varying degrees in crimes. Sometimes their role is pivotal. Often it's just incidental. While there's a problem about proving cases from an evidential perspective (more about this below), many computer-related crimes are adequately covered already. There's been many successful prosecutions where computers are involved.

2.2 However 2 key problems have cropped up:

2.2.1 There have been definitional problems. For example, for the purposes of forgery, does the Crimes Act use of the word, *"document",* include material on a hard drive? Or does it have

to be a physical thing like paper? Under current law, can someone be convicted of taking money by electronic transfer? The answer to such questions depends on which sections of the Crimes Act are involved and upon various court decisions. For a more comprehensive discussion of this and other computer crime issues, see Chapter 4 in Judge David Harvey's new text, *internet.law.nz: selected issues* (LexisNexis 2003).

2.2.2 The existing law often isn't wide enough to cover computer-specific areas such as hacking, DOS attacks and so on.

2.3 In July 2003, out came the Crimes Amendment Act (No 6). This includes computer crimes in 7 sections. In the few weeks leading up to the new Act, important changes have been made to the Bill, following other earlier changes.

2.4 **Other Crimes Act changes:** Before dealing with specific computer crimes, we note that there's also been major changes to Part X of the Crimes Act. That part deals with property crimes, many of which apply to computer-related circumstances. Changes include an extension of the definitions of "document" and "property", to cover problems identified in computer crime cases such as *R v Wilkinson.*

2.5 We'll deal below with new law relating to interception of private emails, etc. So there's a lot more relevant change than just what are called the computer crimes.

2.6 **The computer crimes: the definition of *"computer system"* is key:** The definition of *"computer system"* in s248 is important. Overlooking this definition seems to be one reason why there's been unnecessarily negative comment on the Act. (By the way, in this paper, I'll only summarise the key aspects of the new law; there is more detail and variation on the basic theme).

2.7 A *"computer system"* means **any** one of the following (that's important, it's not everything combined: it's **any one**):

2.7.1 A computer;

2.7.2 2 or more interconnected computers (e.g.: computers on the internet, a LAN, etc);

2.7.3 any *"communication links"* between computers (this could be Ethernet, telephone line links, cellular links, Bluetooth, etc; basically it's anything that links computers);

2.7.4 2 or more interconnected computers, plus *"communication links"*. This could be a LAN, the internet, an intranet, telecommunication systems per se (which of course are computer based nowadays), telecommunication and computer

systems linked by airwaves (including cellular) not just landline, and so on.

2.8 *"Computer System"* is also defined to **include** "*any part of ……"* those 4 items.

2.9 As we'll see later, this last reference to *"any part of..."* those items may be significant. There's a last minute amendment that changes the way that the list of items reads so that it's not so clear cut that "*any part of ..."* those items can be labelled a "computer system" on its own. Whether, for example, a particular segment of a hard drive is a "*computer system*" could be important. As there doesn't seem to be any other reason to add the "*any part*" reference, arguably a part (such as a segment of a hard drive) is a "*computer system*" as defined.

3 The New Computer Crimes

3.1 Each crime attracts differing levels of prison terms and fines. All are set at a relatively high level. We'll deal with each in turn.

3.2 **Accessing computer systems for dishonest purposes:** The first (s249) kicks in when a person, dishonestly or by deception, and without right, accesses a computer system. *"Access"* is widely defined for all these crimes. It includes pretty well anything that's tied up with computers and links between computers. It'll cover getting into a system (including by telecommunications, radiocommunications, and so on), and doing anything within the computer system itself.

3.3 Under this section, a person is convicted if either she gets a benefit (e.g.: steals money electronically or takes intellectual property) or causes loss. She's also convicted if she doesn't pull off the crime but **intended** to do so.

3.4 This crime overlaps with the more traditional crimes such as fraud, forgery, theft and so on. It makes it clear that causing loss is criminal where that's done dishonestly or by deception. In other words, the person can be convicted even though he doesn't gain anything, so long as loss is caused to another. That could cover deliberately infecting with viruses, bringing a system down, hacking so that payments are made by the target organisation to third parties, and so on.

3.5 **Damaging or interfering with a computer system:** The first part of s250 deals with intentional impact on computer systems where danger to life is at stake (an obvious example is an air traffic control system).

