BOOK REVIEW

Cyberlaw

[Brian Fitzgerald and Anne Fitzgerald, *Cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce* LexisNexis Butterworths Sydney 2002; 794p; RRP $242.00 Students $143.00 (inc. GST); ISBN: 1 86316 208 9]

Graham Bassett*

Introduction

At the end of 1999 I ceased work in the information technology (IT) industry.[1] Events that occurred while installing an IT system at a private school in Sydney left me a desire to study how cyberspace was to be regulated. As part of choosing a place to study law, I found myself at the open night of an eminent technology university in a major capital city. I asked a panel of experts what impact information technology, and more particularly the shift to a digital world was having on the world of law. After some hesitation along the row of Professors, one indicated that course lecture notes were available on the Web and case databases were useful for keeping up to date with current litigation. The impact of the digital world was seen as only changing a few legal processes. Any need to re-examine an approach to the laws themselves was not considered.

Apart from extensive work done at the University of New South Wales under the direction of Graham Greenleaf, my research into academic offerings in this nascent field led me to a summer school course by Southern Cross University at Byron Bay.[2] This course was entitled *Cyberlaw* and dealt with the Internet, digital intellectual property and electronic commerce. The main presenter at this course was Lawrence Lessig,[3] then Professor of Law at Harvard, who was

---

* BA, DipEd, MInfoTech, LLB(Hons)

1 The author of this book review studied law at Southern Cross University and worked as a researcher for Professor Brian Fitzgerald.

2 See: <http://www.scu.edu.au/schools/lawj/cyberlaw/>

3 The author of leading works in the area of Cyberlaw including: Lessig L, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999; Lessig L, *The Future of*

writing an *amicus curiae* brief at that time for the Microsoft anti-trust case.

The book[4] which is the subject of this review evolved from such courses taught by the authors and others in Australia and at Santa Clara University in Silicon Valley in the USA since 1996.

About the Authors

Experience in teaching and writing cyberlaw has given the authors ample qualifications to create such a book. It is a work of co-authorship by a sibling team with diverse interests and backgrounds in law.

Anne Fitzgerald, who had a background in social work before coming to law, completed a Doctor of the Science of Law at Columbia University, New York.[5] In compiling *Cyberlaw*, Anne drew on her extensive background in the areas of intellectual property and electronic commerce. She has published several books, numerous articles and book chapters on the law relating to digital technologies, and electronic commerce law.[6] In addition to her role at Southern Cross University's summer school on cyberlaw she presents legal issue modules in professional development units of the Multimedia and Electronic Commerce degrees at Griffith University. She has worked on government standing advisory committees including the Advisory Council on Intellectual Property (ACIP) which advises IP Australia and as a member of the Copyright Law Review Committee's Expert Advisory Group. In 1999 she served on the E-Business Working Party established by the Queensland Government's Communication and Information Advisory Board. She has industry experience as a technology lawyer for Software Engineering Australia and as senior solicitor in the Electronic Commerce group at Gadens

---

Ideas: the fate of the commons in a connected world, Random House, New York, 2001; also see: <http://cyberlaw.stanford.edu/lessig/>.

4 Fitzgerald B & Fitzgerald A, *Cyberlaw Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce*, LexisNexis Butterworths, Sydney, 2002

5 The book based on her Columbia dissertation was on mining agreements*: Mining Agreements: Negotiated Frameworks in the Australian Minerals Sector*, Prospect Media, Sydney, 2002; see <http://www.lexisnexis.com.au>.

6 For example see: *Going digital: legal issues for electronic commerce, multimedia and the Internet*, Prospect Media, St Leonards NSW, 1998; *Intellectual Property Law*, LBC, 2nd ed, March 2002.

Lawyers. She currently works as part of the Technology and Communication Team of the Crown Law Office in the Queensland Department of Justice and Attorney General.

Brian Fitzgerald is a Professor and Head of the School of Law at Queensland University of Technology (QUT) in Brisbane. He was an undergraduate student of law at the same university and holds postgraduate law degrees from Oxford University and Harvard University. During 2001, he was a Visiting Professor at Santa Clara University Law School in Silicon Valley USA, teaching a seminar on Digital Property. He was Head of the School of Law and Justice at Southern Cross University from 1998-2001. He is co-editor of one of Australia's leading texts on e-commerce, software and the Internet - *Going Digital 2000*[7] - and has published articles on Law and the Internet, Technology Law and Intellectual Property Law in Australia, the United States, Europe and Japan. In March 2001 he convened a forum on "Innovation, Software, and Reverse Engineering: Technological and Legal Issues" at Santa Clara University in Silicon Valley to discuss the ongoing significance of intellectual property law to reverse engineering and innovation in the software industry.

