

DEFAMATION LAW

PAPER 3.1

The Modern-Day Soapbox: Defamation in the Age of the Internet

These materials were prepared by Bryan G. Baynham, QC and Daniel J. Reid, both of Harper Grey LLP, Vancouver, BC, for the Continuing Legal Education Society of British Columbia, September 2010.

© Bryan G. Baynham, QC and Daniel J. Reid

THE MODERN-DAY SOAPBOX: DEFAMATION IN THE AGE OF THE INTERNET

I.	Introduction: The Taming of the Wild West	1
II.	Publication	2
III.	Limitation Periods—The Permanence of the Internet	4
IV.	Hyperlinks	5
V.	The Role of the Internet Service Provider	6
VI.	The Illusion of Online Anonymity	7
	A. The Evidentiary Trail	8
VII.	Obtaining Disclosure	9
	A. The Supreme Court Civil Rules.....	10
	B. Norwich Pharmacal Order/Equitable Bill of Discovery	11
VIII.	Balancing Privacy and Disclosure	13
IX.	Conclusion	15
X.	Model Disclosure Order	16

I. Introduction: The Taming of the Wild West

“In the early to mid 1990s it was fashionable to compare the unformed, open spaces of the internet to the 19th century American West: the ‘electronic frontier’.”¹

If the Internet was once the Wild West, it is now a bustling metropolis. What was once the domain of a few early adopters has become a part of everyday life. Most people have at least one email address, and many have Facebook pages, blogs, or Twitter accounts. Since being launched in February of 2004, Facebook (the most popular social networking site) has grown to over 500 million active users. If Facebook was a nation, it would be the world’s third most populous.²

The rapid expansion of the Internet coupled with the surging popularity of social networking services like Facebook and Twitter has created a situation where everyone is a potential publisher, including those unfamiliar with defamation law. A reputation can be destroyed in the click of a mouse, an anonymous email or an ill-timed Tweet.

The law of defamation, driven by judge made common law, has evolved over centuries. While people are exceptionally adept at discovering new ways to defame one another, the common law has proven surprisingly adaptive to the electronic frontier. The Supreme Court of Canada has signalled it is alert

1 <http://www.zdnet.co.uk/blogs/zdnet-uk-book-reviews-10015295/book-review-wild-west-20-10017873/>

2 http://www.economist.com/node/16660401?story_id=16660401&fsrc=rss

to changing technologies: in the recent case of *Grant v. Torstar*,³ the Court extended the “responsible communication on matters of public interest” defence to defamation not just to journalists, but to bloggers and online posters. As will be discussed in this paper, Canadian courts are able to grant effective relief to the defamed in many instances.

This paper explores defamation in the age of the Internet. As it would not be possible to cover all aspects of online defamation in one paper, we have limited our focus to the elements of online defamation, issues of anonymity, and privacy concerns. This paper begins with an overview of some of the fundamentals of online defamation, including the location where publication occurs, the status of “hyperlinks” and the role of internet service providers (“ISPs”). It then examines issues of anonymity and disclosure that often accompany online defamation cases. The paper then turns to two cases out of Ontario that balance privacy rights against disclosure, and concludes with a model procedure and order for obtaining the identity of an anonymous defendant in an online defamation case.

II. Publication

The Internet represents a communications revolution. It makes instantaneous global communication available cheaply to anyone with a computer and an Internet connection ... *the Internet is also potentially a medium of virtually limitless international defamation.*⁴

In the 2004, in the case of *Barrick Gold Corporation v. Lopehandia*,⁵ the Ontario Court of Appeal held that there was something fundamentally distinct about Internet defamation compared to defamatory statements published in other mediums. The Court found that communication via the Internet is characterized by its immediate worldwide ubiquity and accessibility, and for these reasons there is a greater risk online defamatory remarks will be both widely disseminated and easily believed. Online, “the truth rarely catches up with the lie.”⁶

The ubiquity and accessibility of online defamation poses another problem—often the road between publication and consumption passes through many jurisdictions. A disgruntled investor in Brazil may post nasty comments about a TSX-listed company on a BC stock forum, which is then read by prospective investors in New York. Where should the company commence the action? Where the posting originated, in the jurisdiction it is read, or in the jurisdiction where the damage occurs? A further consideration is whether a judgment obtained in one jurisdiction can be enforced in another—on August 10, 2010, American President Barack Obama signed the *Speech Act*, which shields American journalists, publishers (both print and online) and bloggers from foreign lawsuits.⁷ This law requires American courts not to recognize or enforce foreign libel tort judgments that conflict with the First Amendment, and may make it difficult to enforce Canadian defamation judgments in the US.