3.6 The next part of Section 250 covers situations where someone intentionally or recklessly, and without authorisation, either:

3.6.1 *"damages, deletes, modifies, or otherwise interferes with or impairs any data or software in a computer system"* (there's a

change from the Bill as "adds" has been deleted from that list (that's good as "adds" would include adding cookies, for example)); or

3.6.2 causes a computer system to fail or deny service to authorised users.

3.7 This covers people who, without authority, do things that impact on data, software and computer systems (ranging from the Internet through to LANs and individual computers). It applies as much to employees doing unauthorised activities as to external hackers, sources of viruses, etc. The second aspect covers DOS attacks and system failure caused by the person's actions. Often this won't apply as the service will be impaired rather than stopped. But it's difficult to define something that's comprehensive in this area. The first limb may well cover erosion of service anyway.

3.8 **Making, selling and possessing software or other information for committing crime:** Someone can be convicted of making, selling, distributing or possessing software or information, for effecting computer crimes. Note that this includes not only software but also information which helps with effecting computer crimes.

3.9 To be prosecuted under s251, there needs to be an ulterior motive (eg: (a) the software is sold and promoted for hacking purposes or (b) the person must have the software with the intention of using it for criminal purposes). That's important, because quite a bit of software and information, such as IT security books, has legitimate uses. People shouldn't be prosecuted just for having or selling that software or information.

3.10 **Accessing computer systems without authorisation:** Finally there's a provision aimed just at accessing computer systems. For this, it's not necessary to prove something happened as a result, such as theft, failure of systems, etc. Intentional and unauthorised access, alone, is enough.

3.11 Much of the comment seems to focus just on this provision (s252), without looking at the impact of the sections noted above, which can apply to employees anyway.

3.12 Under s252, a person can be convicted if, **without authorisation**, he or she **intentionally** accesses a computer system. (There's a similar outcome when the person is reckless in this regard). This is heady stuff because it encompasses the most minor of infringements, some of which people would regard as too minor to be covered by crimes legislation. An important point though is that the police can and do exercise prosecution discretion. They're unlikely to chase up minor transgressions when other remedies are available (under civil law, etc). Better to have this wider definition (or don't have this section at all) than

be stuck with a clunky technology-specific law which will go out of date?

3.13 By the way, this is probably the most controversial part of the new law, with arguments both ways as to whether it should be included or excluded. It's certainly on the border from a civil liberties perspective. Important though is that the person must **intend** to access the computer system (there's the overlapping *reckless* point as well). A mistake, an innocent error, or the like, won't qualify.

3.14 Commentators are saying that the s252(2) qualification on s252 stops the law working for employees and other internal illicit access. That's not necessarily right. Anyway the comments seem to overlook the preceding sections in the legislation, which generally apply anyway to internal people.

3.15 Section 252(2) says the section doesn't 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."*. It's being said that, because an employee or contractor is authorised to access the computer system for a particular purpose, he can't be convicted when he does something that's unauthorised.

3.16 That would be right if the definition of *"computer system"* is pitched only at the level of computers, LANs, the Internet, etc. But arguably it's not. Included in the definition of "computer system" are **parts** of computers, etc. Say a staff member has authorised access to a certain security level on the company's server (eg: to the company's procurement data, because she's in the purchasing department). If, going outside her security clearance, she accesses other data (eg: accounts payable), she's accessing different physical parts of the hard drive in the server (ie: data which is physically stored on a different **part** of the hard drive). Arguably that's a different "*computer system*", as defined. So even though she's an employee, arguably she can be convicted for doing something that's unauthorised. It's not necessary to prove that she stole anything or caused damage (unlike the other provisions). Mere accessing is enough.

3.17 This conclusion is not clear-cut due to the way the definition of "*computer system*" has been amended in the final Bill stages. The issue could be resolved later in the Court (a key issue will be the use of "*include*" and "*means*" respectively in the definition of "*computer system*" (see Burrows, *Statute Law in New Zealand* (3rd edition) at pp 285-288)).

3.18 It's much more difficult (if not impossible) to succeed where the employee or contractor has wide authorised access (eg: she's the system administrator). But other provisions probably kick in anyway where prosecution is justified in the first case.

3.19 Other than the potential issue about employees, etc., the main issue around the s.252(2) qualification is that it is harder to prosecute where the access under review is within or closely related to where that person has authority to go. There could be some definitional issues around this to work through. It would be possible to tweak this, as Judge Harvey notes in his book at footnote 89 on page 194. In practice there's a sensible balance that's created. And of course there are the other sections on which to base a prosecution anyway. They will usually apply anyway when there's reason enough to prosecute a staff member or contractor.

