INFORMATIONAL SELF-DETERMINATION AND FREEDOM OF EXPRESSION

JAKE STONE*

This article provides a response to the article in this volume entitled 'Responding to Doxing in Australia: Towards a Right to Information Self-determination?' by Åste Corbridge. It begins in Part I by considering some of the elements which might be included in a statutory tort of serious invasion of privacy modelled on the EU General Data Protection Regulations. Part II considers the legal protection currently afforded to freedom of expression in Australia. Part III argues that we should proceed with caution because the proposed elements have serious implications for freedom of expression.

CONTENTS

I INTRODUCTION

I would like to begin by commending Åste Corbridge for her scholarly treatment of an important and difficult area of law reform. Doxing can present a serious and unwarranted intrusion into a person's privacy and the current

* LLB (Hons) (University of South Australia); Lecturer, School of Law, University of South Australia.

state of the law seems ill equipped to deal with these intrusions. Consequently, I am largely in agreement with Corbridge; the ability to have personal data removed from publication, to control personal privacy, and to be free from threats are all laudable goals. I do, however, wish to sound a word of caution: an increase in legal protection of privacy may lead to a diminution in freedom of expression. And, given the importance of free expression, any moves to increase regulation in this area should carefully consider any possible unintended consequences. With these worries in mind I would like to consider the possible impact upon freedom of expression of adopting a statutory cause of action for serious invasion of privacy which incorporates elements of the EU General Data Protection Regulations ('GDPR'). An understanding of these impacts then allows us to better formulate a statutory tort for serious invasions of privacy.

A *New Cause of Action for the Serious Invasion of Privacy*

Before considering possible adverse impacts on freedom of expression, it is helpful to consider some of the elements which might be included in a statutory cause of action for serious invasion of privacy. Corbridge recommends that the Australian Parliament should provide individuals with a right to informational self-determination and a corresponding statutory cause of action for a serious invasion of privacy modelled on the GDPR as a means to protect that right.[1] Two of the elements of the tort that Corbridge endorses in the primary article are:

1. An invasion of privacy as the result of the misuse of personal information about the plaintiff; and
2. The plaintiff must have had a reasonable expectation, objectively determined, of privacy in the circumstances. [2]

These are not the only possible elements of the tort but they are the elements that have important implications for freedom of expression. Under the approach proposed by Corbridge, the term 'personal information' referred to in the first element should be defined in accordance with the GDPR as: 'any information relating to an identified or identifiable natural person'.[3] This would encompass any information that could be used to identify a person, including, but not limited to: names, phone numbers, date of birth, and social

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

[2] Ibid 19, quoting Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) ('*Serious Invasions of Privacy Report*').

[3] Corbridge, above n 1, 24 quoting *Regulation (EU) No 2016/679* [2016] 119/33, art 4(1).

media posts.[4] Key to my worry is the idea, as advocated by Corbridge in the primary article, that the regulation of personal information should extend to both commercial and personal conduct.[5]

As with other torts, there exist situations in which it is desirable to allow exceptions to the right protected. Consequently, we need defences to breaches of an individual's right to informational self-determination. Such defences might include cases where:

1. Disclosure is in the public interest;[6]
2. The information revealed was already public;[7]
3. Disclosure is in the interests of national security;[8] and
4. A right to freedom of information should be protected.[9]

With the two elements listed above in mind let us consider the protection currently afforded to freedom of expression in Australia.

II LEGAL PROTECTION OF FREE EXPRESSION

When I talk of free expression I do not refer only to spoken acts. By free expression I mean more generally the ability to share information in both oral and written forms. Consequently, to characterise the effect of the proposed tort upon free expression we first need to consider the legal protections currently afforded to the sharing of information. Once these protections are set out we will have a clearer idea of the nature of free expression in Australia and whether it is diminished by the proposed elements.

