DOXING IN AUSTRALIA: A PRACTITIONER'S PERSPECTIVE

MALCOLM CROMPTON*

This article provides a response to Åste Corbridge's article entitled 'Responding to Doxing in Australia: Towards a Right to Informational Self-determination' and considers the solutions to the problems of doxing suggested in that article. It also considers whether Australia's privacy laws need further reform and whether Europe's General Data Protection Regulation would provide an appropriate model for a solution in Australia. It concludes that for any change to the law to have an impact, it must not only be complemented by social leadership and education, but must also be backed by enforcement and resources.

CONTENTS

As Cardinal Richelieu is reputed to have said: 'Give me six lines written by the most honourable of men, and I will find an excuse in them to hang him'.[1]

I DOXING AND PRIVACY

The phenomenon where one person uses information about another person to blackmail or attack that person is as old as language in humans. The internet has simply given individuals who want to behave in this way a new medium by which to do so and through which to have a much greater impact. Doxing must be seen in this context: addressing doxing and similar forms of attack will require a strategy of many parts. The law, both statute and case law (and the enforcement of the law), will have an important part to play, but equally, so will culture, social norms, leadership and education.

* AM, BSc, BEc (Australian National University); Managing Director, Information Integrity Solutions Pty Ltd; Privacy Commissioner of Australia, 1999–2004.

1 Chris Berg points out that while these words are commonly attributed to Richelieu, they are possibly apocryphal: 'Surveillance and Privacy' (2014) 97 *Ethics Quarterly* 19, 21.

Åste Corbridge's primary article addresses one aspect of the ways in which doxing might be addressed: possible enhancements to the statute law in Australia.[2] Successive reports to the Commonwealth and state governments have advocated for the introduction of various forms of a 'statutory cause of action' that would give aggrieved individuals a similar right to that which a judge-made common law tort of privacy might deliver.[3] Although there is clearly support both by the public and on public policy grounds for such law as is advocated in the primary article, successive governments and parliaments have not yet delivered.

The main stumbling block in relying on a statutory cause of action is that bringing an action will not be cheap: somebody will have to fund the costs of litigation, whether it be the affected individuals or legal aid services on their behalf. In the real world, this will limit the availability of any protection ostensibly provided by such a new cause of action quite significantly. Accordingly, lower cost approaches to complaint management and restitution are often explored in the form of various regulators. This includes the Commonwealth, State and Territory Privacy Commissioners, Information Commissioners, and Human Rights Commissioners. Governments in Australia have recently strengthened their response to cyberbullying, as have their regulators.[4] The Children's eSafety Commissioner, with an expanded remit as the eSafety Commissioner, is taking a strong stand on these issues and has been empowered with new technologies to 'fight fire with fire'.[5]

[2] Åste Corbridge, 'Responding to Doxing in Australia: Towards a Right to Informational Self-Determination?' (2017-2018) 3 *University of South Australia Student Law Review* 1.

[3] These include Reports 108 and 123 by the Australian Law Reform Commission, summarised in the Commission's 2016 submission to the Senate inquiry into 'Revenge Porn*'* <https://www.alrc.gov.au/submission-senate-inquiry-revenge-porn>; the New South Wales Law Reform Commission report no 120 *Invasions of Privacy* <http://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report-120.pdf>; and the NSW Legislative Council Standing Committee on Law and Justice report on *Remedies for the Serious Invasion of Privacy in New South Wales* <https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryReport/ReportAcrobat/6043/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>.

[4] See, eg, the Australian Human Rights Commission pages on cyberbullying, starting with *Cyberbullying, Human Rights and Bystanders* <http://bullying.humanrights.gov.au/cyberbullying-human-rights-and-bystanders>.

[5] Office of the eSafety Commissioner, 'Online Portal Helps Australians Impacted by Image-based Abuse', Media Release, (16 October 2017) <https://www.esafety.gov.au/about-the-office/newsroom/media-releases/online-portal-helps-australians-impacted-by-image-based-abuse>.

II THE EUROPEAN MODEL

The primary article questions whether Australia's privacy laws need further reform and, as a possible way forward, points to the General Data Protection Regulation ('GDPR') that comes into force in the European Union early in 2018. However, consistent with privacy frameworks worldwide, neither the GDPR nor the various privacy laws in Australia apply to the actions taken by individuals that might invade privacy. The Australian Law Reform Commission, in Chapter 11 of Report 108,[6] rejected a change to these laws that would apply them to the actions of individuals because a number of the privacy principles in such laws are simply inappropriate (consider for example the impact on everyday life if individuals had to give formal notice to others that they are collecting personal information).

In any event, the approach taken in the GDPR does not appear to be appropriate in the Australian context. The GDPR introduces some new and useful concepts such as a 'right to be forgotten'; a broader right of the individual to a copy of personal information about themselves (including in machine readable format); and a potentially broader range of circumstances when Privacy Impact Assessments must be conducted. However, the GDPR is also highly procedural and imposes a significant increase in potential fines. This may result either in the provision being rarely used or in the institution of lengthy and expensive court cases. We are yet to see whether the GDPR leads to real change in people's lives or whether, like the EU Cookie Directive (which even the UK Information Commissioner has questioned),[7] the GDPR simply leads to annoying process and little else.[8]

More importantly, for any change to the law to have an actual impact on society, it must be complemented by social leadership, education, enforcement and hence cultural change. Of these, cultural change — making

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108, (2008) Chapter 11 <https://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20%28ALRC%20Report%20108%29%20/11-individ>.

7 Sophie Curtis, 'Information Commissioner Criticises "Dreamed Up" EU Cookie Directive', *Computerworld UK*, (17 September 2012) <https://www.computerworlduk.com/security/information-commissioner-criticises-dreamed-up-eu-cookie-directive-3381493/>.

8 See, for example, the typical but rather spirited views in Patricio Robles, 'Company Taunts ICO: Sue us Over Cookie Law', *Econsultancy*, (6 September 2012) <https://econsultancy.com/blog/10652-company-taunts-ico-sue-us-over-cookie-law>.

activity such as doxing socially unacceptable — will be most effective but will also be most difficult to achieve. The current debate in Australia about how to reduce the extent of family violence shows just how challenging this kind of cultural change can be.

Effective enforcement takes time and money. Yet whenever the law is changed, the level of additional resources necessary for investigating and enforcing that law is all too often ignored. Instead, debate focuses on the wording of the law, but not on how it will be enforced effectively. Most of the Commissioners mentioned in Part I are woefully under resourced: it seems that somebody keeps on leaving out the necessary additional zero before the decimal point in the moneys voted to the Commissioners in annual government budgets. Lack of resources is the real inhibitor to their effectiveness in Australia at present, not the wording, or existence, of the laws they enforce.[9]

Corbridge's article on doxing is an interesting, well researched and important contribution not only in considering the options for law reform in Australia to address the problem, but also in contributing to greater awareness in the wider world.

[9] Even the privacy regulators in the EU consider that they have the same problem, as set out in a letter from the Article 29 Working Party of EU's data protection commissioners to the President of the Council of the EU (8 March 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=43668>.