International Review of Law, Computers & Technology
Vol. 23, No. 3, November 2009, 169–177

Routledge
Taylor & Francis Group

The right of reputation in the Internet era[1]

Dan Jerker B. Svantesson*

Faculty of Law, Bond University, Gold Coast, Queensland 4229, Australia

Protecting one's reputation has arguably become harder in this time of *YouTube*, 'blogs' and mobile phone cameras. The simple truth is that it is easier to get 'caught' doing something inappropriate and it is easier for people to publish defamatory materials. This article is a somewhat eclectic selection of issues of particular significance to the right of reputation in our modern Internet-based society.

Keywords: reputation; defamation; Internet; law; IT law

Introduction

Protecting one's reputation has arguably become harder in this time of *YouTube*, 'blogs' and mobile phone cameras. The simple truth is that it is easier to get 'caught' doing something inappropriate and it is easier for people to publish defamatory materials. To paraphrase Winston Churchill's famous speech of 20 August 1940: *Never in the field of human interaction has so many been able to publish so much so easily.*

While, as hinted at above, several aspects of our modern society contribute to making it harder to protecting ones reputation, this article focuses on how the widespread use of the Internet has done so. Put differently, this article examines the right of reputation in the Internet context.

Having provided an overview of the sources of the right of reputation and the difference between reputation in the 'real world' and reputation online, it commences with a discussion of how technological developments have blurred the common law's traditional distinction between libel and slander. It then discusses the problems of identifying the publisher of defamatory materials on the Internet and the issues that arise when technology rather than people cause materials to become defamatory. Further, it addresses republication in the Internet context and the complex jurisdictional issues associated with cross-border Internet defamation cases.

As is clear from the outline of the scope of this article, it is by no means intended as an exhaustive examination of the right of reputation in the Internet era. Rather, it is a somewhat eclectic selection of issues of particular significance to the right of reputation in our modern Internet-based society. Further, while the discussion is not focused on the laws of any particular jurisdiction, most materials are drawn from the laws in place in Australia, the UK and the USA.

*Email: Dan_Svantesson@bond.edu.au

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600860903262230
http://www.informaworld.com

A right of reputation

The right of reputation is now firmly established on an international level. Most importantly, Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) states that: '1. No one shall be subjected to … unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'[2] This provision means that each state that has signed and ratified the ICCPR has an obligation to provide legal protection against unlawful attacks on honour and reputation of people subject to the State's jurisdiction and present within its territory, regardless of the origins of the defamatory material.[3]

Similarly, the European Convention on Human Rights provides that:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[4]

Furthermore, most, if not all, legal systems place emphasis on the protection of the right of reputation. Indeed, such a right is constitutionally protected in some states.

Just how serious the law views infringements of this right is illustrated when comparing the level of compensation awarded in two reasonably recent Australian cases. At first instance in *Ettingshausen* v. *Australian Consolidated Press* (1991) 23 NSWLR 443, the plaintiff was awarded Aus$350.000 to compensate for the humiliation of having his penis showing in a grainy picture published in a magazine (with the imputation that he had consented to the publication). In comparison, in a case where a young boy had the head of his penis cut off during a circumcision, the plaintiff was only awarded Aus$275.000 – i.e. Aus$75.000 less than what was awarded in the *Ettingshausen* case.[5]

Online reputation v offline reputation

The right of reputation has played a central role in society for a long time. However, the information society creates an even greater emphasis on reputation. For example, those trading online are clearly dependant on their reputation to a much greater degree than their offline counterparts – online you simply do not have the same possibilities of building trust through means such as location, shop structure, etc. Indeed, the reputational focus is nicely illustrated by, for example, eBay's system for grading traders. Put simply, buyers can rate the conduct of the sellers on eBay, and potential buyers can then use those ratings to assess the credibility/reliability of the various sellers.[6]

Furthermore, with a parallel world in the form of Cyberspace, our reputations are being diversified. A person living in a small village, say 50 years ago, would typically have one single reputation – that held in the village. Today, however, many people have a reputation in the town they live and a completely different reputation online. Indeed, many people have a range of reputations online. For example, in taking part in online discussion communities, a person can build up a reputation that is totally unrelated to that the same person enjoys in a file swapping community. Similarly, the participation in online games such as *Second Life*, will give a person a reputation unrelated to that person's offline reputation

and that person's other online reputations. As people often protect their 'real' identity online, e.g. through the use of pseudonyms, there is typically no connection between a person's various reputations.

