

Contents

- page 22 **Second Life — Real life, real crime!**
Dr Clare Sullivan UNIVERSITY OF ADELAIDE and
Dr Gregor Urbas AUSTRALIAN NATIONAL
UNIVERSITY
- page 27 **A legal model for government intervention to combat
online hate**
Andre Oboler ZIONIST FEDERATION OF
AUSTRALIA
- page 31 **Fairfax versus Meltwater: media monitoring services
and online publications**
Donna Short and **Orla Griffin** HENRY DAVIS YORK
- page 34 **Dealing with the risks associated with the use of
social media**
Judith Miller and **Julie Markoska**
DLA PIPER AUSTRALIA
- page 38 **Hidden in the cloud — the dangers of keeping your
data where you can't see it**
Michael Pattison and **Margaret Walsh**
ALLENS ARTHUR ROBINSON
- page 40 **International e-retail and GST**
Bastian Gasser and **Jeremy Sparkes**
MINTER ELLISON
- page 44 **Bad faith registration and use under the UDRP —
are the requirements explicit or Ferrlecit?**
Devita Pathi
- page 47 **Domain names**
Darren Sommers MEERKIN & APEL LAWYERS
- page 48 **Australia and the Council of Europe's Convention
on Cybercrime**
Dr Gregor Urbas AUSTRALIAN NATIONAL UNI-
VERSITY

General Editor

Sharon Givoni *Solicitor, Melbourne*

Editorial Board

Chris Connolly *Director, Galexia
Consulting*

Patrick Gunning *Partner, Mallesons
Stephen Jaques*

Adrian Lawrence *Partner, Baker &
McKenzie*

Debrett Lyons *IP Australia*

Brendan Scott *Principal, Open
Source Law*

Sally Foreman *Associate, Davies
Collison Cave*

A legal model for government intervention to combat online hate

Andre Oboler ZIONIST FEDERATION OF AUSTRALIA

- Racial hate propaganda is unlawful in Australia, and this extends to non-private online communications. This may create liabilities for technology companies.
- International discussions have highlighted the need for both national and international engagement on the problem of online racism. More active government involvement is inevitable in the future and poses a manageable risk to technology companies.
- The Copyright Act 1968 (Cth) provides a model for technology-based remedies to unlawful acts that take place online. This could serve as a template for remedies to other types of unlawful acts, including the spread of online hate propaganda.
- The Attorney General's announcement of a possible extension of "safe harbour" provisions in the Copyright Act to a larger range of service providers raises the questions of similar provisions for other unlawful activity facilitated by these providers.
- Lawyers advising clients who provide non-private online spaces should consider a range of legal developments in other areas, and should consider how similar provisions in the area of online hate may affect their clients. Engineering solutions to limit risk are possible and could be integrated into future development if considered pre-emptively.

Introduction

Online hate is the use of the internet to harass, defame, discriminate or incite against a person or group. It is a significant problem within the online world.¹ Hate propaganda forms a more limited class of content: it includes content "aimed at, or with the effect of, inciting hatred or contempt for individuals or groups of individuals identifiable on the basis of personal characteristics such as race, religion, ethnicity, gender, family status, marital status, and sexual identity that have historically formed the basis of socially imposed disadvantage".² Some, but not all, aspects of hate propaganda are unlawful in Australia as a result of Commonwealth and state anti-discrimination legislation.

One form of hate that is unlawful at both Commonwealth and state level is racial discrimination. The Racial Discrimination Act 1975 (Cth) and the Racial and Religious Tolerance Act 2001 (Vic) are examples of legislative provisions broad enough to directly tackle hate propaganda. There are, however, serious difficulties in the practical application of such laws to hate propaganda that occurs online. This is particularly true when third party platforms are involved.

This paper begins with a look at the existing law and its adaptability to meet growing demands that the government tackles online hate. It then examines the disempowerment of governments in the online world. Finally, it discusses the opportunity for companies to re-empower government and side-step the difficulties associated with policing their online spaces to prevent hate propaganda.

Online hate and the law

The internet is a powerful medium. Revolutions, enabled by online tools, have recently topped governments, and comparisons have been made to the role of mass printing in the 1848 revolutions in Europe.³ That much power, if used for hate propaganda, presents a real threat to society.

