FOREWORD

DAVID VAILE*

From the early euphoria of cyber-libertarians declaring the independence of cyberspace from 'Governments of the Industrial World, you weary giants of flesh and steel',[1] it has been a one-way trip to ever greater and more pervasive regulation of the online domain. Those using iPads to connect to the net in a coffee shop in Sydney may now find themselves not so much anonymous free spirits beyond the reach of law but subject to laws from, and potential extradition to, many jurisdictions around the globe – whereas offline in the same place they could draw comfort from the hope that compliance with local law would be sufficient.[2]

But even domestic cyberlaw has become a confusing and dangerous maze for the hapless cybernaut. Earnest promises of 'technological neutrality' are honoured more in the breach than the observance (consider the 2006 Amendments to the *Copyright Act 1968* (Cth) legalising certain uses of music players and personal video recorders);[3] there is apparently careless erosion of hard-won civil liberties visited upon online versions of laws that retain those protections offline;[4] and we see the frequent introduction of poorly scrutinised, widely cast 'cyber' provisions for behaviours that may be more effectively regulated by existing law, creatively investigated and enforced.[5]

This edition of *Forum* offers glimpses into this curious regulatory zone, where it seems technological fetishism by stakeholders or legislators or misunderstanding by adjudicators can so easily overturn common sense, respect for long held values, or sober policy analysis. In some cases the nature of the online experience and context are truly different, but unconvincing analogies

* Executive Director, Cyberspace Law and Policy Centre, Faculty of Law; University of New South Wales.

1 John Perry Barlow, *A Cyberspace Independence Declaration* (9 February 1996) Electronic Frontier Foundation <http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration>.

2 See, eg, *United States of America v Griffiths* [2004] FCA 879, in which an Australian was extradited to the US for copyright infringement of US materials.

3 See, eg, David Vaile, 'Shifting Sands? The Moderate Impact of Australia's 2006 Copyright Exceptions' in Jeremy Malcolm (ed), *Access to Knowledge for Consumers: Reports of Campaigns and Research 2008–2010* (Consumers International, 2010) 61 <http://a2knetwork.org/a2k-consumers-reports-campaigns-and-reports-2008-2010>.

4 Compare the presumption of protection of privacy in telephone interception law with the presumption of retention of and easier access to traffic data in 'stored communications' law.

5 See, eg, Alex Steel, 'The True Identity of Identity Theft Offences: Measured Response or an Unjustified Status Offence?' (2010) 16 *Unviersity of New South Wales Law Journal Forum: Cyberlaw* 503.

from the 'real world' sometimes saddle online citizens with inappropriate versions of traditional models.[6] In other areas, the fundamental principles in workable conventional regimes may be a better basis from which to start than those proposed by voices crying 'but the internet is different!'[7]

Alana Maurushat argues that the Council of Europe's *Convention on Cybercrime*,[8] 'the only binding international treaty on cybercrime'[9], is no longer applicable in this the era of obfuscation tools.[10] Modern cybercrime makes use of malware, botnets, onion routing, DNS abuse, encryption, peer-to-peer connections and fast-flux injection, together with obfuscation, anonymity, massive distributed computational power and deniability of trace-back. This swings the balance of power in favour of the constantly evolving offender groups and away from the law enforcement and information technology ('IT') security forces in pursuit. So many of the technical underpinnings and social practices supporting activity propagated over networks have changed since the *Convention* was drafted that its 90s-era remedies may not only offer limited improvement beyond that in existing domestic law, but may also pose risks to free speech and privacy (in an Australia lacking effective legal protection of either). A particularly novel section of the article describes the Australian content warrant framework in conjunction with interception and real-time evidence collection technologies, and obligations for internet service providers ('ISPs') to use such technologies.

Keiran Hardy assesses 'Operation Titstorm' – an online protest against Australia's proposed internet filter – as an act of terrorism, arguing that the embarrassing (for the federal police) but essentially harmless offensive, is caught by Commonwealth terrorism provisions, so widely drafted are these offences borne in the often scrutiny-free territory of the 'war on terror'.[11] This is problematic, he argues, because it leaves no place for legitimate acts of online protest, or at least sets the penalty far too high for relatively minor cyber-vandalism.

Alex Steel argues that Australia's identity theft offences are so alarmingly broad as to criminalise a panoply of behaviour most would regard as legitimate.[12] Steel notes that this newly discovered category of crime has been ushered in

---

6 Lyria Bennett Moses, 'Creating Parallels in the Creation of Content: Moving from Offline to Online' (2010) 16 *University of New South Wales Law Journa Forum: Cyberlaw* 581.

7 See, eg, David Rolph, 'Publication, Innocent Dissemination and the Internet After *Dow Jones & Co Inc v Gutnick*'(2010) 16 *University of New South Wales Law Journal Forum: Cyberlaw* 562.

8 *Council of Europe's Convention on on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004) ('*Convention*').