A *Constitutional Protection*

The High Court has held that a general right to free expression is not protected by the *Australian Constitution*.[10] However, the *Constitution* does contain an

4 Ibid 24–5.

5 Ibid 27.

6 Ibid.

7 Ibid.

8 Ibid.

9 Ibid.

10 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 560; *APLA Ltd v Legal Services Commissioner (NSW)* (2005) 224 CLR 322, 350–1 (Gleeson CJ and Heydon J); *Levy v Victoria* (1997) 189 CLR 579, 594–5 (Brennan CJ), 638–41 (Kirby J).

implied freedom of communication regarding issues of government and politics.[11] This freedom is not a personal right but is rather a restriction on the exercise of legislative or executive power which prevents the use of those powers in a way that limits freedom of political communication.[12] However, this fetter on the exercise of legislative power is not absolute.[13] The legislature may enact laws which curtail freedom of political communication provided that such laws are: (1) compatible with the maintenance of a system of representative government; and (2) reasonably appropriate and adapted to achieving a legitimate purpose.[14] Aims which have been held to constitute a legitimate purpose include: the preservation of order in public places,[15] the prevention of violence,[16] the protection of individuals from insults which would intimidate or upset,[17] and the protection of individuals from the harm that arises by being publicly insulted.[18] Where a statute impinges upon freedom of political communication and is not reasonably and proportionately adapted to a legitimate purpose, it 'must yield to the constitutional norm'.[19]

It seems that it should be possible to establish a statutory tort which is constitutionally sound. Most of the doxing activity captured by a statutory tort will not concern political or governmental matters and consequently will not impinge upon the freedom of political communication. Additionally, doxing activity which does concern political or governmental matters could be regulated in such a way as to accord with the constitutional requirements. This is because freedom of political communication can be curtailed, provided such restriction is reasonably and appropriately adapted to achieving a legitimate purpose. Furthermore, the harmful effects of doxing could be legislated against because they are either included in, or closely related to, the types of harm that the High Court has held do justify curtailing freedom of political

[11] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 559–60.

[12] Ibid 560; *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168 (Deane J); *Cunliffe v The Commonwealth* (1994) 182 CLR 272, 327 (Brennan J).

[13] *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 142 (Mason CJ); *Levy v Victoria* (1997) 189 CLR 579, 598 (Brennan CJ), 619 (Gaudron J).

[14] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561–2; *Coleman v Power* (2004) 220 CLR 1.

[15] *Coleman v Power* (2004) 220 CLR 1, 32 (Gleeson CJ).

[16] Ibid 78 (Gummow and Hayne JJ), 98–9 (Kirby J).

[17] Ibid 121 (Heydon J).

[18] Ibid.

[19] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 566.

communication. In the case of delegitimising doxing, the aim of the doxer is to undermine the doxee's public standing. Conduct aimed at undermining a person's public standing falls within the legitimate aim of preventing public insult. Similarly, the goal of targeting and deanonymising doxing will often be to intimidate, humiliate or insult. And intimidating, humiliating or insulting are legitimate justifications for limiting free expression. Consequently, an action that restricts freedom of political communication in accordance with the *Constitution* seems achievable.[20]

B *International Protection*

In addition to the constitutional protections afforded to freedom of political communication, the international human rights regime also provides protection to free expression. As a signatory to the *Universal Declaration on Human Rights* ('*UDHR*'), Australia has pledged that it will respect this right. Specifically, the Australian Government acknowledges that:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[21]

Similarly, the *International Covenant on Civil and Political Rights* ('*ICCPR*'), to which Australia is a signatory, also acknowledges a right to free expression.[22] Under article 19 of the *UDHR* free expression includes a wide range of material and extends to expression which others might find 'deeply offensive'.[23] The right is not, however, absolute; the *ICCPR* recognises that the right to free expression carries with it obligations. Consequently, the right may be curtailed in order to protect the rights or reputation of others or in cases where it would be in the interests of public order and national security.[24] Importantly, curtailment must be provided for by law and be necessary in the

[20] This is not to say that such a tort could not be unconstitutional were it to target communication on governmental and political matters, just that there is nothing that *necessarily* renders the *Constitution* and a statutory tort incompatible.

[21] *Universal Declaration on Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 19.

[22] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19(2).

[23] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) para 11.