The danger of online hate propaganda was recently recognised in the Inter-parliamentary Coalition for Combating Antisemitism's Ottawa Protocol, which called for more research, expert advice and international cooperation into online hate.⁴

Within Australia, racially-based hate propaganda is unlawful. Section 18C of the Racial Discrimination Act makes unlawful acts that "offend, insult, humiliate or intimidate", on the basis of a person's race. This section was applied to internet material in *Jones v Toben*⁵ and resulted in orders for hate propaganda to be removed from the internet, as well as orders restraining republication.

The Victorian Racial and Religious Tolerance Act gives two standards of racial vilification, noting in both cases that the sections apply to "use of the internet or e-mail to publish or transmit statements or other material".⁶ This approach stands in stark contrast to efforts that address the specific nature of the online world in areas such as online copyright reform.

Government's active engagement with the online world

Attorney-General, Robert McClelland, recently noted that copyright reform "is challenging because of the speed of technological developments" and that "legislative solutions can lag behind reality".⁷ He championed government engagement and the need to "continually examine the areas of copyright that are ripe for reform".⁸ He explained the challenge saying "governments are being asked to try to find a national solution to a global problem — and to do this without stymieing growth in new technology and market solutions that deliver content to the community". This challenge exists in all interactions between government and the online world, including combating online hate.

In tackling digital copyright, new concepts such as the "safe harbour" provisions were created. These provisions give internet access providers a way to limit their liability for specific cases of copyright breach by taking active measures to facilitate general compliance. The measures access providers need to take are given in s 116AH of the Copyright Act. They include having a policy allowing termination of the accounts of repeat infringers, and compliance with industry codes aimed at protecting copyright material.⁹ Specific requirements are made for four types of activity a provider may engage in, each requirement closely tied to the way technology is used for that activity.¹⁰

Specific technical remedies can be written into law

The Copyright Act also provides enumerated remedies. Where the carrier acts as a conduit for information a user requested, the remedies are an order to terminate the users account,¹¹ or to limit access to material hosted overseas.¹² In the case of automatic caching, providing a user with storage capacity, or facilitating connections, the remedies include an order to terminate the user's account,¹³ to remove or disable access to the offending material,¹⁴ or any other less burdensome non-monetary order necessary.¹⁵ The Attorney-General has said that the "purpose of the scheme is to provide legal incentives for ISPs [Internet Service Providers] to cooperate with copyright owners in deterring infringement of copyright".¹⁶

The Attorney-General also suggested the "safe harbour" provisions be extended beyond access providers.¹⁷ This would require the law to gain an understanding of the nature of these services, as it has done with access providers. Many of these providers will be publishers of users' content, and laws setting standards for copyright may provide a model for handling other forms of unlawful conduct including the promotion of hate propaganda.

As the technology paradigm changes, so must the law

Access providers connect physically to the customer, so they must have a presence in Australia. Even when mediating communications within Australia, other service providers may be located entirely outside Australia. International mechanisms are needed to address issues that arise, these exist for copyright but not for the prevention of online hate propaganda. For now, as major service providers operate with such a large degree of autonomy over their online spaces, it begins to look like sovereignty, except for their care over copyright.

In reality, the rights of internet service providers are based on property and contracts law. It is their property rights over servers, networks and data storage devices, as well as intellectual property over source code, that gives technology companies authority. Participation in the virtual community is conditional on a licence to access the company's property. The terms of this licence, literally the "terms of service", give the company power to regulate users' activity.

The legal concept of property refers not to objects but to the rights people have in them.¹⁸ In the digital world, these rights, or the closest thing we have to them, are created by a company's terms of service. These rights can be abrogated or altered by statute, but the law will need to enter the digital world and regulate the activity rather than the technology.

A foundation for further engagement

In entering the digital world, governments need to reassert their rights. The power of internet companies may be legally based on property and contracts, but "property" in a resource stops where the infringement of more basic human rights and freedoms begins".¹⁹ In some jurisdictions, issues over privacy are now causing governments to assert themselves.²⁰ In Australia, the protection of human dignity is said to provide a basis for equities intervention.²¹ As the Supreme Court of New Jersey observed:

[P]roperty rights serve human values. They are recognised to that end, and are limited by it.²²

Today, private companies like Facebook seem to be able to ignore complaints from governments,²³ even over content calling for genocide and war crimes.²⁴ Instead, they are swayed by the media and online public opinion.²⁵ I have previously discussed a penalty model that could hold technology companies responsible when they fail to respond in reasonable time.²⁶ Another approach is for government to intervention in the online world itself. Technology companies, like Facebook,

would need to provide the tools, either voluntarily or in response to legislation. Similar requirements already exist in phone systems to enable wiretaps.²⁷

Powers governments may request, or legislate to require, include:

- the ability to delete public groups/pages;
- the ability to suspend accounts; and
- the ability to trace users and stored communications to an IP address.