Also other aspects of the online world make it possible to argue that the right of reputation has increased in importance with the introduction of the Internet. In a discussion of the different property rights that are associated with open source software, as opposed to traditional software licensing, it has been noted that in open source:

> Anyone can see the code, but not everyone can replicate the coder's influence on the community to which she contributes her code. By virtue of her contribution, she builds influence in her chosen code community, and this influence translates into a new kind of IP: reputation property instead of intellectual property. . . . In this new world of open source, reputation property means as much as or more than traditional intellectual property. . . . As an open source creator, then, my options for deriving profit from my creation are not more limited, but they are different. Instead of a limited monopoly guarded by law, I have a monopoly guarded by common sense: buyers want to buy from the most qualified source of support. They pay to have access to the source: not the source code, but the source of the code.[7]

These observations are relevant, novel and highly interesting. They make clear that current trends and developments ought to make us 'think outside the square' when approaching traditional legal concepts such as the concept of property, and suggests that we may be moving towards recognising a category of reputational property.

Libel or slander?

In addition to the forms of communication that are exclusive to the Internet, Internet technology can also provide, for example, television and radio broadcasts and telephony. The reason for this is found in the Internet's architecture:

> The technical protocols that form the foundation of the Internet are open and flexible, so that virtually any form of network can connect to and share data with other networks through the Internet. As a result, the services provided through the Internet (such as the World Wide Web) are decoupled from the underlying infrastructure to a much greater extent than with other media. Moreover, new services (such as Internet telephony) can be introduced without necessitating changes in transmission protocols, or in the thousands of routers spread throughout the network.[8]

The convergence of technologies has caused, and will continue to cause, problems of definition. For example, common law jurisdictions typically distinguish between different forms of defamation based on the form of communication used to convey the defamatory message. For example, a distinction is sometimes drawn between libel[9] and slander.[10] Under the traditional common law approach to defamation exercised, for example, in Hong Kong, this distinction is determinative in relation to the evidence of damage. In the case of slander, the plaintiff must ordinarily show special damages (i.e. the actual damage must be demonstrated), while that is not necessary in actions for libel. Case law has illustrated that, new technologies such as Internet communication cannot always be easily fitted into pre-existing categories.

For example, in the somewhat dated *Mickelberg* v. *6PR Southern Cross Radio Pty Ltd & Ors* [2002] WASCA 270, an Australian court had to decide whether a radio interview, that could be listened to on a website constituted libel or slander. Drawing upon *Wainer* v. *Rippon* [1980] VR 129, the Court took the approach that 'it is probable that, absent legislative intervention, the spoken words would amount to a slander, and not a libel'.[11] This

conclusion was motivated by the fact that 'only the sound, and not the text of the interview, was obtainable by means of the Internet'.[12] It is respectfully submitted that this conclusion, or at least the base for the conclusion, is flawed. There are two competing definitions of what constitute libel: permanency and the quality of visual comprehension. If focus is placed on whether or not the interview, in question, was visually comprehensible, the answer is obviously *no*, but it has been decided that radiobroadcasts are to be viewed as libel.[13] Thus, it would seem that contemporary focus is placed on permanency rather than visual comprehension. There can be no doubt that an audio file, available for downloading on a website, exists in a permanent form, rather than a transitory form and thereby must be viewed as libel rather than slander. It is somewhat more difficult to determine the status of online live (or 'once off') transmission or re-transmission of radio broadcasts. A great deal of effort has been spent on determining whether this form of communication fits into the category of broadcasting.[14] While important, it would seem inappropriate to limit the question in such a way. If it is concluded that online live (or 'once off') transmission or re-transmission of radio broadcasts do not fit into the category of broadcasting, we must still ask whether the considerations that lead to that radio broadcasts are viewed as libel also are present in relation to online live (or 'once off') transmission or re-transmission of radio broadcasts. If answered in the affirmative, it would only seem natural to conclude that also online live (or 'once off') transmission or re-transmission of radio broadcasts must be classed as libel rather than slander.