In determining whether a defamation action can be brought in Canadian jurisdictions, Canadian courts have applied the common law tests of *jurisdiction simpliciter* and *forum non conveniens* (in BC, these common law tests are codified in the *Court Jurisdiction and Proceedings Transfer Act*).⁸ Although the

3 *Grant v. Torstar Corp.*, 2009 SCC 61.

4 *Barrick Gold Corporation v. Lopehandia*, 2004 CanLII 12938 (Ont. C.A.), (2005) 71 O.R. (3d) 416 (C.A.).

5 *Ibid.*

6 *Ibid.* at paras. 28-34.

7 H.R. 2765: *Securing the Protection of our Enduring and Established Constitutional Heritage Act*. Full text of the Act can be found at <http://www.govtrack.us/congress/billtext.xpd?bill=h111-2765>

8 *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003 c.28.

degree of connection can vary from case to case, it is clear that something more than accessibility is required for a Canadian court to assume jurisdiction. Although online defamatory statements may be available in Canada, it may not always be possible to sue in Canada.

By way of example, in *Bangoura v. Washington Post*,⁹ a Kenyan United Nations worker sued the *Washington Post* in Ontario for an article alleging that his UN colleagues had accused him of sexual harassment, financial improprieties and nepotism that allegedly occurred while he had been posted in the Ivory Coast. At the time he commenced his lawsuit, the plaintiff was an Ontario resident. In terms of publication in Ontario, there was evidence that at least seven Ontario residents had a subscription to the *Washington Post*. With respect to online availability, the article had been freely available globally for a period of fourteen days, and subsequently available for a fee on the pay-to-view *Washington Post* online archives.

While noting that “articles published on the Internet may proliferate well beyond their original target audiences into other jurisdictions”¹⁰ the Court held that there was no evidence that the article “reached significantly” into Ontario. Indeed, it appeared from records provided by the *Washington Post* that the only person who had accessed the pay-to-view online articles was the plaintiff’s lawyer. Accordingly, the Ontario Court of Appeal held that there was not a “real and substantial” connection between the online articles and Ontario, and it would therefore be improper for Ontario to assume jurisdiction.

Conversely, in *Burke v. NYP Holdings, Inc.*,¹¹ Mr. Justice Burnyeat allowed former Vancouver Canucks General Manager Brian Burke to proceed with his lawsuit against the *New York Post* in BC. In this case, the *Post* published an article alleging that Burke “personally challenged” the Canucks to target Colorado Avalanche player Steve Moore during an NHL game in 2004. The *New York Post* did not deliver to BC, however, the Court had before it affidavit evidence that the online version of the article had been accessed in the province, and had been mentioned on a Vancouver call-in radio sports program. The newspaper brought an application to strike the claim on the grounds that BC did not have jurisdiction or ought to decline jurisdiction over the defendants in relation to the claims made.

In dismissing the application, Mr. Justice Burnyeat found there was a sufficient connection between BC and the alleged defamation for the lawsuit to proceed:

While the Defendants have little or no business connection in British Columbia, it is clear that the *Post* is a major newspaper in what many describe as the financial capital of the United States which, in turn, is described by many as the most powerful country in the world. By establishing a website which is available on the Internet worldwide, it is reasonably foreseeable that the story set out in the Column would follow Mr. Burke to where he resided. The concept of a “worldwide web” is aptly named.¹²

More recently, in *Black v. Breeden*,¹³ the Ontario Court of Appeal confirmed that Ontario had jurisdiction and was an appropriate forum to hear Conrad Black’s six libel actions in respect of statements posted on the Hollinger International, Inc. website. The statements had been picked up and republished in Ontario by a number of Canadian newspapers.

9 *Bangoura v. Washington Post*, 2005 CanLII 32906 (Ont. C.A.), leave to appeal to the Supreme Court of Canada refused.

10 *Ibid.* at para. 34.

11 *Burke v. NYP Holdings, Inc.*, 2005 BCSC 1287.

12 *Ibid.* at para. 33.

13 *Black v. Breeden*, 2010 ONCA 547.

