RESPONDING TO DOXING IN AUSTRALIA: TOWARDS A RIGHT TO INFORMATIONAL SELF-DETERMINATION?

ÅSTE CORBRIDGE*

Doxing is the term used to describe the act of publicly revealing an individual's personal information without their permission. It is a problem that concerns informational privacy and data protection. This article argues that the Australian Parliament should provide individuals with a right to informational self-determination and adopt a holistic approach to personal data protection. Part I defines the different aspects of doxing and identifies the adverse effects that doxing can have on victims. Part II considers the right to informational self-determination, before Part III examines solutions to the doxing problem. This article concludes that the Australian Parliament should consider enacting a statutory cause of action for a serious invasion of privacy that provides redress for doxing victims and introduces personal data protection regulations modelled on Europe's General Data Protection Regulation.

CONTENTS

* BA (Journ), University of South Australia; LLB student, School of Law, University of South Australia. I would like to thank Associate Professor Julia Davis for her feedback and comments while I was writing this article.

INTRODUCTION

The term 'dox' originated as slang for 'documents' when 'dropping dox' emerged as 'a form of revenge in 1990s outlaw hacker culture that involved uncovering and revealing the identity of people who fostered anonymity'.[1] The term doxing (or doxxing) is now broader and includes discovering and publicly revealing anyone's personal or identifying information without their permission.[2] It is important to address the doxing problem because the opportunities for exposing another person's private information publicly, and consequently leaving them vulnerable to harassment, are increasing with global engagement on online social networks. In 2014, the American Pew Research Centre surveyed 2849 web users about online harassment.[3] The results revealed that '73% of adult internet users have seen someone be harassed in some way online and 40% have personally experienced it'.[4] However, despite the adverse consequences of doxing, there is no direct cause of action available to victims in Australia who seek a remedy. The only Commonwealth legislation that protects personal information in Australia is the *Privacy Act 1988* (Cth) ('*Privacy Act*'), but it protects only the privacy of individuals who interact with government agencies, private businesses or organisations and does not offer a remedy to those whose details are revealed in a social context by other individuals.[5] Remedies could be sought in criminal or civil law, but only in limited circumstances, because the information that is revealed is often truthful, non-threatening and gained

1 David M Douglas, 'Doxing: A Conceptual Analysis' (2016) 18(3) *Ethics and Information Technology* 199, 200, citing Mat Honan, *What is Doxing?* (3 June 2016) Wired <https://www.wired.com/2014/03/doxing/>.

2 See, eg, Victoria McIntyre, '"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent' (2016) 19 *Tulane Journal of Technology and Intellectual Property* 111, 113; Douglas, above n 1, 200.

3 Maeve Duggan, *Online Harassment* (22 October 2014) Pew Research Center <http://www.pewinternet.org/2014/10/22/online-harassment/>.

4 Ibid.

5 *Privacy Act 1988* (Cth) s 2A ('*Privacy Act*'). See generally Sharon Givoni, 'Interview with the Honourable Michael Kirby AC CMG' (2016) 13 *Privacy Law Bulletin* 150, 151.

lawfully.[6] Examples of when remedies could be sought in equity, tort or criminal law are discussed further in Part I.

A survey conducted in Europe has found that around 'seven out of ten people are concerned about their information being used for a different purpose from the one it was collected for'.[7] Furthermore, only 15 per cent 'feel they have complete control over the information they provide online', and 31 per cent 'think they have no control over it at all'.[8] Informational privacy is a large transnational problem, since anyone can be doxed by anyone in the world. The Australian Parliament has two issues to consider in responding to doxing. The first issue is determining whether personal identifying information, including names, phone numbers and residential addresses, should be protected. The second issue is finding the right balance between personal privacy and freedom of information. While the case law in America is leaning towards protecting freedom of information,[9] the case law in Europe is leaning towards protecting the right to privacy.[10] In Australia, any new right to personal privacy will also need to be balanced against the rights provided in the *Freedom of Information Act 1982* (Cth) ('*Freedom of Information Act*'). The *Freedom of Information Act* provides that, when determining whether personal information has been unreasonably disclosed, regard must be had to 'the extent to which the information is well known', 'whether the person to whom the information relates is known to be (or to have been) associated with the matters dealt with in the document' and 'the availability of the information from publicly accessible sources'.[11] However, the object of the *Freedom of Information Act* is to protect the right of individuals to access 'information held by the Government of the

6 See McIntyre, above n 2, 118.

7 European Commission, 'Data Protection' (Special Eurobarometer Report 431, European Union, 2015) 7 <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf>.

8 Ibid 6.

9 See, eg, *Chan v Ellis*, 770 SE 2d 851, 852 (Ga, 2015); *Wilson v Harvey*, 842 NE 2d 83, 91 (Ohio Ct App, 2005); *Slibeck v Union Oil Company of California*, (Del Sup Ct, No WL-11542, 18 September 1986). These cases were cited by Victoria McIntyre, above n 2, 118.

10 See *Google Spain SL and Google v Agencia Española de Protección de Datos (AEPD)* (C-131/12) [2014] ECR 317.

11 *Freedom of Information Act 1982* (Cth) s 47F(2).

Commonwealth',[12] which may not include personal information posted on a social media website.[13]

This article focuses predominantly on the first issue; it asks whether personal information should be protected and attempts to develop an appropriate legal response to doxing committed in Australia in cases where one Australian resident doxes another. It argues that the Australian Parliament should legislate for the right to personal privacy, and should not leave it up to online service providers to determine the balance between the right to personal privacy and the right to freedom of information. Part I defines the different aspects of doxing and identifies the adverse effects that doxing can have on victims. Part II considers the right to informational self-determination, before Part III examines solutions to the doxing problem, including recommendations made by the Australian Law Reform Commission ('ALRC') and Europe's General Data Protection Regulation. Part IV concludes that the Australian Parliament should consider enacting a statutory cause of action for a serious invasion of privacy that provides redress for doxing victims and introduces personal data protection regulations modelled on Europe's General Data Protection Regulation.

I WHAT IS DOXING?

David Douglas distinguishes doxing from blackmail, defamation and gossip.[14] Doxing is not done with the expectation of receiving something in return.[15] The motives are often boredom or malice,[16] to intimidate, protest, or expose wrongdoing.[17] Neither is it defamation or gossip, because the exposed information is factual and not defamatory.[18] Doxing is a problem that raises the issue of a right to privacy. Nicole Moreham suggests that there are 'two types of overlapping but distinct privacy interference: the misuse of private information (informational privacy) and unwanted sensory access (physical

[12] Ibid s 3.