While the question of whether Internet radio may constitute libel or slander may be settled in large parts of the world by now, the question nevertheless illustrates how difficult it may be to fit novel technological solutions into existing legal definitions. It is likely that these difficulties will continue to stand in the way of an effective protection of reputation online.

Identifying the source

Where a victim becomes aware of defamatory content, the first step is to seek to identify the party responsible for the content. Where the party making the content available is not the originator of the content, special issues of re-publication arises. Those issues are discussed below. Here, I address some questions related to the identification off the source of the defamatory content.

Identifying the party responsible for defamatory content appearing online is not always easy. While the details of how information is made available vary depending on the application being used, typically the trace left by the culprit is an Internet Protocol (IP) address and possibly either an e-mail address or a domain name. Where a person has made a defamatory positing on her/his own website, identifying the responsible party is rather straight forward by looking up the registrations details of the website in question. However, only a very naïve offender would think she/he could make such a posting without the victim being able to find the guilty party.

The identification process can get more complicated where the defamatory content is spread via e-mail. No problems would typically arise where the culprit uses, for example, her/his workplace e-mail. If I send an e-mail from my Bond University e-mail address 'dasvante@bond.edu.au', identifying me as the sender is easily done. However, where the sender uses a third-party e-mail system with which she/he has no other connection, such as would the case if I register for, for example, a Hotmail account and only use it to send the defamatory message, it is not possible to identify the offender simply by looking at the e-mail address.

Further, where the defamatory content is placed, for example, as a posting on a public forum such as a wiki, the culprit may not leave any e-mail address and, of course, no domain name that can be used to identify her/him.

Where there is no other reliable information, one has to look to the IP address to identify the party responsible for defamatory content. An IP address of IPv4 (i.e. the Internet Protocol version currently most widely used) consists of a 32-bit number, usually expressed in four groups separated by dots. Being a unique number, it can be used to identify the particular computer used to make the defamatory content available. The last remaining hurdle is then to link a particular person to that computer at the time the content was distributed.

Where the identified computer belongs to a particular individual, it may be reasonable to presume that she/he is responsible. Similarly, where the computer in question is associated with a limited group of people, such as in a workplace environment, log-in details may reveal who used the computer at the relevant time. In contrast, where the computer that was used to distribute the defamatory material is found in a public space, such as a library or an Internet café, it may be very hard to identify the relevant user, unless the users have to register in some form, or if there are CCTV cameras in the relevant space where the computer is located.

Before looking at some legal issues associated with identifying the source of defamatory content, another technical complication must be addressed – it is possible to hide ones IP address. This can be done in at least two ways. First, one can hide one's IP address by using so-called anonymisers. Anonymisers are applications designed to allow web-users to visit websites anonymously. They act as an added layer – a buffer – between the web-surfer and the websites she/he visits. When a web-surfer uses an anonymiser, her/his IP address is only transmitted to the provider of the anonymiser. She/he is then assigned a new IP address by the anonymiser in relation to any websites she/he visits while applying the anonymiser. For example, the IP address of my work computer is 131.244.15.138. However, if I, for example, use an anonymiser called *The Cloak*,[15] websites I visit would get the impression that my IP address was 216.127.72.7.

In addition to anonymisers, the use of so-called proxy servers opens up further possibilities. A bit simplified, a proxy server is a server that sits between the web-browser and the server being accessed. Thus, just like the anonymisers discussed above, a proxy server acts as a buffer between the web-surfer and the websites visited. The main difference is that while the anonymisers are web-applications, the use of proxy servers are determined by the settings in the web-browser. Using a proxy server to hide one's IP address involves two easy steps. First it is necessary to obtain the address (with its port number) of the proxy server you wish to use. Then the browser settings must be changed to the obtained proxy address (with its port number). For example, users of Microsoft's Internet Explorer can change their proxy server setting by first clicking on *Internet Options* under *Tools*, and then clicking on *LAN Settings* under *Connections*.

