September 1998

Will our law be competitive? Some data protection requirements considered

Jay Forder
Bond University, jay_forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder. (1998) "Will our law be competitive? Some data protection requirements considered" ,

Will our law be competitive
Some data protection requirements considered

by Jay Forder, Consultant Editor

A growing marketplace in legal systems

In a previous issue, we alluded to the analogy between the development of the Law Merchant and modern "cyberlaw." To be competitive and attract merchants in the Middle Ages, a Trade Fair organiser would have to adopt the best trade rules, or develop more efficient ones.

The similarities are obvious. Since electronic commerce knows no boundaries, modern merchants will site their businesses where the legal infrastructure is most supportive. Malaysia’s Multimedia Super Corridor is an example of an early attempt to provide such a supportive infrastructure. Any country wishing to be a major player in the digital marketplace will need to keep up with "legal best practices" in the market.

Thankfully Australian government leaders are beginning to realise this. Two recent examples spring to mind.

In June Alan Stockdale, Minister for Information Technology and Multimedia, announced that Victoria would push ahead with legislation on privacy and data protection. By 1 July his department released discussion papers regarding two legislative proposals: the Data Protection Bill (dealing with the security and privacy of personal data) and the Electronic Commerce Framework Bill (dealing with digital signatures) (see article on page 6).

By the end of July the Federal Minister for Communications, the Information Economy and the Arts, Senator Richard Alston, had joined the movement. He announced the launch of "a strategy for the information economy". It envisages wide business and community consultation in the development of relevant policies. Ten key priorities are identified. From the legal viewpoint, the interesting ones include the need to:

5. Influence the emerging international rules and conventions for electronic commerce, by ensuring a competitive domestic environment and enhanced export capability of Australian firms trading online, and pursuing appropriate bilateral and multilateral frameworks that reflect Australian national priorities.

and

8. Set the legal and regulatory framework for the information economy, by addressing key issues including the legislative framework for electronic commerce, taxation, security and authentication, privacy, protection of intellectual property, objectionable online content and consumer protection.

Development of the strategy will be undertaken by the National Office for the Information Economy (NOIE), a separate entity within the Minister’s portfolio. See page 7 for further details.

We will monitor these developments in future issues. In the meantime recent events highlight the need for data protection laws to be on the agenda.

The EFF announces DEScracker

On 17 July the Electronic Frontier Foundation (EFF) announced that it had cracked a 56-bit implementation of the Data Encryption Standard (DES). Estimates indicate that DES is responsible for between a third and a half of encryption technology sales.

Part of the reason for its market penetration is US Government policy. It prohibits the
The hacking problem

Viewing data protection from the other side of the coin, a supportive infrastructure requires vigorous investigation and punishment of unauthorised access.

Consider these two cases:

- In 1996 a 22-year-old Victorian who had a 49% share in an ISP business resigned to go into competition with his former company. His former company began to suffer innumerable server crashes because of unexplained configuration changes. It transpired that the youngster was using his old access privileges to sabotage his former company. He was given a $300 fine without the recording of a conviction, a 12-month good behaviour bond, and ordered to pay $791 restitution for free accounts he had opened after leaving.

- Compare this with the case of Skeeve Stevens. The events were reported widely in the press in October 1995. Stevens accessed Melbourne and Sydney ISP AUSNet’s server after he was unsuccessful in getting a job with them. He stole and distributed credit card details and changed their Web page, warning that AUSNet was “a disgusting network”. By sending himself (amongst others) anonymous email messages bragging about how he had done it, he managed to get himself quoted as a consultant giving opinions about the hack. He was eventually arrested and charged with several offences under the Crimes Act 1914 (Cth). He pleaded guilty to the main count of altering data stored in or inserting data into a computer (s 76E(a)). Judge Cecily Backhouse rejected the argument in mitigation that Stevens was motivated by “perverse altruism” in trying to show up slack security. In March this year the NSW District Court sentenced Stevens to 3 years jail. 10

Perhaps this shows that attitudes towards “hackers” are hardening. Will they be vigorous enough to facilitate growing commercial activity? One of the worrying features is that it took two and a half years for Stevens’ case to get through the system. He has lodged an appeal. Who knows how long it will be before finality is reached? The merchants of the Middle Ages expected their cases to be finalised “before the ebb and flow of the tide”. Won’t cybermerchants expect similar efficiencies?  

5 See <http://www.eff.org/descracker.html>. This was in response to RSA Laboratories’ “DES Challenge II” (see <http://www.rsa.com/rsalabs/des2/>).
7 See Customs (Prohibited Exports) Regulations as read with March 1994 “Australian Controls on the Export of Defence and related Goods – Guidelines for Exporters”.