In finding that the alleged tort occurred in Ontario, the Court pointed to evidence that defendants did target and direct their statements to this jurisdiction, including the fact that the press releases posted on the Internet specifically provide contact information for Canadian media, as well as US and UK media: “the contact information for Canadian media clearly anticipated that the statements would be read by a Canadian audience and invited Canadian media to respond.”¹⁴

The Ontario Court of Appeal also noted that, while not a resident of the province, Black had significant connections to the province and a reputation in the province. Accordingly, Black’s reputation in the province had been damaged,¹⁵ and the lawsuit was allowed to proceed.

While online publications may be available globally, in order for Canadian courts to assume jurisdiction there must be something more than mere availability. Factors including whether the publication was read in the province, whether the plaintiff had a reputation in the province, and whether the plaintiff’s reputation was damaged in the province will be considered by the court in assuming or declining jurisdiction.

III. Limitation Periods—The Permanence of the Internet

A troublesome issue that arises in online defamation cases is when, if ever, the limitation period begins to run on statements that remain accessible online. Some jurisdictions, namely a number of American states, have adopted a “single publication rule,” under which the limitation period begins to run once a statement is first posted published (including being posted online), and that subsequent sales or deliveries do not constitute a fresh cause of action.¹⁶ Other jurisdictions, including the UK,¹⁷ and Australia¹⁸ have rejected the “single publication rule,” holding instead that each subsequent publication represents a fresh cause of action.

In *Carter v. B.C. Federation of Foster Parents Assn.*,¹⁹ the BC Court of Appeal wrestled with this issue, and came down in favour of the approach adopted in most Commonwealth jurisdictions: an online publication remains actionable so long as it is published.

In this case, the plaintiff became aware of allegedly defamatory postings about her on an online forum in 2000, but did not commence an action against one of the defendants until more than two years had passed. The trial judge adopted the “single publication rule” and dismissed the action as being limitation barred.²⁰

In reversing this decision, the Court of Appeal held that each publication gave rise to a distinct cause of action:

If defamatory comments are available in cyberspace to harm the reputation of an individual, it seems appropriate that the individual ought to have a remedy. In the instant case, the offending comment remained available on the internet because the defendant respondent did not take effective steps to have the offensive material removed in a timely way. Although, for the reasons noted by the trial judge,

14 *Ibid.* at para. 39.

15 *Ibid.* at para. 49.

16 See, for example, *Ogden v Association of the United States Army* (1959), 177 F Supp 498, 502.

17 See, for example, *Loutchansky v. Times Newspapers Ltd.*, [2002] Q.B. 783 (C.A.).

18 *Dow Jones & Company Inc. v. Gutnick*, [2002] HCA 56.

19 *Carter v. B.C. Federation of Foster Parents Assn.*, 2005 BCCA 398.

20 As summarized by the Court of Appeal in *Carter v. B.C. Federation of Foster Parents Assn.*, 2005 BCCA 398 at para. 14.

legislatures may have to come to grips with publication issues thrown up by the new development of widespread internet publication, to date the issue has not been legislatively addressed and in default of that, I do not consider that it would be appropriate for this Court to adopt the American rule over the rule that seems to be generally accepted throughout the Commonwealth; namely, that each publication of a libel gives a fresh cause of action.²¹

Recently, the English Court of Appeal went further, holding that the “responsible journalism in the public interest” defence to defamation (the UK equivalent of Canada’s “communication on matters of public interest” defence) requires that an online archive of a story must be updated to take account of exculpatory developments.

In *Flood v. Times Newspapers Ltd.*,²² a police officer was accused, in a newspaper article, of taking bribes from Russian exiles with criminal connections. The article was printed in the paper edition of the *Sunday Times*, and was also made available in its entirety online. Approximately a year after the article was first published, a report cleared the police officer of any wrongdoing. In rejecting the “responsible journalism” defence, one of the concurring judges the English Court of Appeal noted that the online article was not changed to reflect the findings of the report:

If the original publication of the allegations made against DS Flood in the article on the website had been, as the Judge thought, responsible journalism, once the Report’s conclusions were available, any responsible journalist would appreciate that those allegations required speedy withdrawal or modification. Despite this, nothing was done.²³

In Canada, the “communication on matters of public interest defence” to defamation is applicable to bloggers and other online publishers. This case raises the question—do bloggers and other online media outlets have an ongoing obligation to update their stories to reflect changing facts?

Logic dictates that this new defence be applied consistently, irrespective of whether the defendant is a seasoned reporter at a national newspaper or a “citizen journalist” who publishes his or her own blog.