[24] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19(3).

circumstances.[25] Necessity in this context requires that any measures adopted must be proportionate to the harm protected against.[26]

The question then becomes: which rights will justify placing restrictions on free expression? There is a range of such rights, but in the case of doxing the most pertinent are those contained in articles 7 and 17 of the *ICCPR*. Article 7 provides that:

> No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation.[27]

And article 19 states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[28]

Notably, for the purposes of article 7, the Australian Human Rights Commission argues that cyber bullying and harassment can constitute cruel, inhuman or degrading treatment.[29]

As with the constitutional protections provided to free expression, it seems that there is nothing necessarily inconsistent with the international human rights regime and a statutory tort of serious invasion of privacy. It does not require a great imagination to envisage cases in which doxing would either constitute an arbitrary attack on a person's privacy and reputation, (thus violating article 17) or would constitute bullying (hence amounting to cruel and degrading treatment for the purposes of article 7). Consequently, violation of these rights would provide grounds on which to legislate against doxing even where such legislation would reduce freedom of expression. Furthermore, legislation could be drafted in a way that was proportionate to the harms prevented, by

[25] Ibid.

[26] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) para 34.

[27] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 7.

[28] Ibid art 17.

[29] Australian Human Rights Commission, *Background Paper: Human Rights in Cyberspace* (2013) 10.

limiting the tort's application only to the severe cases most likely to cause serious infringements of protected rights. For these reasons a statutory tort could be drafted which protects against the harms of doxing without violating the international rights regime. We should now turn to a consideration of whether a statutory tort of serious invasion of privacy based on the GDPR would satisfy the constitutional and international law requirements.

III WILL THE PROPOSED ELEMENTS SATISFY INTERNATIONAL AND CONSTITUTIONAL LAW?

Free expression and information are required for the establishment and maintenance of a democratic society.[30] Consequently, the United Nations Humans Rights Committee has determined that any proposed fetter on freedom of expression must satisfy 'a strict test of justification'.[31] Accordingly, a state must be able to show clearly how the proposed restriction protects the rights or reputation of others or is in the interests of public order and national security. The more broadly a limitation on free expression is constructed, the harder it will be to demonstrate that the limitation is justified. In fact, both current and former United Nations Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression have warned against the use of overly vague and broad legislation.[32] Specifically, former Special Rapporteur Frank La Rue advises that '[i]nadequate legal standards increase the risk of individuals being exposed to violation of their human rights, including the right to privacy and the right to freedom of expression'.[33] So when considering the impact of legislation upon free expression, we should be especially vigilant to guard against vague or broad provisions.

In light of the importance of freedom of expression and the admonishments by the United Nations Special Rapporteurs, I have two principal worries regarding

[30] Human Rights Committee, *Communication No 1173/2003*, 90th sess, UN Doc CCPR/C/90/D/1173/2003 (26 September 2007) annex I [8.10].

[31] Human Rights Committee, *Communication No 628/1995*, 64th sess, UN Doc CCPR/C/64/D/628/1995 (3 November 1998) [10.3].

[32] David Kaye, Special Rapporteur, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 35th sess, UN Doc A/HRC/35/22 (23 June 2017) 7 [18]; Frank La Rue, Special Rapporteur, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 23rd sess, UN Doc A/HRC/23/40 (17 April 2013) 13 [50].

[33] Frank La Rue, Special Rapporteur, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 23rd sess, UN Doc A/HRC/23/40 (17 April 2013) 13 [51].

the two elements of a statutory tort of serious invasion of privacy set out in Part I. First, the definition of personal information proposed by Corbridge and the GDPR is very broad and as such it captures a range of pedestrian information. Secondly, the limiting requirement that there be a 'reasonable expectation of privacy' is undermined by the fact that members of the public increasingly expect that what was once shared information will now be kept confidential. These factors mean that the proposed statutory cause of action could result in the sphere of information which is classified as private being dramatically expanded at the expense of free expression. This expansion in turn means that the elements proposed in Part I fall short of the constitutional and international law requirements that legislation be a proportionate response to harm.

A *The Definition of Personal Information*

The definition of personal information in the GDPR, which is approved by Corbridge, includes any information that could be used to identify a person, including, but not limited to: names, phone numbers, date of birth, and social media posts.[34] When applied to a commercial entity that gathers large amounts of personal information, restrictions on dissemination of that data are compelling. As the recent Equifax, Uber, Yahoo, and Target data breaches demonstrate, huge amounts of personal information can be disclosed at once. Consequently, the possible harm presented by commercial misuse of personal information is correspondingly large. This then justifies more expansive regulation of commercial entities; the possible harm that could be caused is large, hence the proportionate response to such harm should be correspondingly large.