[13] See ibid s 27A, 47F.

[14] Douglas, above n 1, 202.

[15] Ibid.

[16] Stuart Blessman, 'What to Look for. How to Prevent It' (2016) 43(7) *Law Enforcement Technology* 33, 33.

[17] Douglas, above n 1, 200.

[18] Ibid 202.

privacy)'.[19] Doxing falls into the first category of informational privacy, which Moreham divides into three further subcategories.[20] To breach informational privacy, a person can: first, *discover* 'things about you that you wish to keep to yourself'; secondly, '*retain* private records or information about you either for his or her own future reference or with a view to sharing the information with others'; and thirdly, '*disclose* private information about you to others'.[21] The information could be a 'full name, date of birth, usernames, email accounts, home addresses, phone numbers, personal images',[22] or any other identifying details. The ALRC suggests that 'the most common type of misuse of personal information that will invade a person's privacy' is the disclosure of personal information.[23]

Gary Marx argues that informational privacy 'involves the expectation that individuals should be able to control information about themselves'.[24] He claims that there are multiple components to 'identity knowledge' and provides a list that classifies the 'degrees of identifiability'.[25] These degrees range from a person's name and address, to social categories, including gender, age and religion.[26] Douglas argues that 'Marx's list suggests, anonymity and obscurity are both forms of protection',[27] and suggests that '[i]t is anonymity's protective value that makes doxing particularly harmful … as it removes the subject's anonymity without an equivalent loss of anonymity for the attacker'.[28] Douglas claims that the control over 'identity knowledge', and the power to decide what and to whom personal information

[19] Nicole A Moreham, 'Beyond Information: Physical Privacy in English Law' (2014) 73(2) *Cambridge Law Journal* 350, 353.

[20] Ibid 354.

[21] Ibid.

[22] David Day, 'Seizing, Imaging, and Analyzing Digital Evidence: Step-by-Step Guidelines' in Babak Akhgar, Andrew Staniforth and Francesca M Bosco (eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Elsevier Science, 2014) 71, 75.

[23] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) 82 [5.44] ('*Serious Invasions of Privacy Report*').

[24] Gary T Marx, 'What's in a Name? Some Reflections on the Sociology of Anonymity' (1999) 15(2) *The Information Society* 99, 100.

[25] Ibid.

[26] Ibid 100–1.

[27] Douglas, above 1, 202.

[28] Ibid.

is revealed, 'is an important aspect of a person's identity'.[29] He argues that our relationships are shaped by what information we choose to reveal and receive in return.[30] Therefore, a person establishes their identity by influencing the way that others perceive them.[31] There is value in 'anonymity and obscurity', because it is 'difficult to build and easy to lose' your identity, including your reputation and public persona,[32] as the following examples of doxing will demonstrate. The examples will also demonstrate what act needs be done against a doxing victim to give rise to a remedy in criminal or civil law.

A *Categories of Doxing*

1 *Deanonymising Doxing*

Douglas states that there are three different categories of doxing: 'deanonymization, targeting, and delegitimization'.[33] The first category involves revealing the identity of a person who is either 'anonymous or known by a pseudonym'.[34] For example, 'Elena Ferrante' is the pseudonym of an Italian author who has sold more than 3.8 million books in over 40 countries.[35] For years readers speculated about the popular author's real identity, which was allegedly revealed in 2016.[36] Italian journalist Claudio Gatti claimed that he had discovered the real identity of the author after months of investigating the real estate transactions and financial records of a translator to whom Ferrante's publisher had made payments.[37] Many people were 'appalled by the attempt to unmask a woman who has purposely steered

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Ibid 200.

[34] Ibid 203.

[35] Claudio Gatti, 'Elena Ferrante: An Answer?', *The New York Review of Books*, 2 October 2016 <http://www.nybooks.com/daily/2016/10/02/elena-ferrante-an-answer/>.

[36] Stephanie Kirchgaessner, 'Elena Ferrante: Literary Storm as Italian Reporter "Identifies" Author', *The Guardian* (online), 3 October 2016 <https://www.theguardian.com/world/2016/oct/02/elena-ferrante-literary-storm-as-italian-reporter-identifies-author>. See also Alexandra Schwartz, 'The "Unmasking" of Elena Ferrante', *The New Yorker* (online), 3 October 2016 <http://www.newyorker.com/culture/cultural-comment/the-unmasking-of-elena-ferrante>.

[37] Ibid.

clear of the limelight and has always said that she only wanted to write books'.[38] Readers raised concerns over whether she would ever write again and called it 'an intrusion into the life of one of the world's most influential female writers'.[39] However, Gatti argued that 'Ferrante' was 'the most well-known Italian figure in the world, and that there was a "legitimate right for readers to know ... as they have made her such a superstar"'.[40] According to Gatti, the publishers had released an autobiographical essay about Ferrante's personal story which was 'full of untruths' and Gatti had felt compelled to expose the lies.[41]

In Australia, there would be no direct cause of action for Ferrante. The *Privacy Act* gives an individual the option of using a pseudonym when dealing with an agency or organisation, unless identification is required 'under an Australian law, or a court/tribunal order' or 'it is impracticable'.[42] However, Gatti, in his capacity as an individual or as a journalist acting for 'a media organisation' would not be liable under the *Privacy Act*.[43] The question is whether Ferrante should have a right to her anonymity in these circumstances. Douglas argues that it may be acceptable to reveal someone's identity in circumstances where 'a pseudonym is being used to deceive others for personal gain' and it is in the public interest to reveal it.[44] However, Ferrante did not use a pseudonym to deceive. She used it because she valued her anonymity. Ferrante would have a cause of action in Australia only if there was a right to informational self-determination, which is discussed in Part II.

2 *Targeting Doxing*

The second category, 'targeting doxing', involves revealing information about a person's physical location.[45] Douglas argues that targeting doxing can result in forms of harassment ranging from 'irritating pranks to physical

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid.

42 *Privacy Act 1988* (Cth) cl 2.

