Wigley & Company

BARRISTERS and SOLICITORS

ON-LINE TRANSACTIONS AND SECURITY RISK: A BRIEF OVERVIEW

PAPER PRESENTED TO
ASIA OCEANIA ELECTRONIC MARKETPLACE ASSOCIATION
SEMINAR

Christchurch and Palmerston North
March 2003

P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833
also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

In March 2003 Michael Wigley addressed the Asia Oceania Electronic Marketplace Association on online transactions and security risk. This paper provides a brief overview and links into other papers that we have prepared.

INDEX

1 Introduction

1.1 This paper briefly overviews security and transaction legal risk issues. For more detail, see our papers from our New Zealand Computer Society "Law and IT" series on www.nzcs.org.nz.

1.2 We'll focus on the New Zealand scene but of course offshore issues are key too. Often the answer will be the same elsewhere.

2 On-Line Transactions

2.1 Small deals (eg: smaller on-line consumer purchases) involve little legal risk for both supplier and vendor. Consumer protection legislation is significant (eg: Fair Trading Act, Consumer Guarantees Act, Privacy Act, and their overseas counterparts). However, class actions are unlikely here and complaints to regulatory bodies (eg: Commerce Commission and the Privacy Commissioner) are relatively rare. Few are going to sue on small deals (it costs too much). More important are commercial and PR realities. We buy from Amazon because we trust them. We'll never sue them.

2.2 Legal risk is generally more significant for larger deals. Organisations do enter multi-million dollar deals just by email. That can be legally enforceable. Where certainty and contractual limitation of liability is important, signing a hand-written agreement will be safer. Otherwise it might be too hard to confirm execution of the agreement in Court. More robust verification processes such as PKI are – on present technology – generally not in use, and anyway have their problems (eg: there is no certainty that the person using the PKI private key is the authorised person).

2.3 The Electronic Transactions Act won't be in force until the 2nd half of 2003 (that is, until regulations are brought in to deal with tax, credit contracts and other issues). Even then, its impact on normal business

dealings is minimal. Its key focus is on statutory and regulatory requirements. But business dealings are usually governed by other types of law.

3 Organisation's Inadequate Security: Legal Risk

3.1 Say that inadequate security at ABC Limited leads to another organisation (Acme) losing confidential information (eg: it's hacked). Is ABC liable to Acme? There are 2 groups of outsiders to address. First those closely related to ABC (eg: a contracted customer). Here, there's a "special relationship" of some sort. 2nd, those more removed. In the first group, what the contract says governs. If there's a 100% obligation to preserve the information, ABC is liable. ABC should never sign such an agreement. It's too risky. If liability is expressly excluded, then that result follows (if it's done carefully). In the other cases in the 1st category, a Court may say that ABC 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).

3.2 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 impose similar types of liability and risk in relation to corporate information.

3.3 For end-user consumers, there can be additional Consumer Guarantees Act risk (but in practice – as noted above – this is low risk).

3.4 Now the 2nd category (where there's no "special relationship"). ABC might be liable to parties with which it isn't contracted or doesn't owe a close duty of confidentiality. But this usually is less likely than with parties in the 1st category. This risk derives from the "snail in the ginger beer bottle" line of cases, from confidentiality cases, etc. But there is understandable reluctance in the Courts to impose widespread liability upon ABC to strangers. So policy mechanisms come into play which limit ABC's exposure. Where liability starts and stops is unclear.

3.5 What if, for example, ABC failed to instal a SQL patch and, as a result, a virus passes on to and infects other networks. Or what if 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. By analogy, sooner or later, it's likely 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 ABC caused the attack, the degree to which it should be liable, and the degree to which a "special relationship" is required for there to be liability. Particularly where liability can be especially widespread and high (such as with computer viruses) the Courts are cautious.

3.6 For a hot-off-the-press article on this, see M. de Villiers *Virus Ex Machina* 2003 Stanford Technology Law Review 1 (it's on Stanford's website).

4 Staff AUPs

4.1 Physical security, and security measures involving staff, etc. can be as – if not more – important than computer system security (eg: hardware). Staff AUPs are important. Often staff don't sign them. But that's important, so the employer can prove the case later. And on-line "click accept" is not enough. A hand signature is important.

5 Limiting Liability

5.1 Those involved in providing security solutions (penetration testers, software and firewall providers, etc.) must carefully agree the scope of their responsibilities and limit their liability. The risk is too high to do otherwise.