



Wigley & Company

BARRISTERS *and* SOLICITORS

**LEGAL DEVELOPMENTS FOR IT SECURITY**

**10<sup>th</sup> ANNUAL IT SECURITY SUMMIT**

**11 April 2005  
Auckland**



This paper updates our comprehensive IT security summaries in 2003 and 2004, and deals with recent developments.

## INDEX

<b>1.</b>	<b>Introduction.....</b>	<b>2</b>
<b>2.</b>	<b>Privacy, Confidential Information, etc.....</b>	<b>2</b>
<b>3.</b>	<b>Authentication.....</b>	<b>2</b>
<b>4.</b>	<b>Criminal prosecutions.....</b>	<b>3</b>
<b>5.</b>	<b>Security policies.....</b>	<b>4</b>

### **1. Introduction**

- 1.1 Our website contains many papers dealing with legal aspects of security and the related area of privacy. There is a comprehensive summary on privacy issues in our paper this month, "*Privacy Implications for Information Technology*".<sup>1</sup>
- 1.2 We have dealt comprehensively with the legal aspects of IT security in our 2004 paper, "*Legal Compliance and IT Security*"<sup>2</sup> and our subsequent follow up, "*Ensuring your Legal and IT Security*".<sup>3</sup> For more detail, refer to these papers.
- 1.3 We now bring developments up to date.

### **2. Privacy, Confidential Information, etc**

- 2.1 The law of privacy and confidential information raises a number of issues relevant to security obligations. We have summarised these comprehensively in our paper noted above, *Privacy Implications for Information Technology*.

### **3. Authentication**

- 3.1 There couldn't be a better reminder about the risks around authentication than the banks' current problems with internet banking: things are badly wrong when the banks recommend against online banking at internet cafes etc. Already Bruce Schneier – in an April 2005 article<sup>4</sup> - is raising

---

<sup>1</sup> See <http://www.wigleylaw.com/privacy-implications-for-information-technology.html>

<sup>2</sup> See <http://www.wigleylaw.com/LegalComplianceAndITSecurity.html>

<sup>3</sup> See <http://www.wigleylaw.com/EnsuringYourLegalITSecurity.html>

<sup>4</sup> <http://www.schneier.com/essay-083.html>

questions as to whether two factor authentication will do the trick long term (or even short term).

- 3.2 These problems of course have wide implications for security and privacy generally. There are legal implications as well such as an organisation's liability risk for inadvertent release of information, hacking, breach of contract, and so on.
- 3.3 A particular aspect is the weakening of the key and therefore the authentication process, which in turn weakens the 3 interrelated drivers of non-repudiation, integrity and confidentiality, all of which present interrelated legal issues. In a legal context, erosion at the authentication level erodes, in turn, non-repudiation and integrity. Unlike a handwritten signature (for which fraud is almost always detectable), presentation of a key proves only (in the absence of any other evidence) that someone is presenting as Joe Bloggs, not that the person using Joe Bloggs' key is in fact Joe Bloggs.
- 3.4 That is potentially an evidential issue (and weakness) in the Courts and other Tribunals. In view of other evidence in some contexts (eg: tax non-compliance) it doesn't matter too much. But often it does. That is particularly so in a criminal context, as the required standard of evidence is very high.
- 3.5 The Electronic Transactions Act, on current technology, does not make things any easier.<sup>5</sup>
- 3.6 It is expected that this year there will be a new Evidence Code introduced as legislation in New Zealand. This will allow the Courts to take a more flexible approach to electronic evidence, but this also is unlikely to save the day.
- 3.7 In short, the strength of the key has legal implications just as it has implications from a security and privacy perspective.

#### **4. Criminal prosecutions**

- 4.1 We have dealt extensively with the computer crimes and related offences that are available in a criminal context in our 2004 paper on IT Security.<sup>6</sup> However, none of the reported cases arising out of the changed legislation provide any particular guidance to its application. The cases so far involve guilty pleas or no particular issue as to legal implications.
- 4.2 The computer crimes and other offences available under the Crimes Act remain potent in any event.

---

<sup>5</sup> Section 24 provides a presumption that online authentication is valid, if certain conditions are met. But it is unlikely that all the requirements are met on current technology. In any event, the section applies only to legislative compliance.

<sup>6</sup> <http://www.wigleylaw.com/EnsuringYourLegalITSecurity.html>.

## 5. Security policies

- 5.1 Security policies (often incorporated in a document such as an Acceptable Use Policy (AUP)) remain particularly important and are often flawed in their application. To increase the prospect of successful prosecution under the Crimes Act, it should be made clear that a person's access to the LAN is limited to certain areas.<sup>7</sup>
- 5.2 Our view remains unchanged that these documents should stand alone (in the sense that they are not directly part of the employment contract or agreement for engagement of a contractor etc). They need to be able to be changed at short notice to reflect new security threats, technology developments etc. For that and other reasons, they need to be standalone. But they should still be hand-signed and not click-accepted, unless the organisation is prepared to take a significant risk. Likewise, ideally, any amendments to the AUPs should be hand-signed (proof of acceptance can otherwise be difficult). This is not the only solution and sometimes the assessment will be that it is better to have something such as a click-accept, although that does come with risk (largely because of the authentication problem noted above (click-accept does not prove that the particular individual has click-accepted)). AUPs (dealing with security, privacy, porn, or other non-acceptable use, and so on) are important enough to get right.
- 5.3 In a recent case involving Air New Zealand, the desirability of getting the process right is highlighted. Even though in that case there was a shorthand way of achieving change in contract terms, that is generally too risky in this environment. For further background, see our paper, *Queen's Counsel Battles Air New Zealand: Can a Supplier Unilaterally Change Contract Terms?*<sup>8</sup> We specifically address AUPs in that paper.

---

<sup>7</sup> We go into more detail on this in the last paper mentioned above.

<sup>8</sup> See <http://www.wigleylaw.com/mainsite/QCBattlesAirNewZealand.html>

Wigley & Company is a specialist technology (including IT and telecommunications), procurement and marketing law firm founded 11 years ago. With broad experience in 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.*

© Wigley & Company 2005