The Authors' Approach

The authors have taken a systematic approach in analyzing and presenting materials on the regulation of cyberspace. The book goes beyond traditional Australian and English blackletter cases and legislation. In fact, England is no longer the dominant source of precedent or influential case law. In addition to Australia, the authors derive material from the USA and European contexts as it is these jurisdictions that have been at the forefront of the law relating to cyberspace.

In addition to this transnational examination of regulation, the paradigm for regulation promoted by Lawrence Lessig is the basis for the organization of the book's materials. The selection of materials acknowledges that case law and legislation can not act alone in regulation and they coexist with other modalities of regulation – *social*

7 Fitzgerald B, et al (eds), *Going digital 2000: legal issues for e-commerce, software and the Internet*, 2nd ed, Prospect Media, St Leonards NSW, 2000.

norms (education), *markets* and *architecture* in the form of code.[8] Code manifests itself as a form of regulation in the creation of technological devices that enhance or promote an objective. For example, privacy enhancing technologies allow a user to survey a Web site before entry and content filters allow a user some control over unwanted content. Coded technological solutions allow creators of digital property to build copyright enforcement measures into their products. Mechanisms to protect copyright include pay-per-view, setting a number of uses before expiry limitations or requiring use of hardware keys to ensure a program runs on only one workstation. It is this state of flux between law, social norms, market forces and code that form the range of regulatory options that emerge in the materials of the book.

Who Should Use this Book

Lawyers who have secure practices applying the verities of Torrens Title to the transaction of atoms in real property may not find this book enticing. Practitioners who deal in property that is increasingly made up of intellectual property rights, assignment of such rights and licensing agreements that form the property of the future will find this book indispensable. Academics in the field of law should also make it a set reference book. In-house counsel in IT companies and in relevant government departments would find it has little time to gather dust on their shelves. In addition, because the book covers the four modalities of regulation it is highly relevant to system operators, chief information officers and IT managers in a local or wide area network.

What's Inside

The book is presented in four parts.

Part I - Nature of Cyberlaw

The first section examines the nature of cyberspace, content regulation and jurisdiction. The central platform of cyberspace is the Internet which is much more than a technical device. Through simulation the

---

8 Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harv. L. Rev.* 501, p 506-7

Internet "facilitates a plurality of lives or personalities…that legal discourse must appreciate in dealing with cyberspace".[9] Articles examine the liberty that is available on the Net due to its end-to-end architecture which places power and control in the hands of end users and disintermediates traditional forms of regulation.[10] Central to this examination is the debate between those who argue that current law can apply in cyber scenarios with minimal change and others who argue for a complete overhaul. "Regulators must decide how best to respond to this change in the effectiveness of a pre-existing legal protection or regulation."[11] The intangibility of information and consequent rise of the intellectual property domain over tangible property is addressed and the capacity of cyberspace to facilitate commerce but threaten its income is highlighted.

Post and Johnson[12] propose a Lex Internet with four types of jurisdiction. Firstly, existing sovereignties can extend current jurisdictions to the Internet. Secondly, existing sovereignties can enter multilateral agreements to establish new uniform rules. Thirdly, new international organizations can establish and enforce new rules. Finally, de-facto rules may emerge due to the complex interplay of the system architects such as sysops, users and Internet Service Providers. For example, a sysop in a school may apply the law by setting the parameters of filtering software.

Jurisdiction is closely examined. The State of Minnesota in the USA warns everyone they must submit themselves to their jurisdiction "knowing that information will be disseminated in Minnesota".[13] Another document demonstrates ways of minimizing Internet liability

---

9 Fitzgerald B, "Life in Cyberspace: A Simulating Experience" [1997] 3 *Computer and Telecommunications Law Review* 136-139, cited in Note 4, p 49-50

10 For example see: Lessig L, & Lemley M, "Petition to the FCC In the Matter of the Transfer of Control of Licenses form MediaOne Group, Inc to AT&T Corp" (1999), cited in Note 4, p 9.