9 Nigel Phair, 'Cybercrime and the Legal Dimension' (Speech delivered at the AusCERT Asia Pacific Information Security Conference 2009, Gold Coast, 19 May 2009) cited in Alana Maurushat, 'Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crimetools?' (2010) 16 *University of New South Wlaes Law Journal Forum: Cyberlaw* 431.

10 Maurushat, above n 9, 431.

11 Keiran Hardy, 'Operation Titstorm: Hacktivism or Cyber-terrorism?' (2010) 16 *University of New South Wales Law Journal Forum: Cyberlaw* 474.

12 Steel, above n 5.

since 2004 by those 'making hyperbolic claims that [identity theft or fraud] is the "fastest growing crime in the world" or the "crime of the millennium"',[13] recasting traditional fraud or impersonation offences as offences of identification information 'possession'. Steel argues that possession of information is here an inappropriate basis for criminalisation – on both theoretical and practical grounds – and contrasts the concept's less procrustean use in insider trading and child pornography offences.

Paul Roth examines the different approaches to data protection for 'web 2.0' content in Commonwealth jurisdictions.[14] 'Web 2.0' is Tim O'Reilly's popular term for second-generation internet applications through which people interact and collaborate with each other and content providers online, sharing information and forming web communities, in contrast to earlier, more passive non-interactive web services.[15] Roth argues that although the problems with privacy and web 2.0 content are significant, the role the law can play is probably minimal. Traditional privacy law, aimed at business and government as data collectors, assumes there is a third party extracting this information as the first step, and fails to cope with (often quite young) individuals voluntarily publishing their own personal information to the world in effect forever. Particularly problematic is user-generated content containing personal information about others posted online without authorisation from the individual to whom it relates.

David Rolph traces developments in online defamation law since *Dow Jones & Co Inc v Gutnick*[16] prompted alternating hot flushes (on the part of much of the Australian and global media industry, intervening fruitlessly) and unimpressed claims of 'storm in a teacup' from its critics.[17] A decade ago, when the case was decided, it raised a fundamental issue for cyberspace regulation: whether 'rules and principles should be technology neutral or technology specific, against the background of the common law's resistance to adapt, of its own motion, to reflect technological changes'[18]. Although past commentators tended to focus on private international law issues arising from *Dow Jones*, Rolph focuses on the case's impact on defamation: case law and legislative developments since 2002 suggest that while internet technologies triggered a revolution in communications, 'their impact on defamation law has not been equally radical'[19] – the teacup has not been as stormy as predicted.

Lyria Bennett Moses argues, against the backdrop of Australia's foreshadowed ISP-level complaints-based blacklist internet filter, that the internet is a qualitatively different medium from other means of information

13 Ibid, 503.
14 Paul Roth, 'Data Protection Meets Web 2.0: Two Ships Passing in the Night' (2010) 16 *University of New South Wales Law Journal Forum: Cyberlaw*, 532.
15 Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software* (30 September 2005) O'Reilly <oreilly.com/web2/archive/what-is-web-20.html> in ibid, n 2.
16 (2002) 210 CLR 575 ('*Dow Jones v Gutnick*').
17 Above n 7.
18 Ibid, 562.
19 Ibid.

distribution.[20] Just because we censor offline media in certain circumstances, does it necessarily follow that we should censor online media? She helps unravel a labyrinth of federal and state legislation regulating obscene and controversial content – a system that fails to address the extreme diversity in the format, source, audience, business model and culture of online material, where a book with its separate 'publication' classification scheme offline can become a mere file online, and a single text page online can be treated as a five minute film for classification purposes. The comforting technological neutrality principle behind the seemingly sensible proposal that 'what applies offline ought to apply online'[21] conceals the unwelcome reality that offline classification is itself a web of technologically specific special cases and is itself inconsistent.

Finally, Melissa de Zwart looks at the rights arising with respect to internet gaming communities and users of interactive social platforms.[22] A dramatic example is the class action earlier in 2010 'on behalf of persons who had owned, possessed, purchased, created or sold virtual land or other items of virtual property in Second Life.'[23] De Zwart asserts that contractual arrangements such as an End User Licence Agreement ('EULA'), Terms of Service ('ToS') or Terms of Use ('ToU') are inadequate to protect users' interests. In particular, the shared hallucination of 'property' rights in a virtual world does not map well onto the hard reality that the operator of such a world can ultimately pull the plug, whether literally (so the world just disappears), or figuratively (so the entity in which property is asserted suddenly behaves inconsistently with the 'owner's' claim, morphs, or just disappears).

The Editor of this edition is to be commended for drawing together such a diverse range of perceptive analyses to help illuminate the complex and inconsistent legal mosaic that the multi-jurisdictional, hyper-regulated internet has become.

20 Lyria Bennett Moses, above n 6.

21 Ibid.

22 Melissa de Zwart, 'Contractual Communities: Effective Governance of Virtual Worlds' (2010) 16 *University of New South Wales Law Journal Forum: Cyberlaw* 605.

23 *Evans v Linden Research Inc* (ED Pa, No 10-1679, 15 April 2010) (still at trial at time of print) Complaint [28] citedi n ibid, 605.