IV. Hyperlinks

Are online publishers liable for the content of their “hyperlinks”? Is merely linking to defamatory content actionable? Later this year the Supreme Court of Canada will hear an appeal from the BC Court of Appeal that will likely decide this very issue.

In the case of *Crookes v. Newton*,²⁴ a website provided links to a number of articles which Mr. Crookes alleged were defamatory of him. Mr. Crookes plead that, by creating these hyperlinks, or, by refusing to remove the hyperlinks when advised of their defamatory character, the website publisher became a publisher of the impugned articles found at the hyperlinked websites.

In dismissing his appeal 2-1, the majority of the BC Court of Appeal held that merely linking to a website, without comment or invitation, did not constitute publication:

Whether the hyperlink is a web address, as is often the case, or a more specific reference, both require a decision on the part of the reader to access another website, and both require the reader to take a distinct action, in the one case typing in a web

21 *Ibid.* at para. 20.

22 *Flood v. Times Newspapers Ltd.*, [2010] EWCA Civ 804.

23 *Ibid.* at para. 78.

24 *Crookes v. Newton*, 2009 BCCA 392, leave to appeal granted, 2010 CanLII 15601 (S.C.C.).

address and in the other case clicking on the hyperlink. In other words, there is a barrier between the accessed article and the hyperlinked site that must be bridged, not by the publisher, but by the reader. The essence of following a hyperlink is to leave the website one was at to enter a different and independent website.²⁵

The majority cautioned that, while linking to an external website will not generally constitute publication, “the circumstances of a case may add more so as to demonstrate that a particular hyperlink is an invitation or encouragement to view the impugned site, or adoption of all or a portion of its contents.”²⁶ Although all three judges agreed that the context of hyperlinks matters, the Court of Appeal split on the issue of whether, in the context of the website, the particular hyperlink at issue amounted to publication. In her dissenting reasons, Madam Justice Prowse found the article which linked to the impugned publication amounted to an “invitation” to click on the hyperlink and therefore constituted publication,²⁷ whereas the majority held that the article did not offer such encouragement.²⁸

Although the Supreme Court of Canada may decide otherwise, it is likely that context of the link matters will be upheld. Lower courts in Canada and England have held that merely referencing a website or linking to its content does not constitute an actionable publication.²⁹

V. The Role of the Internet Service Provider

One area of online defamation Canadian courts have yet to fully explore is whether Internet Service Providers (“ISPs”) such as Bell Canada, Shaw Communications Inc., Rogers Communications Inc., and Telus Inc. can be held liable for hosting defamatory content. Unlike the UK and the US, Canada has not established a statutory or common law defence of “innocent dissemination,” whereby ISPs are not liable for hosting defamatory content authored by a third party.

In the UK, one of the earliest cases dealing with online defamation dealt with the issue of whether the host of an online bulletin board could make use of the “innocent dissemination” defence codified in s. 1 of the *Defamation Act 1996*. In *Godfrey v. Demon Internet Limited*,³⁰ the English Court of Queen’s Bench found the host of a bulletin board service liable for failing to remove defamatory postings once they were made aware of the content. While the host of the bulletin board could have made use of the defence had they been unaware of the content, by failing to act promptly once requested to do so by the plaintiff the host lost the innocence required to rely on the “innocent dissemination” defence. In effect, the Court imposed a “notice-and-takedown” requirement on ISPs, and UK ISPs now routinely remove defamatory content once they receive notice of it.

In the US, the protection afforded ISPs is even broader. Section 230 of the *Communications Decency Act*³¹ provides statutory immunity for online services, including blogs, forums and ISPs, who publish defamatory content, so long as that content is authored by a third party. This immunity applies even if the ISP receives notice of the defamatory material.

25 *Ibid.* at para. 82.

26 *Ibid.* at para. 84.

27 *Ibid.* at para. 71.

28 *Ibid.* at para. 89.

29 See, for example, *Carter v. B.C. Federation of Foster Parents Assn.*, 2005 BCCA 398, *Sauvé v. Canada*, 2010 FC 734, and *Islam Expo Ltd v. The Spectator*, [2010] EWHC 2011 (Q.B.).

30 *Godfrey v. Demon Internet Limited*, [1999] EWHC QB 244.

31 Section 230 of the *Communications Decency Act of 1996* (a common name for Title V of the Telecommunications Act of 1996).

Although there are no cases directly on point, it is likely that Canada would follow England's lead in providing a limited defence of "innocent dissemination," provided that the ISP or host removes the offending material on demand.