43 Ibid s 7B(4).

44 Douglas, above n 1, 204.

45 Ibid.

assault'. [46] Accidentally or innocently revealing someone's personal information does not amount to targeting doxing. The information must be presented 'in a manner that promotes harassing the subjects'.[47] For example, in the UK, Chloe Davis unknowingly had her photos, phone number and home address posted on an online dating website.[48] She had (incorrectly) assumed that her Facebook page was private, but someone accessed her page and used her personal information and photos to create a fake dating profile in her name.[49] Davis received a 'string of inappropriate texts' from strangers and was 'inundated with calls from delivery drivers and taxis claiming they had been sent to her house'.[50] She felt unsafe and contacted the police, who gave 'safeguarding advice', and suggested that she 'lock the doors' and contact the police again if there were any further incidents.[51] The online dating website removed the fake profile and Davis called taxi companies and takeaway food outlets to let them know not to take bookings or orders to her address.[52] If these events had occurred in Australia, Davis may have had a cause of action in tort and the doxing conduct may have given rise to criminal liability.

A doxer may be liable for a penalty of three years imprisonment under the *Criminal Code Act 1995* (Cth)[53] if a reasonable person would regard their online publication (and misuse of a telecommunication service) as menacing, harassing or offensive.[54] But the issue is whether a reasonable person would regard the initial publishing of the personal information in itself as menacing, harassing or causing offence. In South Australia, if the doxer has doxed another person on more than 'two separate occasions', the conduct may be

[46] Ibid.

[47] Ibid 205.

[48] Emma Lake, 'Plenty of Fish "Catfish" Con Sees Young Mum Bombarded with Seedy Texts from Strangers after Scammer Stole Her Facebook Photos for Fake Profile', *The Sun* (online), 22 March 2017 <https://www.thesun.co.uk/news/3131727/plenty-of-fish-catfish-con-sees-young-mum-bombarded-with-seedy-texts-from-strangers-after-scammer-stole-her-facebook-photos-for-fake-profile/>.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] *Criminal Code Act 1995* (Cth) s 474.17.

[54] Ibid.

categorised as stalking[55] and the doxer may be liable for a penalty of three years imprisonment.[56] The *Criminal Law Consolidation Act 1935* (SA) provides that a person stalks by 'electronic communication in a manner that could reasonably be expected to arouse apprehension or fear in the other person'.[57] This includes both a victim's fear for their reputation and their fear of public embarrassment.[58] However, a victim may not want to report the conduct and see the case brought to court, because the publicity could potentially prolong and increase the problem by exposing the doxee's personal information further — and as the ALRC has pointed out, the '[c]riminal law generally punishes the offender without necessarily providing redress to the victim'.[59]

If the doxing causes nervous shock or psychiatric injury, a victim of targeting doxing could attempt to bring a civil cause of action under the intentional tort established in *Wilkinson v Downton*.[60] For this action to succeed, the doxee must prove: first, that the personal information published by the doxer 'indirectly caused nervous shock or psychiatric injury' to the doxee; secondly, that the doxer 'wilfully intended to shock' the doxee, or was 'reckless about causing it'; and thirdly, that the doxing conduct was '"calculated" or objectively likely to cause nervous shock or psychiatric injury'.[61] The problem is that a remedy, which compensates for the 'natural and probable result of' the conduct,[62] will be available only in limited cases where the doxing victim suffers a psychological illness and not in cases where the victims experience only emotional distress and embarrassment.[63] Therefore, even though tort law's guiding principles include 'the principle of human dignity', 'self-determination and autonomy' and 'personal privacy',[64]

55 *Criminal Law Consolidation Act 1935* (SA) s 19AA(1)(a)(ivb).

56 Ibid s 19AA(2)(a).

57 Ibid s 19AA(1)(a)(ivb).

58 *Police v Gabrielsen* [2011] SASC 39 (25 March 2011) [14].

59 *Serious Invasions of Privacy Report*, above n 23, 295 [14.87]. In many states and territories, however, victims of crime may be eligible for awards under the relevant legislation dealing with victims of crime.

60 [1897] QB 57.

61 Julia Davis, *Connecting with Tort Law* (Oxford University Press, 2012) 149.

62 *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417, 488 [81] (Spigelman CJ).

63 *Serious Invasions of Privacy Report*, above n 23, 51 [3.50], citing *Wainwright v Home Office* [2004] 2 AC 406.

64 Davis, above n 61, 12.

it is unlikely that many doxing victims will find redress in this tort. For this reason, the ALRC has recommended the introduction of a new tort covering the serious invasion of privacy,[65] which is considered in Part III.

3 *Delegitimising Doxing*

The third category, 'delegitimizing doxing', involves revealing 'private information with the intention of undermining the subject's credibility, reputation, and/or character'.[66] Douglas argues that delegitimising doxing causes 'virtual captivity',[67] which means that a victim 'has few options to effectively avoid or exit cyber harassment.'[68] Once personal information has been posted on the internet, it is difficult to have the information removed.[69] This means that anyone who knows and interacts with the victim can potentially be exposed to the information.[70] Douglas argues that this possibility of exposure 'is enough to cause significant emotional distress and social withdrawal'.[71] For example, in Germany, a profile of a teacher was created on a website where students can rate their teachers. The profile provided 'her name, her school and the subjects she was teaching'.[72] The teacher 'filed a lawsuit seeking the erasure of the data and an injunction restraining the website provider from publishing this information again.'[73] However, the Court did not grant her request.[74] It held that the students' right to freedom of expression 'prevailed over the teacher's right to informational self-determination' on the grounds that: the information that had been posted was publicly available on the school's website; the comments were not defamatory and 'were only related to her working life as a teacher'; and

65 *Serious Invasions of Privacy Report*, above n 23, 9.

66 Douglas, above n 1, 205.

67 Ibid, quoting Mary Anne Franks, 'Sexual Harassment 2.0' (2012) 71(3) *Maryland Law Review* 655, 682.

68 Mary Anne Franks, 'Sexual Harassment 2.0' (2012) 71(3) *Maryland Law Review* 655, 682.

69 Ibid 683.

70 See Douglas, above n 1, 206.

71 Douglas, above n 1, 206.

72 Claudia Kodde, 'Germany's "Right to Be Forgotten" — Between the Freedom of Expression and the Right to Informational Self-Determination' (2016) 30(1)–(2) *International Review of Law, Computers & Technology* 17, 26.

