EDITORIAL

RENEE J WATT*

Networked transactions are the currency of modern life. From commercial to quotidian exchanges, critical infrastructure to the entertainment industry and the plethora of user generated fora, there are few activities in the developed world that do not at some point involve an internet connection. Recently, the international limelight has fallen on Iran, whose nuclear reactors have fallen to a computer virus so sophisticated it is thought to be the work of a nation state.[1] Recognising the risk of international and local cyber-attack, in 2010 the Australian Government created CERT Australia, a 'national computer emergency response team'.[2] As well, Australia is contemplating legislating for a national, mandatory internet filter, a system similar not only to those operating in Iran, Saudi Arabia and China, but also in Canada, the UK and Sweden.[3]

With a focus on the Australian legal landscape, this *Forum* of the *UNSW Law Journal* aims to promote an understanding of cyberlaw and some of the regulatory issues it generates. It does not intend to provide detailed analysis of all facets of the area but aims rather, through an eclectic collection of articles falling under cyberlaw's broad umbrella, to demonstrate the ubiquity of the technologies on which we rely and the pervasive importance of the law that regulates those technologies. While still scary and weird, cyberlaw is no longer an obscure niche interest, the domain of the computer nerd alone. Nor is cyberlaw merely a subset of intellectual property law. As the implications of online content for copyright law are both vast and popularly acknowledged, I have deliberately excluded intellectual property issues from this Edition. Articles in this Edition explore the (in)effect of the *Council of Europe's Cybercrime Convention*,[4] the possible operation of the Commonwealth terrorism provisions[5] on hacktivism, cyber-vandalism cyber-terrorism, the strange new breadth of identity theft offences, the

* Editor, Forum 16(1) and General Edition 33(2).

1 Edward Moyer, 'Stuxnet Worm Hits Iranian Nuclear Plant' *Cnet News* (online) 16 September 2010, <http://news.cnet.com/8301-1009_3-20017651-83.html>.

2 *CERT Australia: About Us* (January 2010) Australian Government <http://www.cert.gov.au/www/cert/cert.nsf/Page/About_Us>.

3 Alana Maurushat and Renée J Watt, 'Clean Feed: Australia's Internet Proposal' [2009] 7 *University of New South Wales Faculty of Law Research Series*, <http://law.bepress.com/cgi/viewcontent.cgi?article=1149&context=unswwps>.

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

5 *Criminal Code Act 1995* (Cth) s 100.1.

implications for privacy and data protection where user generated content is concerned, the scope of defamation law online, parity between online and offline content regulation, and, finally, the rights accruing to gamers and users of other online interactive social platforms.

Naturally, this Edition would not have been possible without the support and help of many. In particular, I thank Alana Maurushat, my advisor on all things cyberlaw; Alex Steel, whose advice as former Faculty Advisor to the *Journal* has been invaluable; Michael Handler and Edward Santow, the Faculty Advisors for this Edition; the anonymous referees; the *Journal*'s Executive Committee for its behind the scenes support; and of course the Editorial Board of the *Journal*, without whom there would simply be no *Journal*.