

**AUSTRALIAN CYBERLAW CASEBOOKS V 1.0**

DAVID LINDSAY<sup>1</sup>

Brian Fitzgerald & Anne Fitzgerald, *cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce*

LexisNexis/Butterworths, Chatswood, 2002

ISBN 1863162089

Yee Fen Lim, *Cyberspace Law: Commentaries and Materials*

Oxford University Press, South Melbourne, 2002

ISBN 0195515765

[341] The internet boom of the late 1990s was followed, especially in the United States, by a boom in academic courses dealing with the law relating to the internet, with academic articles concerned with aspects of internet law, and by cases dealing with the application of substantive areas of the law to the internet. In the United States, this newly emerging field of law soon became known as ‘cyberspace law’ or ‘cyberlaw’. The term ‘cyberspace’, which had been coined by science fiction author William Gibson in the 1980s, was rapidly adopted, first, by the US internet community, then by policy-makers. The term became part of US legal discourse when it was defined by a federal district court, in the seminal decision in *ACLU v Reno (No 1)*, as ‘a decentralized, global medium of communications ... that links people, institutions, or corporations, and governments around the world’.<sup>2</sup>

In Australia, there was an initial reluctance, especially among sections of the legal profession, to use the term ‘cyberlaw’. The profession appeared more comfortable with ‘electronic commerce’, which seemed at once more definite and more serious. This preference seemed to reflect the practical bent of much Australian legal thinking. Messy conceptual issues relating to whether we were [342] seeing the emergence of a new area of the law and, if so, what it entailed, could perhaps be avoided by focusing on practical legal issues relating to the use of information technologies for commercial purposes. This sort of approach persisted in Australian policy circles

---

<sup>1</sup> Research Fellow, Centre for Media, Communications and IT Law, The University of Melbourne.

through the late 1990s. A good example of this thinking was the approach adopted to what was, perhaps, the first major public policy issue specifically related to the internet: the question of the regulation of internet content and, in particular, 'cyberporn'. Commonwealth legislation was introduced with the express object of restricting adult access to internet content, even though it was accepted that there were real technical obstacles in doing so.<sup>3</sup> The legislation was supported by arguments, essentially to the effect that 'it was better to attempt to do something than it is to do nothing'.<sup>4</sup> The normative issues associated with attempting to regulate access to content on a global, decentralised communications system were ignored, or given breathtakingly short shrift.

Yet, the challenges posed by the internet to the substantive law could not long be ignored. A considerable number of cases, in a diversity of areas, emerged from the United States. A relatively consistent cyberlaw syllabus appeared in most American law schools. The legal issues faced in the United States could not be avoided in Australia; although there were naturally fewer cases, the challenges posed to the substantive law by the internet were much the same in Australia as in the US (although the answers delivered by the respective legal systems sometimes differed). Some Australian legal scholars, especially those who had been working in the area of information technology law, began to devote more attention to the internet. Many Australian law schools introduced graduate courses in cyberlaw or internet law. The structure and content of the courses were influenced by approaches adopted in the United States, where the emergence of the internet spurred considerable thinking about the role of law in cyberspace. Academics responsible for cyberlaw courses were required to compile their own course material, which commonly consisted of the extant Australian cases and legislation, with quite a lot of American material. There was a dearth of quality Australian texts, and no Australian casebooks. The absence of

---

<sup>2</sup> 929 F Supp 824, 831 (1996).

<sup>3</sup> *Broadcasting Services Amendment (Online Services) Act 1999* (Cth), introducing Sch 5 to the *Broadcasting Services Act 1992* (Cth).

<sup>4</sup> The Second Reading speech to the Bill stated that: 'The Government acknowledges that the unique characteristics and rapidly changing nature of the internet present specific difficulties for regulation of internet content. It recognises that there are technical difficulties with blocking all illegal and offensive material that is hosted overseas but considers that where it is technically feasible and cost effective to block material this should be done. It is not acceptable to make no attempt at all on the basis that it may be difficult': *Broadcasting Services Amendment (Online Services) Bill 1999, Second Reading Speech*, Commonwealth of Australia, *Parliamentary Debates*, Senate, 21 April 1999, 3963.

an Australian casebook has now been addressed with the publication of two comprehensive collections of material: one edited by Brian Fitzgerald and Anne Fitzgerald; the other by Yee Fen Lim. The purpose of this review is to assess the strengths and weaknesses of the two books, which may assist academics seeking a suitable casebook for a cyberlaw course, or those seeking an introduction to cyberlaw from an Australian perspective.

### **The specificity of the internet**

Before comparing the casebooks, it may be helpful to review the differences between the internet and previous communications systems, and to explain why the internet challenges existing areas of the law.

The internet is the first global communications system that is not subject to centralised control, and which allows for individuals to communicate large amounts of information on a point-to-point basis. Unlike previous systems for transferring content from centralised sources, such as a publisher or broadcaster, the internet promotes horizontal transfers of information among geographically dispersed users. The internet is, in effect, a culmination of previous developments in communications and [343] information technologies combining, as it does, decentralised machines for efficiently producing and reproducing content (computer hardware and software) with a robust, multiply-redundant system for distributing information (a packet switched network of networks, using the TCP/IP suite of protocols).

The internet is an efficient communications system, mainly because it is global and decentralised. Nevertheless, the advantages of the internet as a communications system may, from the perspective of conventional legal systems, be seen as weaknesses. The internet is essentially without borders; from the point of view of a user, the ability to communicate should not depend upon physical location. Nation states, however, are geographically bounded entities. The authority of national governments to make or apply laws to extra-territorial activities and entities is limited. Moreover, the legitimacy of national governments derives mainly from the consent of geographically defined communities.

This may create difficulties where some harm is experienced within national borders, but the source of the harm is outside the jurisdiction of the nation state. Of course, problems involving the trans-border application of national laws pre-dated the internet. It is just that the internet has resulted in a volume of trans-border activities and transactions of an order of magnitude greater than anything previously experienced. Furthermore, the combination of the global and decentralised nature of the internet has created further difficulties. With centralised communications systems, such as the press or broadcasting, determining who should be liable for some wrong was not difficult. The internet, however, has facilitated a process known as 'disintermediation', meaning the removal of intermediaries. For example, information may be published to a large audience without being subjected to editorial filtering by a publisher or broadcaster. As the source of the harm may be an individual located anywhere in the world, it may be difficult to enforce a national law against the perpetrator, or to locate him or her. In a communications system in which users can be anonymous, at least to an extent, it may even be difficult to determine the identity of the perpetrator.

These difficulties do not mean that national laws cannot be applied to the internet. What they do mean, however, is that the law works differently online to the way in which it works off-line. In the online world, the law must work with the rules established by the technological infrastructure. The importance of understanding the role of technology in constraining online behaviour was first seriously examined by American scholars, such as Joel Reidenberg and Lawrence Lessig.<sup>5</sup> An important implication of this work is that, to be effective, the law may need to constrain behaviour indirectly, by first operating on the technological infrastructure. For example, as the internet is designed to facilitate the transmission of information regardless of the nature of the content, the technological infrastructure makes it difficult to discriminate between different kinds of content. In order to control information flows, then, [344]