Where the person who is responsible for the distribution of defamatory content has taken such steps to hide her/his IP address, the only way to identify the culprit is to seek help from the provider of the anonymiser or proxy-server. Proxy servers, and anonymiser, can log all information that passes through them. In other words, all the web-surfer's traffic can be accessed by the operator of the anonymiser or proxy server.

This takes us to the legal side of identifying the source. Where the identification is dependent on information held by a third-party, the question arises; under which circumstances can access be had to third-party information necessary for the identification of the culprit in a defamation action? The answer to this question is strongly dependent on the applicable law, and significant differences exist between the common law and civil

law systems. In common law countries one can often initiate proceedings without knowing the identity of the party one is taking action against.[16] In contrast, such an approach is typically not possible in civil law countries.[17]

Technology as the publisher

While it is acknowledged that technology does not act on its own (so far), and that whatever technology does can be seen as the programmed intention of the programmer, existing technological setups can lead to very interesting questions of liability. Imagine, for example, that you want to read a particular article that happens to be written in a language you do not speak. You can then use an automatic translation service such as *Yahoo!'s Babel Fish*.[18] What happens if, as a result of a translation error made by the automatic translation service, the article becomes defamatory about a third person? While the automatic translation service has done what it was programmed to do, it is questionable whether the programmer reasonably could be held liable. Further, it would seem inappropriate to place liability on the author where the original text is not defamatory. In such a situation we have defamatory content being published without a human being that suitably can be held as the publisher.

A similar scenario could arise in relation to services that collect and merge information from various sources.

Republication

The issue of republication arises where somebody, with or without endorsing the message, transmits a defamatory statement, made by somebody else, to a third person. The most typical example of republication would perhaps be where a newspaper publishes allegations made by a person against another person. In such a situation, the newspaper is not the source of the allegation, but it republishes it.

The republication issue is, as already illustrated, not unique to the Internet context. However, when placed in the Internet context particular complications arise and several Internet-related cases have focused on republication.

One of the early cases of this type is the UK case of *Godfrey* v. *Demon Internet*.[19] There, the provider of an electronic bulletin board, Demon Internet, argued that it 'were not at common-law the publishers of the Internet posting defamatory of the Plaintiff'.[20] The court did not agree:

> In my judgment the Defendants, whenever they transmit and whenever there is transmitted from the storage of their news server a defamatory posting, publish that posting to any subscriber to their ISP who accesses the newsgroup containing that posting.[21]

More recently, an action was taken in France against the Wikimedia Foundation (the organisation operating Wikipedia). The action was based on suggestions posted on Wikipedia that the plaintiffs were homosexuals. In the end, however, the Court ruled in Wikimedia's favour.

While the above merely represents a small sample of the cases that have dealt with the republications issue in the Internet context, it clearly highlights the potential dangers of making available third-party content on the Internet. If we consider that one of the Internet's most fundamental advantages is its ability to make possible the sharing, and linking, of information, the conflict is obvious.

Jurisdictional issues

The Internet is a near global communications medium. Consequently, once material is available online, it can typically be accessed virtually all over the world. This means that material uploaded in one country, for example, can be read in another country, affecting somebody's reputation in a third country. Where such a situation results in litigation, the litigants are faced with the questions of which courts will accept to exercise jurisdiction, which country's laws will be applied and where can a favourable judgment be recognised and enforced?

When discussing theses jurisdictional issues, it must be remembered that Internet publishing is fundamentally different to traditional publishing. The publisher of a newspaper, for example, would ordinarily be publishing within a local area, or a country or, if very large, a region. The technology of newspaper publications is such that a newspaper will only be available at those places the publisher has targeted. It could be said that the starting point is 0% publication-coverage, and for that number to increase the publisher must target a community, country or region with its newspaper. Web publication, works in exactly the opposite way. Once the material is made available on the web, it has virtually 100% publication-coverage, and for that percentage to decrease, the publisher must take action by 'dis-targeting' undesirable forums.