3.20 **Search warrants:** Sections 252 to 254 confirms the ability of the Police, SIS and GCSB to access computer systems when authorised, such as by search warrant.

3.21 **What can an organisation do to increase the ability to prosecute cyber-crooks and hackers?** Obviously this should not be the key focus. Protecting the organisation (with good internal systems, firewalls, and so on) is far more important. Important also is contract, employment, privacy and civil law compliance. But we note there's one thing that organisations can do, particularly in relation to internal breaches. Most of these computer crimes apply when someone does something that's not **authorised.** Getting clarity around what's **authorised** will make it easier to prove a case.

3.22 There's not a lot that can be done for external people in this regard. Whether someone is or isn't authorised will usually be implicit anyway (eg: it's implicit that a hacker is not authorised to intrude behind an organisation's firewall). Some steps might be taken. For example, ISPs can clarify what's authorised in their terms. And outsiders, such as suppliers and customers, getting access within the organisation's firewall, can be required to sign up to restrictions. However, note the points below about getting clear enough acknowledgment of those terms and policies.

3.23 Internally, the employee's or contractor's contract, on-line code, and/or acceptable use policy can make clear what's authorised and what's not. This should be written up with clarity. If it's made clear where an employee's authority to use the LAN and the Internet starts and stops, it'll be easier to show that the employee has strayed into a *"part"* of the *"computer system"* where he's not *"authorised"* (and so he can be convicted).

3.24 Such clarity is important too for civil remedies (eg: under employment law). More about this below. Criminal cases have to be proven to a much higher standard of proof (*beyond reasonable doubt*) than civil cases (generally, *on the balance of probabilities*). So getting this right is particularly significant for criminal cases. Organisations that need to have a strong focus on the ability to prosecute (eg: those handling and paying out substantial funds) should be particularly vigilant about this.

3.25 Especially important is to get adequate confirmation of acceptance of the authorised boundaries, by clear-cut acknowledgement and signed acceptance. It's unlikely to be enough to have the details lurking in some manual or on-line guidelines (that's a very common situation). It should be clearly identified in upfront fashion, and acknowledged in **handwriting** by the employee or other person. We set out the reasons for this, and strategies, in our paper http://www.wigleylaw.com/EffectiveTransactionsOnLineLiability.html, for the 2002 New Zealand Law Society Business On-line seminar:

3.26 **"Authorisation":** It's suggested that someone who gets authorisation into a computer system at one level can't be prosecuted if he or she unilaterally elevates his or her access to another level, without authority. That's not necessarily so, (arguably even for many employees and internal contractors). Remember that the computer crimes pivot around any 1 of several definitions of *"computer system"*. For example, we've all got broad authorisation to access the "*Internet*" (it's one way in which "*computer systems*" are defined in effect). But we don't have access to particular computers, behind firewalls, or particularly parts of computers, that are connected to the Internet. The *"computer system"* definition treats those parts as separate for prosecution purposes. The new law is well drafted in this regard.

3.27 That's the specific computer crimes. Now we'll turn to communication interception.

4 Communication Interception

4.1 The Crimes Act stopped interception of voice phone calls except in limited circumstances. The new changes extend this to electronic and data communications as well, in sections 216A-F. Under s216B(1), there's an offence when someone intentionally *intercepts* any *private communications* by means of an *interception device*. (Other offences flow from this primary offence). The words in italics are defined. An *interception device* is widely defined and would include all computers. That in itself doesn't cast the net too widely because, to be convicted, the other features of the offence need to be present. To *intercept* means to listen, monitor, record etc while the communication is taking place. And *private communication* would include all electronic communication (including emails) where it's implicit that at least one party considers the communication should be confined to the parties to that communication. There's an exception to this that applies when the party would expect there could be interception.

4.2 There's no offence in some limited circumstances:

4.2.1 Police search warrants and comparable law enforcement activity.

4.2.2 When the person intercepting is a party to the communication. How these provisions apply depends very much on the circumstances of each situation. Say a customer emails an order addressed to an employee. Often it will be possible to say that the employer is really a party and so it is entitled to read ("*intercept*") the email.