In each case, this power could be limited to content controlled by users from within the country's territory. Checks and balances, including judicial oversight, could be included. Judges could give time limited authorisation, and all activities done using the authorisation could be logged. By empowering government, technology companies may be able to side step the problems and potential liabilities of online hate.

Conclusion

The current law in Australia makes race-based hate propaganda unlawful, but does not effectively tackle the online problem. Law reform may create greater liabilities for companies, or cases may establish existing liability. The development of copyright law provides a template for more technology specific remedies, and discussions on extending "safe harbour" provisions may provide an opportunity to discuss generally new considerations and remedies to unlawful acts online.

Those advising clients in the technology sector should be aware of the potential for increased government intervention. In particular, the mechanisms of the Copyright Act and the Telecommunications (Interceptions and Access) Act may suggest possible approaches government may consider to ensuring compliance with the Racial Discrimination Act in the future. Building such capabilities into platforms now may prevent future risk and disruption from legal reform.

Governments have a responsibility to take an active role in the online world; if they don't, they cannot meet their wider obligations to the people they serve. The powers, rights and limitations that apply to governments and private citizens in the real world need to be reflected online. The discussion over updates to the Copyright Act provides an opportunity to consider a wider picture of government involvement online.



Dr Andre Oboler,
Director, Community Internet Engagement Project,
Zionist Federation of Australia.

Footnotes

1. Digital Journal Staff, "Online hate" (2003) *Digital Journal*, available at www.digitaljournal.com;
2. J Bailey, "Private regulation and public policy: towards effective restriction of Internet hate propaganda" (2003) 49 *McGill Law Journal* 59, fn 6, pp 63–64.
3. F Zakaria, "Why it's different this time" (2011) *Time Magazine* (New York) 30–31.
4. A Oboler, "The ICCA tackles online hate" (2011) 13 *Internet Law Bulletin* 178.
5. *Jones v Toben* (2002) 71 ALD 629; (2002) EOC 93-247; [2002] FCA 1150; BC200205411, pp 655–656 at [113].
6. See, eg, Racial and Religious Tolerance Act 2001 (Vic), ss 7 and 24.
7. R McClelland, "Address to the Blue Sky Conference on future directions in Copyright law", speech delivered at the Blue Sky Conference on future directions in Copyright law, Sydney, 25 February 2011.
8. See above note 8.
9. Copyright Act 1968 (Cth), s 116AH(1).
10. Copyright Act 1968 (Cth), s 116AH(1).
11. Copyright Act 1968 (Cth), s 116AG(3)(b).
12. Copyright Act 1968 (Cth), s 116AG(3)(a).
13. Copyright Act 1968 (Cth), s 116AG(4)(b).
14. Copyright Act 1968 (Cth), s 116AG(4)(a).
15. Copyright Act 1968 (Cth), s 116AG(4)(c).
16. Above note 8.
17. Above note 8.
18. R Chambers, *An Introduction to Property Law in Australia*, 2nd edition, Lawbook Co, 2008, p 5.
19. K Gray, "Property in thin air" (1991) 50 *The Cambridge Law Journal* 252, 297.
20. Letter from Jennifer Stoddart, Alex Turk, Peter Schaar, et al, to Erich Schmidt, accessed 19 April 2010, available at www.online.wsj.com.
21. Above note 21, p 226 at [43].
22. *New Jersey v Shack* (1971) 277 A 2d 369, 372 (NJ, 1971).
23. E Levy, "Israel tells Facebook: remove intifada page", on *Ynet News*, 23 March 2011, available at www.ynetnews.com.

Internet Law

Bulletin

24. A Oboler, "Facebook and the third intifada: the aftermath", on *Jerusalem Post*, 30 March 2011, available at www.blogs.jpost.com.
25. A Oboler, "The rise and fall of a Facebook hate group", (2008) 13 *First Monday*, available at www.firstmonday.org.
26. A Oboler, "Time to regulate internet hate with a new approach" (2010) 13 *Internet Law Bulletin* 102.
27. Telecommunications (Interceptions and Access) Act (1979)(Cth), s 189.