73 Ibid.

74 Ibid 27, citing *Bundesgerichtshof*, decisions volume 181, 328.

'were not related to her private life'.[75] Unlike the case in Germany, Australia's *Constitution* does not give a right to informational self-determination. However, even if a legislative right to informational self-determination were to be provided in Australia, the outcome in a similar case could well be the same in an Australian court because this type of information is more likely to be classified as public information — and not as private information.

In Australia, the teacher may have had an action in equity if the information had been given in confidence. In an action for breach of confidence a victim must prove that: the information was confidential; 'that it was imparted so as to import an obligation of confidence'; and 'that there will be "an unauthorised use of that information to the detriment of the party communicating it"'.[76] However, using this cause of action raises two concerns. First, it is unusual to award equitable compensation for a noneconomic loss like 'emotional distress',[77] but an equitable remedy of an injunction could also be sought. Secondly, this action will not be made out in cases where the doxers themselves have sought out the personal information, because then the circumstances will not have imposed an obligation of confidentiality. Despite these limitations, the ALRC has noted that:

> in the absence of a statutory cause of action, the development of the equitable action for breach of confidence is the most likely way in which the common law may, in time, develop greater protection of privacy in relation to misuse and disclosures of private information.[78]

In all three categories, Douglas argues that the burden of proof should be 'on whoever wishes to disclose identity knowledge about the subject to justify why her anonymity or obscurity should be removed.'[79] Victims, on the other hand, should have to prove the harmful effect of the doxing. If it were otherwise, victims could make a claim based on any offensive conduct, regardless of whether it had any adverse effect. Douglas also argues that doxing may be acceptable in circumstances where 'there is a compelling public interest justification for revealing someone's identity' or 'if it exposes evidence of actual wrongdoing of public interest, and that the information

[75] Ibid.

[76] *Commonwealth v John Fairfax & Sons Ltd* (1980) 147 CLR 39, 51 (Mason J), quoting *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47.

[77] *Serious Invasions of Privacy Report*, above n 23, 270 [13.27].

[78] Ibid 265 [13.10].

[79] Douglas, above n 1, 206.

revealed must only be sufficient to establish that such wrongdoing has occurred'.[80] This is arguably the case for the anti-social wrongdoer who harasses other people.

B *The Effect of Doxing*

Regardless of whether doxing is justified, all categories have the effect of instilling fear in the victim about 'where the information may be posted next',[81] which can have adverse effects on both the users and the use of the internet. Doxing of users can lead to 'severe emotional distress to the victim',[82] which can lead to self-harm.[83] In the worst case, this can cause 'victims to take their own lives'.[84] Targeting doxing, where victims can be physically located, also 'increases the risk of physical harm' caused by a third person.[85] Furthermore, the publication of personal information:

> may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.[86]

The use of the internet can also be affected because victims will tend to leave the services or stop using the social media websites where they are harassed.[87] Victims may also lose trust and confidence in other online service providers. However, they may still want to keep using the service, because the alternative could mean 'less contacts with friends' and 'being considered

[80] Ibid.

[81] McIntyre, above n 2, 113.

[82] Ibid 118.

[83] Tom van Laer, 'The Means to Justify the End: Combating Cyber Harassment in Social Media' (2014) 123(1) *Journal of Business Ethics* 85, 85.

[84] Ibid.

[85] Douglas, above n 1, 200.

[86] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/16 [85] ('*General Data Protection Regulation*').

[87] Laer, above n 83, 85.

inefficient as a colleague'.[88] Consequently, online users may not exercise real choice in disclosing personal information. Julie Cohen argues that 'individuals may simply concede, and convince themselves that the loss of privacy associated with this particular transaction is not too great'.[89] These are issues that existing laws in Australia do not address.

If the Australian Parliament does not address the doxing problem, people may take matters into their own hands and turn to what Daniel Trottier refers to as 'digital vigilantism'.[90] Digital vigilantism 'is a process where citizens are collectively offended by other citizen activity, and respond through coordinated retaliation on digital media'.[91] Trottier argues that it 'is a user-led violation of privacy that not only transcends online/offline distinctions but also complicates relations of visibility and control between police and the public'.[92] Therefore, harassment of the doxer should not be allowed for the same reasons that doxing itself should not be allowed.[93] Furthermore, online service providers currently decide on how to balance the personal right of privacy with the public interest in freedom of information when asked to remove personal information from their websites. Leaving it up to online service providers to determine whether personal information should be removed from publication may result in adverse outcomes, not only because decisions may be made by a person not familiar with Australian law, but also because there is a possibility that no set precedents or rules will be followed.

The ALRC's two reports on privacy law in Australia demonstrate the value that Australians place on personal privacy and the need for further privacy legislation.[94] Given the value of anonymity, the effect that doxing can have on victims, and the possibility of 'digital vigilantism', the Australian

[88] Tobias Matzner et al, 'Do-It-Yourself Data Protection — Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer, 2016) 277, 297.

[89] Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (1999–2000) 52(5) *Stanford Law Review* 1373, 1397.

[90] Daniel Trottier, 'Digital Vigilantism as Weaponisation of Visibility' (2016) 30(1) *Philosophy & Technology* 55, 56.

[91] Ibid.

[92] Ibid 55.

[93] See generally Douglas, above n 1, 208.

[94] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) ('*For Your Information Report*'); *Serious Invasions of Privacy Report*, above n 19.

Parliament should consider protecting true, personal and identifying facts from publication under certain circumstances. While many phone numbers and addresses are publicly available, this older tradition is arguably decreasing with the increasing use of technology. People are becoming more protective of their personal details because the internet has opened the possibility for anyone in the world to contact another person at any time. This has resulted in many people electing to have silent or private phone numbers and to have mail sent to post office boxes rather than residential addresses.

Claudia Kodde argues that lawmakers have two options when responding to the rapid development of technology and the increase in sharing and collecting data over the internet.[95] They 'can either decide there is a legal obligation to protect the individuals' rights or [they] can decide in favour of a system of self-regulation.'[96] Australia is arguably leaning towards choosing the former. However, doxing victims will want their personal information removed from publication as quickly as possible, and going to court may not satisfy this desire. Victims may also avoid going to court because they want to avoid further publicity. Therefore, the Australian Parliament should consider the latter option of self-regulation and provide individuals with a right to informational self-determination.