4.2.3 When a **public** communication service provider (eg: an ISP or telco, not an organisation in relation to its own LAN or external communications) gets an employee to intercept communications, for the purpose of maintaining that service.

4.2.4 Equipment and/or in circumstances defined in regulations, yet to be introduced.

4.3 We emphasise the point that each situation needs to be individually addressed. Take employee communications as an example. Even if solely internal, those communications are still potentially covered by this law. Often it may be arguable that there's an implicit acceptance by the employee that his personal and business emails can be read by the employer, his boss, the systems administrator, etc. But as we noted above, it's desirable to have clarity in this area. Ideally, the employees and contractors should consent to all emails, etc, being read on behalf of the employer. Sometimes this right may be important enough to be confirmed in relation to third parties dealing with the organisation (eg: where large sums are at risk and audit/monitoring is desirable). Usually that won't be done, won't be necessary, and will be too difficult anyway.

4.4 Intrusion and penetration testers say this new law could cause them problems. It will do so only if they start intercepting private communications where there's neither express nor implicit consent to this by the parties to the communications. That's easy enough to sort out with employees and contractors (they should agree to this in writing). It's harder when external emails are to be checked. But why would much work in this area be affected by this law, as usually it won't be necessary to check private communications? If this truly is a problem, one option is to seek specific exemption by regulations.

5 Evidence

5.1 We note briefly the need for New Zealand's laws on evidence to be developed. A new Evidence Code is in the pipeline. See the overview in Judge Harvey's book at Chapter 4 and in the CCH *E-Commerce* text.

6 Civil Remedies Against Hackers, DOS Attackers, Virus Sources, Spammers and Others

6.1 It's likely that our judge-made law will evolve to enable injunctions and damages to be obtained against many of those causing computer problems. The courts will work from established traditional world

categories such as intentional torts (eg: trespass), negligence, and so on. The law tends to take an incremental and evolutionary approach in this area, yet responds well over time to new threats such as cyber-problems. The path is not clear cut nor straightforward. See more detail in the Law Commission's E-Commerce reports and Judge Harvey's new book at Chapter 6.

6.2 For a very recent offshore example of the development of legal claims, see *Intel v Hamidi.* Intel failed on 30 June 2003 to persuade California's highest court that a former employee (Hamidi) had trespassed on Intel by sending numerous emails to Intel employees. But the court confirmed that this was a situation quite different to spam, hacking, etc., where orders would have been made. Hamidi's emails had low impact on Intel's LAN (and the court said, for technical legal reasons, that staff downtime caused by reading the emails wasn't enough to invoke the long standing tort of trespass). This is a contentious outcome that can be debated both ways. The point is that the law should evolve over time to meet threats appropriately.

6.3 Often of course hackers and others are offshore, can't be traced or aren't worth suing. Who else is at risk of being sued? We now turn to this.

7 Organisation's Inadequate Security: Legal Risk

7.1 Say that inadequate security leads to an organisation (Acme) losing confidential information (eg: it's hacked). Is it liable? There are 2 groups of outsiders to address. First those closely related to Acme (eg: a contracted customer). Here, there's a special relationship of some sort.[1] 2nd, those more removed. In the first instance, what the contract says governs, if one exists. If there's a 100% obligation to preserve the information, Acme is liable. Acme should never sign such an agreement. It's too risky. If liability is expressly excluded, then that result follows. In the other cases in the 1st category, a Court may say that Acme should have security that's suitable for the circumstances. If it isn't, there's liability. This liability can flow from the law of contract, the general law as to confidentiality, and from non-contract law (tort).

7.2 Overlapping is possible Privacy Act risk and liability. Broadly the Act requires security appropriate to the circumstances. The Act only applies to information about individual people. However, the general law as to confidentiality may "*fill in the gaps*" in relation to corporate information.

7.3 For end-user consumers, there can be additional Consumer Guarantees Act risk (but in practice this is low risk).

7.4 Now the 2nd category (where there's no "*special relationship*"). Acme might be liable to parties with which it isn't contracted or doesn't owe a

[1] We're not using "*special relationship*" here in a technical legal sense, but rather to cover closer relationships such as contract, and close relationships for tort liability purposes.

close duty of confidentiality. But this usually is less likely. This risk derives from the "*snail in the ginger beer bottle*" line of cases, from confidentiality cases, etc. There is understandable reluctance in the Courts to impose widespread liability upon Acme to strangers.