This fundamental difference has lead courts and commentators to reach troubling conclusions. For example, in the majority judgment of the High Court of Australia decision in *Dow Jones & Company Inc* v. *Gutnick*,[22] it is noted that.

> However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so knowing of the reach that their information may have. In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction.[23]

Similarly, Goldsmith states that:

> A manufacturer that pollutes in one state is not immune from the antipollution laws of other states where the pollution causes harm just because it cannot predict which way the wind blows. Similarly, a cyberspace content provider cannot necessarily claim ignorance about the geographical flow of information as a defense to the application of the law of the place where the information appears.[24]

This line of reasoning is clearly too simplistic. What the Court and Goldsmith are saying is undeniably true, but their observations represent an antiquated view of Internet use, and seem to completely overlook the widespread use of the Internet for domestic, or even local, spread of information. In today's society a website is not only, or indeed always, aimed at attracting distant attention. People rely on the Internet in searching for local information (e.g. searching for a local restaurant or finding out the opening hours of a local library), and websites are often aimed at a local market. Thus, even if people know that everything they put on the 'net' *can* be accessed from virtually anywhere in the world, that does not necessarily mean that they *intended* to publish in every jurisdiction on the planet, or indeed, that publication all over the world was a *natural and probable consequence*.[25]

In other words, focusing on the potential reach of Internet publications does not bring us close to finding a suitable balance between freedom of speech and the right of reputation. However, nor should we focus blindly on the publishers' intentions. The dangers of doing so are well illustrated in the US case of *Young* v. *New Haven Advocate*.[26] There, two

newspapers based outside Virginia published articles in part discussing the conduct of residents of Virginia in Virginia.[27] The articles were available both offline and online. Despite this, the US Court of Appeals for the Fourth Circuit concluded that:

> The newspapers did not post materials on the Internet *with the manifest intent of targeting* Virginia readers. Accordingly, the newspapers could not have 'reasonably anticipated being haled into court [in Virginia] to answer for the truth of the statements made in their articles'. *Calder, 465 U.S. at 790* (quotation omitted). In sum, the newspapers do not have sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them.[28] (emphasis added)

This approach is problematic as it might leave a plaintiff with no forum in which to defend her/his reputation.

The enormous difficulties associated with finding the right balance between overly wide jurisdictional claims, and too strict requirements being imposed on a plaintiff seeking to take action to protect her/his reputation, are clear when looking at efforts made in relation to international agreements.

In 1992, work on a new and ambitious convention was initiated at the *Hague Conference on Private International Law*. The previously proposed Convention, which was an initiative of the US Government,[29] was titled the *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters* and was to address jurisdiction and recognition and enforcement in relation to a wide range of areas of law. Article 10 of the previously proposed Convention was to deal with torts, including the tort of defamation. However, the extensive work on the Convention made clear that no consensus was likely in relation to that issue.

Somewhat similarly, while the Member States of the European Union have managed to reach consensus as to how the applicable law should be identified in a wide range of property related disputes,[30] they have so far failed to reach consensus in relation to defamation and privacy matters.[31]

Concluding remarks

The above has highlighted that protecting one's right of reputation in relation to online publications is associated with great practical difficulties. It has also alluded to the fact that, balancing the legitimate interests of Internet publishers with the legitimate interests of individuals seeking to protect their reputations, is a highly complex task.

This article has also sought to highlight that the right to reputation faces particular difficulties in the online environment. Some of those problems, such as the issue of republication, are versions of the problems faced in the 'real world'. Others, such as technology as the publisher, are unique to the online environment.

If I was to try to reach a conclusion that incorporates speculations as to the future, I would suggest that the right of reputation has never been more important than it is in our information driven society and its importance is likely to continue to increase. Further, it has never been more difficult to protect one's reputation than it is today and doing so is not likely to get any easier.

Notes

1. In part, this article draws upon Dan Svantesson, *Private International Law and the Internet*, The Haague: Kluwer Law International (2007).