II THE RIGHT TO INFORMATIONAL SELF-DETERMINATION

David Lindsey argues that the rise of social networking services 'coupled with virtually unlimited online storage capacity and powerful search functionality, creates significant challenges for individual autonomy and self-determination'.[97] He argues that due to 'the ease with which digital data can be copied and distributed, the most that can be done is to reduce the accessibility of the data'.[98] This is because 'it is impossible to ensure the removal of all data, although it is possible to restrict access by, for example, removing data from search engine indexes'.[99] Lindsay explains that '[t]he

95 Kodde, above n 72, 17–18.

96 Ibid.

97 David Lindsey, 'The "Right to Be Forgotten" in European Data Protection Law' in Normann Witzlebb et al (eds) *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 290, 332.

98 David Lindsay, 'The "Right to Be Forgotten" by Search Engines under Data Privacy Law: a Legal and Policy Analysis of the Costeja Decision' in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, 2016) 199, 201.

99 Lindsay, above n 97, 333.

"right to informational self-determination" is an attempt to apply the fundamental German constitutional concepts of respect for human dignity and individual autonomy to the context of data processing'.[100] In 1983, Germany was 'the first country to establish the principle of informational self-determination for its citizens'.[101] Germany's constitutional law recognises a general 'right to informational self-determination granting individuals the right to decide for themselves on how their personal data are released and used'.[102] In Germany, the right to informational self-determination is a personality right based on two constitutional rights: first, 'the protection of human dignity'; and secondly, 'the protection of general personal liberty'.[103] However, 'it is not an absolute right', because it must be balanced against other constitutional rights, including freedom of speech and information.[104] For some, the right to informational self-determination is a right to be 'the "master of one's private data"' and includes the right to ask to have it removed from the internet.[105] Others criticise it as 'a pantomime of privacy', due to intrusive surveillance measures surviving 'constitutional scrutiny so long as they are adapted to accommodate … safeguards that are meant to minimize and mitigate infringements on privacy'.[106]

Simone Fischer-Hübner et al argue that '[t]he principle of informational self-determination is of special importance for online privacy due to the infrastructural and interactive nature of modern online communication and to the options that modern computers offer'.[107] This is because the internet has become 'more complex', with businesses relying 'on a wide-range collection of user data for various purposes, such as marketing of online shops or

[100] David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) *Melbourne University Law Review* 131, 171.

[101] Simone Fischer-Hübner et al, 'Online Privacy — Towards Informational Self-Determination on the Internet' in Mireille Hildebrandt, Kieron O'Hara and Michael Waidner (eds), *Digital Enlightenment Yearbook 2013: The Value of Personal Data* (IOS Press, 2013) 123, 123.

[102] Kodde, above n 72, 18.

[103] Ibid 20.

[104] Ibid 20–1.

[105] Ibid 28.

[106] Russell A Miller, 'A Pantomime of Privacy: Terror and Investigative Powers in German Constitutional Law' (Working Paper No 5, Washington & Lee University, 19 February 2017) 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920115>.

[107] Simone Fischer-Hübner et al, above n 101, 123.

targeted advertising', including 'user profiling'.[108] Fischer-Hübner et al argue that 'many users of online services are unaware of the implications of this business model'.[109] They therefore suggest that 'informational self-awareness' about the consequences of sharing personal information online is necessary 'to give meaningful effect to the right to informational self-determination'.[110] However, Antoinette Rouvroy and Yves Poullet argue 'that the right to informational self-determination should not be interpreted as suggesting that controlling and manipulating information and data about oneself is an exercise of "self-determination"'.[111]

Australians do not have a constitutional right to informational self-determination. However, the ALRC argues that while the *Australian Constitution* does not expressly list privacy as a subject upon which the Australian Parliament can make laws, 'this does not mean that the Australian Parliament has no power in relation to privacy'.[112] New privacy legislation could be enacted under the external affairs power of the *Australian Constitution* s 51(xxix), which enables the Australian Parliament to make laws 'relating to Australia's obligations under bona fide international treaties'.[113] In 1980, Australia ratified the *International Covenant on Civil and Political Rights*, which provides in art 17 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 or reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[114]

The Australian Parliament can therefore enact legislation providing a right to informational self-determination. However, while informational self-

[108] Ibid 124.

[109] Ibid.

[110] Ibid 133.

[111] Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009) 45, 51.

[112] *For Your Information Report*, above n 94, 195 [3.18].

[113] Ibid 195 [3.19], citing *Commonwealth v Tasmania* (1983) 158 CLR 1; *Polyukhovich v Commonwealth* (1991) 172 CLR 501; *Horta v Commonwealth* (1994) 181 CLR 183.

[114] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

determination could assist in removing personal information from publication, it may be only a limited solution, because the information can be published quickly and widely on websites across the world.[115] The Australian Parliament should therefore consider a response to doxing that not only provides redress for victims, but also prevents misuse of personal information and facilitates timely responses to requests to remove personal information from publication. Lindsay argues that concerns about the power imbalance between data processors and individual data subjects is the reason behind the development of the European Union's data protection laws.[116] Europe provides informational self-determination through a 'right to be forgotten' in its General Data Protection Regulation, which gives individuals the right to seek to have personal information removed from publication.[117] Lindsay argues that 'the right to be forgotten' in Europe's General Data Protection Regulation 'was never meant to provide a perfect solution to the problems of digital eternity, but merely to strengthen the rights of data subjects to have data removed when it is legitimate and possible to do so'.[118] This article considers Europe's General Data Protection Regulation as a solution to the doxing problem in Part III.

III SOLUTIONS

This Part considers two solutions to the doxing problem: first, the recommendation by the ALRC to introduce a statutory cause of action for serious invasion of privacy; and secondly, Europe's General Data Protection Regulation, which takes a holistic approach to the protection of personal information and offers individuals a right to informational self-determination.

A *Recommendations by the ALRC*

The ALRC explains that the concept of information privacy 'involves the establishment of rules governing the collection and handling of personal data'.[119] Information privacy is, therefore, commonly known as 'data protection'.[120] In response to the issue of informational privacy in Australia,

[115] *Invasions of Privacy Report*, above n 23, 313–4 [16.16]–[16.17].

[116] Lindsay, above n 100, 171–2.

[117] *General Data Protection Regulation* [2016] OJ L 119/1, 11.

[118] Lindsey, above n 97, 333.

[119] *For Your Information Report*, above n 94, vol 1, 142 [1.31].