When we consider the extension to cover the conduct of individuals rather than commercial entities, this argument is less compelling. Individuals are unlikely to have access to personal information on the scale that commercial entities do. They are, however, likely to share others' personal information regularly. Consequently, the potential harm that can be caused by an individual is relatively small in scale, but the potential intrusion upon an individual's free expression by limiting the use of personal data is large. The potential intrusion is large because the definition of personal information used by Corbridge and the GDPR encompasses such a broad range of pedestrian information. Remember that personal information is: 'any information relating to an

[34] Corbridge, above n 1, 24 citing EU General Data Protection Regulation Organisation, *GDPR FAQs* <http://www.eugdpr.org/gdpr-faqs.html>.

identified or identifiable natural person'.[35] For example, just today I have shared a friend's social media post, let my partner know the name of a work colleague, and checked in at a local restaurant letting others know who I was with. All of these cases involve the sharing of personal information as defined by the GDPR. Consequently, it is arguable that a tort based on the GDPR definition of personal information fails the constitutional requirement of reasonableness as well as the international law requirement that any restriction on free expression be proportionate; information misuse cases committed by a few are used to justify the restriction of everyday communication for everyone.

B *A Reasonable Expectation of Privacy*

The immediate response to this worry is to point to the fact that the tort would not be available for just any old sharing of personal information. There must be a reasonable expectation of privacy in the circumstances and in each of the everyday examples given above there is no such expectation. However, the limit imposed by the requirement that there be 'a reasonable expectation of privacy' cannot do enough on its own to make the tort reasonable and proportionate. The limiting requirement that there be a reasonable expectation of privacy is eroded by the fact that members of the public increasingly expect that certain types of information, which were once shared, will now be kept confidential. This means that it is now reasonable to expect a large range of pedestrian information to be kept private. Consequently, a reasonable expectation of privacy would allow much of our information sharing behaviour to remain the potential target of tortious liability.

Corbridge acknowledges, correctly, that the conspicuousness and reach of technology has made individuals more protective of their personal information.[36] As it becomes easier and easier to share information with the world, expectations about what information should be shared have become more stringent. Before the advent of the internet, people did not need to worry about the sharing of their personal information because the number of people that this information could be shared with was limited. Now, given that information can easily be shared with huge numbers of people, it is prudent to safeguard even relatively pedestrian information; my address being shared in my local village is much less worrying than it being shared with millions around the world. Consequently, it is reasonable to expect much more privacy regarding personal information than in the past. Therefore, even if we use a reasonable expectation of privacy as a limit on the statutory tort, many

[35] Ibid 24, quoting *Regulation (EU) No 2016/679* [2016] 119/33, art 4(1).

[36] Ibid 13–14.

commonplace acts of information sharing and collection will now give rise to tortious liability. It is for this reason that a reasonable expectation of privacy cannot do enough by itself to make the proposed tort reasonable and proportionate. But these concerns are not insurmountable. If we carefully construct the tort by adding additional elements and a range of defences, we can satisfy both the constitutional and international law requirements. Particularly promising additional elements include the Australian Law Reform Commission's recommendation that the invasion must be serious and that the misuse of information be intentional or reckless.[37] And if these extra elements are not enough, the defences listed in Part I should go a good way towards ameliorating the worries I have raised.

IV CONCLUSION

The fact that a limit based on 'a reasonable expectation of privacy' is unworkable, does not mean that a statutory cause of action based on the GDPR's definition of personal information is unsalvageable. Just that, the two elements I have discussed might fail the requirements of proportionality and reasonableness on their own. And to be fair, the tort has not been stated by Corbridge without restriction; several defences to the tort were proposed. This is important because appropriately designed defences could properly limit the scope of the tort, thus making it reasonable and proportionate. Elaborating on the nature of these defences is beyond the scope of this article. However, I hope that the concerns I have raised will encourage careful consideration of the limitations which should be placed on any legislation reducing freedom of expression.

[37] *Serious Invasions of Privacy Report*, above n 2, 19.