7.5 What if, for example, Acme failed to instal a SQL patch and, as a result, a virus passes on to and infects other networks. Or a systems administrator fails to take steps to halt a virus in its tracks? Again there is greater risk of liability, as between more closely related parties. This area of the law (tort including negligence, nuisance, etc) tends to move incrementally to meet perceived risk. But history demonstrates that the law over time responds practically to commercial and technical developments. The Courts held that a farm – which had inadequate sanitation – can be liable to other farmers for passing on animal diseases "*received*" from another farm.[2] By analogy, sooner or later, it's likely that organisations with inadequate security/anti-virus measures will be liable to others affected by intrusions which otherwise would have been stopped. There will be a debate about what level of security is adequate, and also about issues such as whether Acme caused the attack, the degree to which it should be liable, and the degree to which a "special relationship" is required. Particularly where liability can be especially widespread and high (such as in relation to viruses) the Courts are cautious. Organisations should assume though that they could be at risk of being sued, whether in New Zealand or offshore. Potential liability is multi-million.[3]

7.6 For a hot-off-the-press article on this, see M. de Villiers *Virus Ex Machina* 2003 Stanford Technology Law Review 1 (http://stlr.stanford.edu/STLR/Articles/03_STLR_1/).

7.7 Just announced is that California will introduce legislation that requires organisations to advise third parties such as customers when their confidential information is hacked or otherwise leaked. That's likely to force improvement of security, and claims against organisations where information gets out because security is inadequate. Under our privacy and confidentiality laws, it's already possible to get compensation when someone's information gets out because there's inadequate security.

8 Confidentiality and Privacy

8.1 We've touched on this in the preceding section. See also our NZCS paper *http://www.wigleylaw.com/ConfidentialityAndRestraintOfTradePracticalIssues.html* . Since then there's been the Mike Hosking case in our High Court. He and his wife tried unsuccessfully to stop publication of photos of his children. The case is going to appeal. While this has called into question whether there's a separate tort of privacy (or whether that's subsumed within the law of confidentiality) there's no

[2] *Weller v. Foot & Mouth Disease Research Institute* [1964] 3 All ER 560.
[3] They might be caught in offshore Courts where damage occurs overseas.

doubt that there are confidentiality/privacy obligations additional to the Privacy Act. However framed, both (a) a source of an information leak and (b) someone who enabled the leak (such as by having poor security), can be exposed to compensation claims.

8.2 Generally, obligations as to privacy and confidentiality can be overridden by the affected party's agreement. So it's wise for example for employers to get express consent, by contract, to read and intercept employee/contractor personal and business emails and other material on the LAN.

9 Employee Issues

9.1 This is a subset within the overall civil remedies area. We've dealt with a number of employee issues already. Of course a high percentage of cybercrimes and problems are internal. They're often handled by warnings, dismissals, etc. rather than under criminal law. For the reasons noted above, it's best to have real clarity around what employees and contractors can and can't do, carefully signed and accepted. This will increase the chance of successfully implementing internal procedures and employment law procedural requirements.

9.2 Documents such as AUPs can be hard to draft and get right. Take the allied area of porn. Using porn legislation as the benchmark for what is or isn't acceptable in an office environment would give blessing to huge amounts of nasty material, which can't be attacked by the employer. The porn statute precludes only particularly serious porn.

10 International Issues

10.1 Stopping these attacks internationally will always be a problem area. But things improve as new laws come through internationally, such as our own new criminal law, the *Gutnick* defamation decision in Australia, and so on.

acting for both vendors and purchasers, Wigley & Company understands the issues on "both sides of the fence", and so assists its clients in achieving win-win outcomes.

While the firm acts extensively in the commercial sector, it also has a large public sector agency client base, and understands the unique needs of the public sector. While mostly we work for large organisations, we also act for SMEs.

With a strong combination of commercial, legal, technical and strategic smarts, Wigley & Company provides genuinely innovative and pragmatic solutions.

The firm is actively involved in professional organisations (for example, Michael is President of the Technology Law Society and Stuart van Rij its secretary).

We welcome your feedback on this article and any enquiries you might have in respect of its contents. Please note that this article is only intended to provide a summary of the material covered and does not constitute legal advice. You should seek specialist legal advice before taking any action in relation to the matters contained in this article.