In the Supreme Court of Canada case of *Society of Composers, Authors and Music Publishers of Canada ("SOCAN") v. Canadian Assn. of Internet Providers*,³² SOCAN sought to impose liability for royalties on various ISPs for copyrighted music downloaded in Canada. The Supreme Court of Canada held in an 8-1 majority that, so long as ISPs acted as a "neutral-conduit" for information, they enjoyed the statutory protection of s. 2.4(1)(b) to the *Copyright Act*,³³ which provides that persons who only supply "the means of telecommunication necessary for another person to so communicate" are not themselves to be considered parties to an infringing communication.

Writing for the majority, the Hon. Mr. Justice Binnie cited *Godfrey v. Demon Internet*, and stated the following:

I agree that notice of infringing content, and a failure to respond by "taking it down" may in some circumstances lead to a finding of "authorization." However, that is not the issue before us. Much would depend on the specific circumstances. An overly quick inference of "authorization" would put the Internet Service Provider in the difficult position of judging whether the copyright objection is well founded, and to choose between contesting a copyright action or potentially breaching its contract with the content provider. A more effective remedy to address this potential issue would be the enactment by Parliament of a statutory "notice and take down" procedure as has been done in the European Community and the United States.³⁴

Although the law is not fully developed, there is a strong foundation for the defence of "innocent dissemination" of defamatory material in Canada, and it is therefore unlikely that ISPs would be found liable for third-party content unknowingly made available through their services.

VI. The Illusion of Online Anonymity

The internet is the most revolutionary communications tool since the printing press. It is extraordinarily accessible and powerful. It is available to anyone who has a computer and an account with a service provider. The user has the ability to roam the internet with anonymity to read and write just about anything he or she chooses. As is always the case, however, technological advancement breeds new legal questions. Can the Internet be used with impunity to spray libelous electronic graffiti in cyberspace? How absolute is the user's anonymity? Will the court compel the internet provider to disclose a customer's name?³⁵

In January of 2009, a Canadian-born fashion model brought a proceeding in the Supreme Court of New York State to seeking to compel Google to disclose the identity of the author who had started a Google-hosted website describing her in disparaging and allegedly defamatory terms.³⁶

The "Anonymous Blogger," as she was referred to in the action, was notified by Google of the proceedings and filed a brief in opposition to the application. In her brief, the Anonymous Blogger (through counsel) argued that the Internet has "evolved as the modern day soapbox for one's personal

32 *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45.

33 *Copyright Act*, R.S.C. 1985, c. C-42.

34 *Supra*, note 32.

35 *York University v. Bell Canada Enterprises*, 2009 CanLII 46447 (ON S.C.), at para. 1.

36 *Cohen v. Google Inc.* (N.Y.S.C. Index No. 100012/09, August 17, 2009).

opinion” and that “blogs have become a phenomenon, providing an excessively popular medium not only for conveying ideas, but also for mere venting purposes, affording the less outspoken a protected forum for voicing gripes, levelling invectives, and ranting about anything at all.”³⁷

In granting the application for disclosure, Judge Madden cited a Virginia case which noted that the anonymous nature of the internet must be measured against the protection of reputation:

In that the Internet provides a virtually unlimited, inexpensive, and almost immediate means of communication with tens, if not hundreds, of millions of people, the dangers of its misuse cannot be ignored. The protection of the right to communicate anonymously must be balanced against the need to assure that those persons who choose to abuse the opportunities presented by this medium can be made to answer for such transgressions.³⁸

As will be discussed further below, Canadian courts have likewise recognized that the cloak of anonymity must be stripped from those who use the internet to sully reputations.

A. The Evidentiary Trail

Many Internet users have online aliases or code name they use to protect their identities. At times, this anonymity may lead some to believe that they can write whatever they wish without fear of repercussions. However, in most cases it is possible to obtain evidence about the author of online defamation.

Every publication on the Internet, be it a posting to a bulletin board, blog, email message, or Facebook posting leaves behind an evidentiary trail that can be used to track the identity of the publisher.

The easiest way to obtain the identity of an anonymous online publisher is through the tracking of an IP address. An IP address is a numerical label that is assigned to devices that access the internet, and contains information about the routes by which information travels across the Internet. Every device that accesses the Internet, be it a computer, server or router, has a unique IP address, and this IP address can often be followed back to the original author.