[120] Ibid.

the ALRC recommends a new Commonwealth statutory cause of action for serious invasion of privacy, which 'should be described in the Act as an action in tort'.[121] The new Act would aim to 'ensure uniformity and consistency in the operation of the cause of action throughout Australia'.[122] The ALRC prefers a new statutory cause of action separate from the *Privacy Act*, because it argues that the '*Privacy Act* largely concerns information privacy' and has a number of exemptions, including acts by small businesses,[123] journalistic acts,[124] and political acts,[125] which would not apply to the new action.[126]

The ALRC considers the new '*Serious Invasions of Privacy Act*'[127] to be 'a court-ordered remedial regime' and the *Privacy Act* to be a 'regulatory regime'.[128] The proposed statutory cause of action would 'remedy a number of different types of invasions of privacy',[129] and could 'be used against an individual acting in a non-commercial capacity, as well as against an agency or organisation'.[130] However, the ALRC also recommends an amendment to the *Privacy Act* that would extend the existing powers of the Privacy Commissioner to investigate 'complaints about serious invasions of privacy more generally',[131] and which would complement the new statutory tort.[132] Currently, the Australian Information Commissioner has the power to investigate complaints and make declarations that the complainant is entitled to compensation and/or that a respondent is to stop their conduct.[133] However, the declarations are 'not binding or conclusive between any of the parties to the determination',[134] which means that a complainant must go to

[121] *Serious Invasions of Privacy Report*, above n 23, 9.

[122] Ibid 59 [4.2].

[123] *Privacy Act 1988* (Cth) ss 6C(1), 6D.

[124] Ibid s 7B(4).

[125] Ibid s 7C.

[126] *Serious Invasions of Privacy Report*, above n 23, 59 [4.3].

[127] Ibid 62 [4.13].

[128] Ibid 60 [4.8].

[129] Ibid 59 [4.3].

[130] *For Your Information Report*, above n 94, vol 3, 459 [11.21].

[131] *Serious Invasions of Privacy Report*, above n 23, 27 [1.54].

[132] Ibid 309 [16.1].

[133] *Privacy Act 1988* (Cth) s 52(1).

[134] Ibid s 52(1B).

court to enforce it.[135] Under the new Act, a plaintiff would also need to go to court to enforce the breach. The difference is that an action under the new Act 'would lead only to a range of civil remedies sought by and for the benefit of the plaintiff', unlike the regulatory response under the *Privacy Act* which generally leads to civil penalties being imposed on an entity.[136] The issues are whether a victim of doxing would want to take a matter to court and whether it would be considered a serious invasion of privacy.

1 *A Response to Targeting and Delegitimising Doxing?*

A person who has had their phone number or residential address revealed (targeting doxing) or personal information released to undermine their credibility and reputation, (delegitimising doxing), could have an action under the ALRC's proposed new Act. For an action to succeed under the proposed Act, the plaintiff would have to 'prove that his or her privacy was invaded … [by] misuse of private information, such as by collecting or disclosing private information about the plaintiff'.[137] The ALRC recommends an objective test under the proposed new privacy tort, which would require the plaintiff 'to establish that a person in the plaintiff's position would have had a reasonable expectation of privacy, in all of the circumstances'.[138] However, different factors may affect what would be considered in relation to 'the reasonable expectation of privacy test'.[139] A court would need to consider the circumstances and context of each case,[140] including whether the information was considered public and whether a doxee had 'invited publicity'.[141] The Australian Government Attorney-General's Department has asked for clear guidelines 'to establish the point at which telephone numbers, email addresses or IP addresses become personal information'.[142]

[135] See ibid s 55A.

[136] *Serious Invasions of Privacy Report*, above n 23, 61 [4.10].

[137] Ibid 9.

[138] Ibid 92 [6.5].

[139] Ibid 97–8.

[140] Ibid 99 [6.37].

[141] Ibid 10.

[142] *For Your Information Report*, above n 94, vol 1, 302 [6.33], quoting Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007.

(a) Definition of Personal Information

The *Privacy Act* describes 'information privacy' as a breach in relation to an individual's personal information,[143] and defines personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable', including whether it is true or not.[144] Furthermore, it defines 'identification information' to mean an individual's full name, alias or previous name, date of birth, sex, 'current or last known address, and 2 previous addresses', current or last known employer, or driver's licence number.[145] The ALRC agrees with the definition of personal information in the *Privacy Act*, but recommends that '[t]he Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'identified or reasonably identifiable'.[146] The ALRC has considered the issue of whether a stand-alone phone number should be included in the definition of personal information if it is 'sufficient to allow communications with an individual'.[147] The ALRC argues that it 'would not fall within the recommended definition of "personal information"', unless it is used to target an individual, 'for example, with advertising material', because 'the *Privacy Act* is not intended to implement an unqualified "right to be let alone"'.[148]

Samuel Warren and Louis Brandeis defined privacy as 'the right of the individual to be let alone' in 1890.[149] They argued that the 'principle which protects … against publication in any form, is in reality not the principle of private property, but that of an inviolate personality'.[150] Additionally, the value of privacy was 'in the peace of mind or the relief afforded by the ability to prevent any publication at all'.[151] In Australia, the Public Interest Advocacy Centre ('PIAC') supports the right to be let alone and argues that it

[143] *Privacy Act 1988* (Cth) s 13(1)(a).

[144] Ibid s 6(1).

[145] Ibid.

[146] *For Your Information Report*, above n 94, vol 1, 309 [6.63].

[147] Ibid 298 [6.20], citing Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004; Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007.

[148] Ibid 309 [6.61].

[149] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193, 205.

[150] Ibid.

[151] Ibid 200.

'is an important element of the right to privacy and should be included in the *Privacy Act*'.[152] The PIAC supports the view of the Senate Committee privacy inquiry that the definition of personal information should 'include information "that enables an individual not only to be identified, but also contacted"'.[153] This would include the publication of a person's name and address. For example, telemarketers can be a nuisance and make a person feel like their privacy is invaded, because the person often does not know where the stranger obtained their phone number and would prefer not to be called if they had been given a choice.