2. ICCPR, Article 17(1–2).
3. Svantesson, *Private International Law*, 249–51.
4. *The European Convention on Human Rights* (Rome, 4 November 1950), Art. 8.
5. Paul Reidy, 'The Correct Approach to Defamation Damages', *Communications Law Bulletin*, 13, no. 2 (http://www.camla.org.au/clb/CLB%20-%20Volume%2013,%20Issue%202.pdf).
6. See http://pages.ebay.com/help/tp/know-seller-ov.html (accessed September 18, 2009).
7. Danese Cooper *et al.*, *Open Source 2.0* (O'Reilly, 2005). Available at http://safari.oreilly.com/0596008023/opensources2-CHP-7-SECT-3 (accessed April 1, 2008).
8. K. Webach, 'Digital Tornado: The Internet and Telecommunications Policy' (working paper of the Federal Communications Commission, Washington DC, 1997), p. 2.
9. Defined either as defamation in permanent form, or as defamation expressed in a mode of communication capable of being comprehended visually (see P. Nygh and P. Butt, *Butterworths Concise Australian Legal Dictionary*, 2nd ed (Sydney: Butterworths, 1998)).
10. Defined as: 'a non-permanent defamatory statement expressed in spoken words or some other transitory form such as gestures or non-verbal sounds such as hissing' (Nygh and Butt, *Butterworths Concise Australian*).
11. *Mickelberg* v. *6PR Southern Cross Radio Pty Ltd & Ors* [2002] WASCA 270, para 44.
12. *Mickelberg* v. *6PR*, para 44.
13. See, e.g. the Australian *Broadcasting Services Act 1992 (Cth.)* s. 206 and Hong Kong *Defamation* Ordinance, s. 22.
14. See e.g. Raani Costelloe, 'Internet Television and Radio Services – The Streaming Controversy', *Communications Law Bulletin* 19 (2000): 9.
15. http://www.the-cloak.com/login.html, 5 February 2007.
16. For an interesting discussion of this issue, from a US perspective, see David L. Sobel, 'The Process that 'Joe Doe' is Due: Addressing the Legal Challenge to Internet Anonymity', *Virginia Journal of Law and Technology* 5 (2000): 3.
17. Alzbeta Krausova, 'Identificatiion in Cyberspace', Paper presented at Cyberspace 2007 'Normative Framework', December 2007, Brno, Czech Rep.
18. http://babelfish.yahoo.com/
19. [1999] EWHC QB 244 (26 March, 1999).
20. Ibid., para 2.
21. Ibid., para 33.
22. *Dow Jones & Company Inc* v. *Gutnick* (2002) 210 CLR 575.
23. *Dow Jones & Company Inc* v. *Gutnick* (2002) 210 CLR 575, 605.
24. J.L. Goldsmith, 'Against Cyberanarchy', *University of Chicago Law Review* 65 (1998): 1244.
25. A very similar, but more limited, reasoning can be found in: *Young* v. *New Haven Advocate* 315 F 3d 256 No. 01-2340 (13 December 2002), 6. It is interesting to note that not even the plaintiff in that case presented as wide claims, in this regard, as the majority judgment of the High Court did in the *Gutnick* case (see: *Young* v. *New Haven Advocate* 315 F 3d 256 No 01-2340 (13 December 2002), 5).
26. 315 F 3d 256 No 01-2340 (13 December 2002).
27. Maximum-security prisons in Connecticut were overcrowded and, as a consequence, Connecticut had contracted with Virginia to house a number of Connecticut prisoners. The articles, in question, discussed the state of a penal institution in Virginia as well as the conduct of its warden.
28. *Young* v *New Haven Advocate* 315 F 3d 256 No 01-2340 (13 December 2002), 7. The targeting approach has also been strongly advocated in a recent literature. See, e.g. G.J. Wrenn, 'Cyberspace is Real, National Borders are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace', *Stanford Journal of International Law* 38 (2002): 97.
29. M. Davies, 'Time to Change the Federal Forum Non Conveniens Analysis', *Tulane Law Review* 77, no. 2 (2002): 381.
30. See the *Rome Convention* (593/2008/EC)
31. See the *Rome II Regulation* (864/2007/EC).