By way of example, an email sent from Computer A will typically carry with it the IP information of Computer A. This email might be routed through Email Server B, on to Router C before arriving at Computer D. Each device on this route will have its own IP address. Depending on the nature of the online services involved, some or all of the IP addresses of the devices may be visible as part of the email delivered to Computer D. A perhaps overly-simple analogy can be drawn to a telephone number—Computer D will be able to see that it was called by Router C, which will know that it was called by Email Server B, which will keep a record of the original call from Computer A. Similarly, each server hosting a website will have its own unique IP address. Many websites also keep track of the IP addresses of those computers that access it, or of those users that post content to their site.

A detailed overview of the process for obtaining IP addresses is beyond the purview of this paper,³⁹ however one or more IP addresses (for some or all of the various devices along the route) will typically accompany an email message. In the event the online defamation is in the form of a posting to a website, the website administrator will usually have a record of the IP address or email from which the

37 *Cohen v. Google Inc.* (N.Y.S.C. Index No. 100012/09, August 17, 2009), Doe Memorandum on Law in Opposition to Application for Pre-Action Disclosure, page 10.

38 *re Subpoena Duces Tecum to America Online Inc.*, 2000 WL 1210372 (Va. Cir. Ct.), rev'd on other grounds, 261 Va. 350, 542 S.E. 2d 377 (Va. Sup. Ct. 2001).

39 For an excellent overview of electronic evidence, see Crerar, David and Purita, Ryan. *No Hiding Place in Cyberspace: Electronic Discovery from Non-Parties* (The Advocate Vol. 64, Part 6, November 2006 at 781).

publication originated, and the IP address can be obtained (usually by way of court order, the processes for which are outlined below). Finally, if the entire website itself is defamatory, there are a number of free online tools that provide the IP address of the individual or company hosting the website.

Armed with an IP address, it is then possible to look up the device or company that assigned the IP address.⁴⁰ The IP address will usually point to a company that provides internet access or email services, such as Shaw, Telus, Microsoft or Google, however the IP address alone will not typically reveal the identity of the online author.

These companies usually will have additional identifying information about the author, either in the form of a further IP address pointing to an ISP (in the case of email providers) or the identity of the ISP account holder. As will be discussed in the next section, there are tools available in both the Supreme Court Civil Rules and at common law that can be used to compel websites, ISPs and email providers to disclose the identifying information in their possession.

A note of caution: it is relatively easy for an individual to mask or disguise their IP address—there are numerous free online “IP masking” services that provide false IP addresses and make it exceedingly difficult to track down the true identity of an online author. However, while such services are readily available, in practical terms they are rarely used by the authors of online defamation. Due to the personal and often emotional nature of attacks on reputation, defamatory postings or emails are typically spur of the moment in nature, and more often than not the author will not take these additional steps to mask their online identity.

A greater concern lies with the proliferation of public wireless internet (“Wi-Fi”) networks, from which anyone can access the internet anonymously and freely. The concern with these public Wi-Fi networks, which can increasingly be found in coffee shops, libraries and restaurants, is that even if one were to obtain the identifying information of the source of the online publication, it may only lead back so far as the place where the author accessed the Internet.

A potential ray of hope lies in the emergence of the cellular networks as a means of accessing the Internet. Increasingly, people are relying on cell phones, laptops with built in “3G” cellular wireless and devices such as Apples iPad to write emails, post on Facebook and update their blogs. Due to the way these devices access the Internet through the wireless carrier’s data services, it is more difficult for a user to hide their online identity.

VII. Obtaining Disclosure

Before turning to the courts to compel disclosure of identifying information of online publishers, as a first step one should always write to the ISP, website or email provider requesting that they disclose the identifying information. For ease of reference, this section will refer to obtaining disclosure from ISPs, although the same principles apply to email service providers and websites.

Provincial and/or federal privacy legislation generally precludes ISPs from releasing the requested information without consent or court order. In BC, s. 18 of the *Personal Information Protection Act*⁴¹ (“PIPA”) reads as follows:

18(1) An organization may only disclose personal information about an individual without the consent of the individual, if:

...

⁴⁰ *Ibid*, at 785.

⁴¹ *Personal Information Protection Act*, S.B.C. 2003 c.63.

- (i) the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information.

Similar wording is found in s. 7(3)(c) of the federal *Personal Information Protection and Electronic Documents Act*⁴² (“PIPEDA”).

Although the ISPs will not disclose the requested information without a court order, asking the ISP is a necessary step toward obtaining the sought-after court order. The courts will be exceedingly reluctant to grant a disclosure order without other avenues of potential disclosure being exhausted, further, the ISP may be willing to confirm or deny the existence of the requested information. While asking won’t result in the requested information being granted, it will make the next steps significantly easier.