11 Lawrence L, "Expert Brief A&M Records Inc v Napster Inc: The architecture of the internet: end-to-end", cited in Note 4, p 7-9

12 Johnson D & Post D, "And how shall the Net be governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law", <http://www.cli.org/emdraft.html>, cited in Note 4, p 123

13 Jew B, "Cyber Jurisdiction – Emerging issues and Conflicts of Law When Overseas Courts Challenge Your Web" (1998) 37 *Computers & Law* 24, <http://www.gtlaw.com.au>, cited in Note 4 p 187

in foreign countries.[14] The role of jurisdiction arises in other parts of the book, particularly with regard to e-commerce. Contract jurisdiction is examined in the Model Law on E-Commerce of the United Nations Commission on International Trade Law (UNCITRAL). Article 15 asserts contractual obligation arises at the place of business, or if more than one place of business then the one bearing the closest relationship with the transaction. If no place of business can be established then habitual residence of the contracting parties will be examined.[15]

Material on content regulation reflects the full range of the modalities of regulation. The Australasian Broadcasting Authority (ABA) places the responsibility on Internet Service Providers (ISP's) to apply architectural solutions in preventing access to overseas hosted illicit material by mandating the use of filters. The ABA suggests the application of market forces so ISPs provide differentiated filtering services based on demand. A clean service allows access to a known list of filters only. Alternately, a best effort service utilizes a proxy to block a list of known sites resulting in a best effort by the ISP that cannot be guaranteed. The ABA also enhances norm reinforcement through provision of an education framework.[16]

Part II – Digital Intellectual Property

One contributor pithily stated that the challenge to conventional law and commerce that has emerged in cyberspace is as follows:

> The enigma is this: if our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds? And, if we can't get

---

14 Cameron B, "Jurisdiction and the Internet" (2000) 42 *Computers & Law* 13, cited in Note 4, p 192

15 Article 15 (4) (b), UNCITRAL Model Law on Electronic Commerce, (1996) prepared by the United Nations Commission on International Trade Law (UNCITRAL), <http://www.un.or.at/uncitral/English/texts/electcom/ml-ec.htm>, cited in Note 4, p 483

16 Australian Braodcasting Authority, "What every Family Should Know – Filters and Label Tools", <http://www.aba.gov.au/family/family/tools.html>, cited in Note 4, p 267

> paid, what will assure the continued creation and distribution of such work?[17]

The book offers cases, legislation and persuasive material that relates to protection of informational value. International agreements, particularly for transmission of copyrighted material in digital form, are included such as the World Intellectual Property Organization (WIPO) Copyright Treaty (WCT). Current debate about what should emerge as the dominant form of control is examined in detail. Hugenholtz[18] indicates that in a digital economy direct contract relations by way of user licenses have become the norm. He poses the question whether the terms of these licenses and technological solutions that enforce intellectual property rights through code can override the statutory limitations and rights of copyright legislation. Arguing that we must be wary of a pessimistic future where the Net will lose much of its open character, he concludes "code will rule the Internet with iron logic". To counter such a future Hugenholtz champions the development of a body of public information law that secures a right of access to important information and safeguards the public domain in areas such as fair use.

The authors provide extensive coverage of Australian copyright legislation. Source code and the object code of a computer program are protected as a literary work. New provisions for non-infringement under the *Copyright Amendment (Computer Programs) Act 1999* (Cth) are detailed.[19] The Australian legislators have been careful to explicitly indicate that contractual provisions that seek to remove these provisions will be void. In addition, in order to maintain the open architecture of the Net, ISPs are not liable for breaches "where they merely provide facilities for communication and are not responsible for the content of the communication".[20] There is a call for an extension of protected works to a new category called 'indigenous

---

17 Barlow J P, "The Economy of Ideas: A framework for patents and copyrights in the Digital Age (Everything you know about intellectual property is wrong)", 2.03 *Wired* (March 1994) 84, cited in Note 4, p 281

18 Hugenholtz P, "Copyright, contract and code: What will remain of the public domain?", *Brooklyn Journal of International Law Symposium*, Brooklyn NY, 28 January 2000, cited in Note 4, p 287

19 Fitzgerald, Note 4, p 295. This act amends the *Copyright Act 1968* (Cth)

20 Fitzgerald, Note 4, p 297

cultural work' incorporating a recognition of communal ownership and right of cultural attribution.[21]

The extension of patents to business methods, which seek to emulate current practices in an Internet environment, is examined and lamented by many commentators. Patent applications that are contentious include a system for making bids at an online auction and the placing of a purchase order over the Internet.[22] The extension of a proprietary right over domain names via use of trademark law is examined. A domain name is seen as a contractual service rather than a proprietary right. Consequently, in *Network Solutions Inc v Umbro Intl Inc*[23], a group of registered names could not be garnisheed by a bankruptcy trustee to satisfy creditors. Conversely, once a domain name infringes on trademark law it becomes property and can be litigated as occurred in *Telstra Corporation v Nuclear Marshmallows*[24]. Usefully, the materials indicate how one may declare their rights in a domain name if a complaint is made against them.[25]

These materials indicate a central concern. The extension of intellectual property rights, particularly registrable ones that convey exclusive rights, may chill innovation and creativity in cyberspace if monopolies continue to arise.