Daniel Solove, however, argues that many view the definition of 'the right to be let alone' as being too broad, with the potential for any 'offensive or harmful conduct' to be taken 'as a violation of personal privacy'.[154] The ALRC also does not provide an exhaustive list of what 'unqualified' means regarding the right to be let alone. Furthermore, it argues that the definition of personal information 'will continue to give rise to theoretical uncertainty' due to the need for the new laws to be applicable to a general range of circumstances.[155] However, the description of personal information by the ALRC as information that enables a person to be targeted, arguably includes a doxer who enables others to harass an identified individual. But if the personal information was published in isolation, without it attaching to an individual, it would not fall within the ALRC's 'recommended definition of "personal information"'.[156] In these circumstances, the doxee would have no right to remove the personal information from publication.

(b) The Right of Data Erasure

The ALRC supports the right of individuals to have personal information removed from publication.[157] This right is also known as 'the right to be

[152] *For Your Information Report*, above n 94, vol 1, 304–5 [6.44], citing Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007.

[153] Ibid, quoting Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.14].

[154] Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1102, citing Anita L Allen, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield, 1988) 7.

[155] *For Your Information Report*, above n 94, vol 1, 309 [6.62]–[6.63], citing Malcolm Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

[156] Ibid 309 [6.61].

[157] Ibid 459 [11.23].

forgotten' or the right of data erasure.[158] However, the ALRC does not recommend 'a take-down notice scheme', even though it 'might help to address the circumstances where individuals refuse to remove from their website personal information about another person'.[159] The ALRC recommends that 'it is more appropriate for a court, rather than a regulator', to consider a remedy based on a statutory cause of action for a serious invasion of privacy, because a take-down scheme requires 'a decision maker to balance the right of freedom of expression and the right to individual privacy'.[160] Instead, the ALRC recommends new regulatory powers that 'would complement a statutory tort, providing a low cost alternative to litigation, which may, in some cases, lead to a satisfactory outcome for parties'.[161] However, the new powers would extend only to investigating complaints and making 'appropriate declarations', including referring the matter 'to a court for enforcement'.[162] They would not have the power to remove personal information from publication. If a respondent refused to adhere to a declaration to 'not repeat or continue the conduct complained about … the complainant would need to apply to the Federal Court or Federal Circuit Court for enforcement'.[163] Considering the ALRC acknowledges the importance of an individual being 'empowered to have their personal information destroyed — or, at a minimum, de-identified — when appropriate',[164] it should allow for a timely response to the request of an individual to remove personal information.

2 *A Response to Deanonymising Doxing?*

The ALRC also supports the right of 'individuals to retain greater control over their privacy by giving them the option to transact anonymously' and pseudonymously, when appropriate,[165] 'lawful and practicable'.[166] The

[158] EU General Data Protection Regulation, *GDPR Key Changes* <http://www.eugdpr.org/key-changes.html>. David Lindsay makes a slight distinction between 'right to erasure' and 'the right to be forgotten': above n 98, 201.

[159] *For Your Information Report*, above n 94, vol 1, 459 [11.22].

[160] Ibid 459 [11.23].

[161] *Serious Invasions of Privacy Report*, above n 23, 309 [16.1].

[162] Ibid 310.

[163] Ibid 313 [16.14].

[164] Ibid 319 [16.44].

[165] *For Your Information Report*, above n 94, vol 1, 693 [20.14]; 696 [20.25].

[166] Ibid 696 [20.28].

Privacy Act provides that individuals who deal with an agency or organisation 'have the option of not identifying themselves, or of using a pseudonym'.[167] However, this refers only to individuals interacting with agencies or organisations and not with other individuals. The ALRC only considers anonymity between an individual acting in a personal capacity and a business, and does not discuss the issue of anonymity between individuals acting in a personal capacity. Consequently, doxers may not be liable for revealing the identity of a person who is either anonymous or known by a pseudonym. However, the test may be whether a person considers that the doxee 'had a reasonable expectation of privacy'.[168]

The ALRC recognises the importance of individual private persons being able to 'exercise a degree of control over their personal information, especially information that they may themselves have provided previously'.[169] However, the proposed Act does not apply between individuals acting in a personal capacity. Furthermore, it may not assist in the timely removal of personal information from publication and it does not assist in preventing doxing through better data protection regulation. The Australian Parliament should therefore consider providing individuals with a right to informational self-determination and greater data protection regulation in a similar manner to Europe's General Data Protection Regulation.

B *The EU General Data Protection Regulation*

The European Parliament and the Council of the European Union provide that it is a fundamental right for individuals to have control over their personal data and that it is a right that must be protected.[170] They recognised the increase in individuals collecting, sharing and making available personal information 'publicly and globally'.[171] Consequently, in April 2016, the European Union ('EU') adopted the General Data Protection Regulation ('GDPR'), which will come into full effect in May 2018. The intention of the GDPR is 'to update the standards to fit today's technology while remaining general to simply protect the fundamental rights of individuals throughout

[167] *Privacy Act 1988* (Cth) sch 1 cl 2.

[168] *Serious Invasions of Privacy Report*, above n 23, 92 [6.5].

[169] Ibid 319 [16.44].

[170] *General Data Protection Regulation* [2016] OJ L 119.

[171] Ibid 2.

future waves of innovation'.[172] The GDPR is based on 'principles for the processing of personal data' set by the Organisation for Economic Co-operation and Development,[173] of which Australia is a member.[174] However, these principles are non-binding guidelines.[175] The GDPR is a binding legislative act across the EU that 'seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States'.[176] However, the jurisdiction of the GDPR extends to all organisations that 'offer goods and services' and hold personal data of individuals residing in the EU, regardless of where the organisation is located in the world.[177] There are ongoing discussions around setting 'up a one-stop-shop for data privacy regulation'[178] to replace the current model where each state has a supervisory authority.[179]

The GDPR seeks to balance the rights of individuals to control their personal data (user control), the responsibility of the processors of personal data (data processors), and the role of the monitors who ensure 'compliance with the rules for the protection of personal data' (data controllers).[180] It defines personal data as meaning 'any information relating to an identified or identifiable natural person'.[181] This includes any personal information which can be used to identify a person, 'directly or indirectly', for example, a name, telephone number, date of birth and 'posts on social networking websites'.[182] Breaches by organisations can include: 'not having sufficient customer consent to process data or violating the core of Privacy by Design concepts'; 'not having their records in order'; and 'not notifying the supervising

[172] EU General Data Protection Regulation Organisation, *How Did We Get Here?* <http://www.eugdpr.org/how-did-we-get-here-.html>.

[173] Ibid.

[174] Organisation for Economic Co-operation and Development, *Members and Partners* <http://www.oecd.org/about/membersandpartners/#d.en.194378>.