There are two methods by which one can use the courts to obtain identifying information in a libel action: by way of the Supreme Court Civil Rules or by relying on the common law “equitable bill of discovery” or Norwich Pharmacal Order. Each will be discussed in turn detail below.

A. The Supreme Court Civil Rules

The most common method for obtaining identifying information is to bring an action for defamation naming “John Doe” defendants, following which an application can brought under Rules 7-1(18) and 7-5 of the Supreme Court Civil Rules (formerly Rules 26(11) and 28 of the Rules of Court). These rules provide for disclosure of documents and information from non-parties.

The proper procedure involves bringing a notice of application, supported by affidavit material which sets out the alleged defamatory publication, the extent to which the defamatory publication was disseminated, the nature and extent of the harm, the information sought, the necessity of the information and the previous steps taken to obtain disclosure.⁴³

This notice of motion should then be served on the ISP. The ISPs will likely take no position on the application; however it is advisable to contact the ISP before bringing the notice of application and discuss the terms of the order being sought, which may include a term compensating the ISP for reasonable legal or administrative fees associated with obtaining the requested information.

The test for disclosure under Rule 7-1(18) is not onerous; it is only necessary for the party to show that the documents sought relate to a matter at issue and the plaintiff is not embarking on a “fishing expedition.”⁴⁴ Similarly, under Rule 7-5, the application must be supported only by an affidavit setting out:

- (a) the matter in question in the action to which the applicant believes that the evidence of the proposed witness may be material,
- (b) if the proposed witness is an expert retained or specially employed by another party in anticipation of litigation or preparation for trial, that the applicant is unable to obtain facts and opinions on the same subject by other means, and
- (c) that the proposed witness
 - (i) has refused or neglected on request by the applicant to give a responsive statement, either orally or in writing, relating to the witness’ knowledge of the matters in question, or
 - (ii) has given conflicting statements.

42 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5.

43 *Supra*, note 34, at 791.

44 *Dufault v. Stevens*, 1978 CanLII 366 (BC C.A.), at para. 9.

Following a successful application, one may then substitute the names of the actual defendants for the John Doe defendants and proceed with the litigation. While an application under the Supreme Court Civil Rules is the easiest method to obtain disclosure of anonymous information, recent jurisprudence suggests that this method does not sufficiently protect the privacy rights Internet users. Accordingly, the *Norwich Pharmacal* procedure set out below may be preferable for obtaining pre-action discovery.

B. Norwich Pharmacal Order/Equitable Bill of Discovery

A *Norwich Pharmacal* order is a form of discovery which permits a plaintiff or potential plaintiff to identify a potential defendant by way of an “equitable bill of discovery.” Although typically used as a form of pre-action discovery, there is nothing which precludes this order from being sought in the context of ongoing litigation.

The order is named after the UK case of *Norwich Pharmacal Co. v. Commissioners of Customs & Excise*, [1974] A.C. 133 (H.L.). In this case, the House of Lords held that where a person becomes involved in the tortious acts of others, even innocently, that person has a duty to give full information to the injured party, by way of discovery, to disclose the identity of the wrongdoer. The authority for granting this order was found in a number of historical cases dating back to the 19th century.

The availability of *Norwich Pharmacal* orders in BC was confirmed by Madam Justice Saunders in the 1999 case of *Kenney v. Loewen*.⁴⁵ In this case, the plaintiff brought an application for summary judgment as well as a bill of discovery. The plaintiff alleged that he had been defamed by a person whose identity was not known to him, but was known to the defendants.

The defendants argued that the remedy of a bill of discovery was not available, as it was not part of the law of England when English law was received in BC, and further, that this form of discovery was not provided for in the Rules of Court and should therefore not be permitted.