Part III - Electronic Commerce; social issues concerning the networked environment

In this section the extent to which e-contracts should have equivalence with paper-based contract law is examined. Equivalency is hardest to maintain with regard to authenticity of contract and in ensuring integrity of the transaction. Electronic signatures are compared with their application to deeds and wills, particularly with regard to the old

---

21 Jaenke T, "Our Culture, Our Future: Report on Australian Indigenous Cultural and Intellectual Property Rights", cited in Note 4, p 334

22 Hartman, et al, Amazon.com United States patent 5,960,411 (28 September 1999), cited in Note 4, p 396

23 Id.au, [www.id.au/id-au.html], cited in Note 4, p 417

24 *Telstra Corporation v Nuclear Marshmallows*, WIPO Arbitration and Mediation Center Administrative Panel Decision Case No. D2000-0003 (18 February 2000), cited in Note 4, p 458

25 See: auDA Dispute Resolution Working Group, *Proposed .au Dispute Resolution Policy (auDRP) and Rules Report to the auDA Board,* June 2001, <http://www.auda.org.au/docs/auda-audrp-final.html>, cited in Note 4, p 471

requirement for a deed to be on parchment, vellum or paper.[26] The government infrastructure necessary for digital certificates and public key infrastructure is examined under the auspices of the National Office for the Information Economy via their Gatekeeper program.

Curiously, the authors have included social issues in the same section as that of e-commerce issues. This may be because economic rationalism tends to regard a social issue as having importance if it chills acceptance of economic opportunity in cyberspace. Consequently, privacy was seen as an important issue by the authors of one report because lack of trust has resulted in relatively slow adoption of consumer e-commerce "partly due to the reticence of consumers to supply information about themselves over the Internet".[27]

In cyberspace law the government legislates and it is up to industry associations to establish benchmarks by way of industry codes. The authors include material where the code may lift the bar of legislative obligation. For example, the Internet Industry Association (IIA) targets three areas for special attention. These are protection of data about children, use of direct marketing online favouring opt-in permission models and providing additional limits to use, collection and disclosure of data on residents of the European Union.[28]

If you do not know the difference between a 'samurai', a 'dark-side hacker', a 'cracker', a 'hacker', 'phreaking', 'spamming' and 'spoofing', the section on cybercrime is indispensable. It also contains interesting material for those who may have fallen for pump and dump online trading in recent share dealings, particularly during the tech boom. The move to global uniformity in criminal laws relating to computer attacks on computer data is also examined.

The final chapter on digital entertainment covers one of the most vexed areas of cyberspace. Development of technologies such as MP3 file compression and peer-to-peer connectivity has enabled widespread copying, communication and distribution of digital entertainment products. The targets of legal action have not been users

---

26 McCullagh A, Little P & Caelii W, "Electronic signatures: understand the past to develop the future" (1998) 21(2) *UNSWLJ* 452, cited in Note 4, p 499

27 Freehill's Internet Privacy Survey Report 2000, "Internet privacy survey shows Australian websites lacking", [2000] *PLPR* 1

28 Internet Industry Association Privacy Code launch Site, <http://www.iia.net.au/index2.html>, cited in Note 4, p 641

but creators of machines used to play infringing copies, operators of web sites containing infringing content and intermediaries such as Napster that allow searching and downloading of data. Cases on this are covered in detail in the materials. Nevertheless, at the time of writing this article it appears that some record labels are finally succumbing to the cyberspace model of distribution and marketing. EMI has announced plans in Australia to sell music through an online subscription service as a reaction to figures that show sharply declining CD sales in the USA.[29]

Conclusions

While the book has an excellent index of cases and legislation it suffers from lack of a page index. Lex Internet is replete with terminology. Such an index would be a valuable tool for the busy reader. Of even more concern is the lack of a Web site for updating information in the book that by its nature changes rapidly. The authors themselves speak of the "traumatic hours" spent culling the book.[30] They had to dispense with whole chapters on ISP liability and select business issues. A Net site would enable atom world publishers to 'walk the talk' in cyberspace by maintaining current materials. At the time of writing this review, the authors indicate such a site is nearly operational subject to permissions being granted.

These limitations aside, this book is a vast work of scholarship in a new legal domain. It presents big ideas and seeks to paint a big picture for our digital millennium. However, it is not a book that provides comfortable answers. Presenting such a vast range of material it emulates the open nature of the Net itself by enabling the end user, the reader, to ponder how cyberspace will be regulated.

---

29 Newman K, "If you can't beat 'em: CD label goes online", *Sydney Morning Herald*, 28 August 2002, p 3

30 Note 4, p xv