[175] EU General Data Protection Regulation Organisation, above n 172.

[176] *General Data Protection Regulation* [2016] OJ L 119/1, 1[3].

[177] EU General Data Protection Regulation Organisation, *GDPR FAQs* <http://www.eugdpr.org/gdpr-faqs.html>.

[178] Ibid.

[179] *General Data Protection Regulation* [2016] OJ L 119/1, 65, art 51.

[180] Ibid 3[11].

[181] Ibid 33, art 4(1).

[182] EU General Data Protection Regulation Organisation, above n 177.

authority and data subject about a breach or not conducting impact assessment'.[183] A breach of the GDPR can result in a fine of €20 million or up to 4 per cent of an organisation's annual global turnover, 'whichever is higher'. [184] A controller must 'implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed' (privacy by default).[185] This means 'that privacy-friendly default settings should be the norm — for example on social networks'.[186]

One of the key features of the GDPR is its recognition of 'privacy by design'. Privacy by design means that protection of privacy must be considered throughout the 'life cycle of the system or process development'.[187] The GDPR provides:

> the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures…[and] integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects [privacy by design].[188]

Nevertheless, the GDPR 'does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity'.[189] In 2013, a recommendation to Europe's previous Data Protection Directive (95/46/EC) argued that regulating 'natural persons' personal or household processing activities … could inhibit individuals' freedom of speech and could in itself constitute a breach of the individual's right to privacy'.[190] This is arguably the reason why the GDPR does not currently apply to individuals

[183] Ibid.

[184] *General Data Protection Regulation* [2016] OJ L 119/1, 83, art 83(5).

[185] Ibid 48, art 25(2).

[186] European Commission, 'How Does the Data Protection Reform Strengthen Citizens' Rights?' (Factsheet, European Union, 2016) 3 <http://ec.europa.eu/newsroom/document.cfm?doc_id=41525>.

[187] EU Data Protection Regulation Organisation, *Data Protection by Design and by Default* <http://www.eudataprotectionregulation.com/data-protection-design-by-default>.

[188] *General Data Protection Regulation* [2016] OJ L 119/1, 48, art 25(1).

[189] Ibid 32, art 2(2)(c).

[190] *Council Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* [1995] OJ L 281/31, Annex 2 ('Proposals for Amendments Regarding Exemption for Personal or Household Activities') 2.

acting in a personal capacity, which means that a doxer would not be held liable for their actions under the GDPR. However, the GDPR does apply 'to controllers or processors which provide the means for processing personal data for such personal or household activities', including social networking websites.[191] This means that the doxee could seek to have their personal information removed by lodging 'a complaint with a supervisory authority',[192] who has the power to investigate, 'to order the rectification or erasure of personal data' and to impose administrative fines.[193] The GDPR provides that a person should be provided with 'mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object'.[194] A response to a request should be provided 'without undue delay and at the latest within one month'.[195] Alternatively, a doxee can also pursue, according to the GDPR, 'an effective judicial remedy'.[196] However, to receive a judicial remedy, the doxee would need to commence proceedings in a court and, as discussed above, this is not the preferred method to address doxing.

IV CONCLUSION AND RECOMMENDATIONS

The Australian Parliament should consider implementing a similar scheme to the GDPR to keep up with technological changes and to improve the protection of informational privacy in Australia. It has been argued that the 'GDPR will set a new global standard for personal data protection'.[197] If the GDPR were to be adopted in Australia, it would provide doxing victims with the right to request erasure of personal information and to have the request promptly assessed and, if approved, actioned. It would also prevent doxing because companies would have to implement privacy by design and integrate safeguards into the processing of personal information. Concerns that regulating the processing of personal information in household activities could restrain freedom of speech or breach a person's right to privacy are valid, but they do not justify ignoring the problem of doxing. Doxing can

191 *General Data Protection Regulation* [2016] OJ L 119/1, 3–4.

192 Ibid 80, art 77(1).

193 Ibid 69–70, art 58.

194 Ibid 11.

195 Ibid.

196 Ibid 80, art 78–79.

197 Beata A Safari, 'Intangible Privacy Rights: How Europe's GDPR Will Set a Standard for Personal Data Protection' (2017) 47 *Seton Hall Law Review* 809.

have severe adverse effects on victims and it opens the possibility for 'digital vigilantism'. This article has demonstrated that the value of anonymity and obscurity is worth protecting and should be protected by law, and not regulated by individual online service providers who may have different views on what should be protected.

Concerns that a right to informational privacy would impose on the right to freedom of speech and information should not prevent the enactment of the right. The right to informational privacy needs to be balanced against the rights provided in the *Freedom of Information Act*. Defences to the right to informational privacy could include circumstances where the information is already public, which can be the case with doxing. Each circumstance will have to be considered in context, including the way that the personal information was obtained, retained and disclosed. Defences could also include circumstances where a right to freedom of information should be protected, and where it is an issue of national security.[198] The ALRC agrees with the *International Covenant on Civil and Political Rights* that there are competing interests, but 'both the individual and public interests in the protection of privacy and the individual and public interests in freedom of speech are important values and neither is absolute nor always in conflict with the other'.[199]

If the recommendations by the ALRC were to be implemented, doxing victims would not have a right of data erasure without having to take a matter to court. This article has argued that the preferred response to the doxing problem is to provide victims with the opportunity for timely removal of personal information, while also providing for the possibility of compensation for the victims and the imposition of fines on the doxer as a deterrent measure. The Australian Parliament should therefore consider enacting a statutory cause of action for a serious invasion of privacy that applies both to companies and to individuals acting in a personal capacity. The statute should provide individuals with the right to informational self-determination and access to a regulator with the power to enforce the new privacy laws, including the power to action requests for erasure of personal information, to impose fines and to order compensation. The Australian Parliament should extend the existing powers of the Privacy Commissioner, not only to investigate 'complaints about serious invasions of privacy more generally',[200] but also to enforce declarations and action requests for erasure

[198] *For Your Information Report*, above n 94, 104.

[199] *Serious Invasions of Privacy Report*, above n 23, 244 [12.128].

[200] Ibid 27 [1.54].

in a timely manner. Better data protection regulation may initially burden companies when they implement privacy by design, but it will also enhance trust in online services and ensure that individuals feel confident in providing their personal information online.