After reviewing the law prior to 1858, Madam Justice Saunders held that the remedy was available in BC prior to the receipt of English laws in BC, and was therefore valid in BC.⁴⁶

In respect of the second argument, that the Rules of Court precluded pre-action discovery, the court found that there was nothing in the Rules of Court inconsistent with the remedy sought. The Court in *Kenney* further affirmed the utility of *Norwich Pharmacal* orders as a method of discovery, as they avoid actions in which a party is sued simply to gain discovery:

Further, the remedy of a bill of discovery is transparent, having the virtue of clear definition of the real issues in dispute between plaintiff and defendant. Unlike the slight of hand where a party who is not the ultimate target is sued simply to gain discovery, a process highly improper as noted in *Wilson v. Church* (1878), 9 Ch.D. 378 (C.A.) and *MacRae v. Lecompte* (1983), 143 D.L.R. (3d) 219 (Ont.H.C.J.), a claim for a bill of discovery reveals on its face the real extent of legal risk faced by a defendant in a case.⁴⁷

The equitable remedy of a bill of discovery has since been considered in a number of cases in Ontario. In *Isofoton S.A. v. Toronto Dominion Bank*,⁴⁸ the applicant sought a Norwich order to compel third party banks to provide it with access to bank records in a case of alleged fraud. After noting that “requests for Norwich relief are largely unfamiliar to Canadian courts” (at para. 2), the Court reviewed

45 *Kenney v. Loewen*, [1999] B.C.J. No. 363 (S.C.).

46 *Ibid.* at para. 23.

47 *Ibid.* at para. 30.

48 *Isofoton S.A. v. Toronto Dominion Bank*, 2007 CanLII 14626 (ON S.C.).

the appropriate standard to be applied to the granting of an order, and concluded that the applicant need only demonstrate a *bona fide* claim against the alleged wrongdoer, as opposed to the “strong *prima facie*” case required to obtain other forms of interlocutory relief.⁴⁹

In *GEA Group AG v. Ventra Group Co.*,⁵⁰ the Ontario Court of Appeal conducted an extensive review of Canadian cases in which bills of discovery had been sought, and formulated a set of factors to be considered in determining whether this equitable remedy should be granted. While agreeing with jurisprudence that held that the “scope and nature of *Norwich Pharmacal* principle is far from settled” (at para. 54), the Ontario Court of Appeal set out the following principles as central to the inquiry of the court:

1. Whether the applicant has provided evidence sufficient to raise a valid, *bona fide* or reasonable claim;
2. Whether the applicant has established a relationship with the third party from whom the information is sought such that it establishes that the third party is somehow involved in the acts complained of;
3. Whether the third party is the only practicable source of the information available;
4. Whether the third party can be indemnified for costs to which the third party may be exposed because of the disclosure, some [authorities] refer to the associated expenses of complying with the orders, while others speak of damages; and
5. Whether the interests of justice favour the obtaining of the disclosure.⁵¹

Similar factors were recently identified by the BC Supreme Court in *College of Opticians of British Columbia v. Coastal Contacts Inc.*⁵² In this case, the College of Opticians attempted to obtain a *Norwich Pharmacal* order to compel Coastal Contacts to disclose the identity of the optician or eye care professional it employed. After reviewing *Kenney*, Madam Justice Gerow set out the following test for granting a *Norwich Pharmacal* order:

1. the plaintiff must show that a *bona fide* claim exists against the unknown wrongdoer;
2. the plaintiff must establish that disclosure will facilitate rectification of the wrong;
3. the defendant must be the only practicable source of the information;
4. there is no immunity from disclosure;
5. the plaintiff must establish a relationship with the defendant in which the defendant is mixed up in the wrongdoing. Without connoting impropriety, this requires some active involvement in the transactions underlying the intended cause of action;
6. disclosure by the defendant will not cause the defendant irreparable harm; and
7. the interests of justice favour granting the relief.⁵³

49 *Ibid.* at paras. 46-47.

50 *GEA Group AG v. Ventra Group Co.*, 2009 ONCA 619.

51 *Ibid.* at para. 51.

52 *College of Opticians of British Columbia v. Coastal Contacts Inc.*, 2010 BCSC 104.

53 *Ibid.* at para 16.

Although this test appears at first blush to be more onerous than the one set out under the Supreme Court Civil Rules, there are a number of advantages to proceeding by way of *Norwich Pharmacal* application.

First, this application can be sought by way of petition. In many circumstances it will be faster to bring a petition seeking *Norwich Pharmacal* order than to commence an action against anonymous defendants and then bring a notice of application, given the longer waiting times for notices of application under the Supreme Court Civil Rules.

Second, because this remedy can be sought pre-litigation, it is possible to obtain the identity of the author of the defamatory publications without having to commence a lawsuit. This may be advantageous where the identity of the anonymous author may be more important than the defamatory postings themselves. For example, a party to matrimonial proceedings may wish to obtain the identity of the creator of an anonymous defamatory Facebook group, but may not wish to actually commence an action against their former spouse.

Finally, as set out in the next section, Canadian courts are increasingly recognizing the legitimate privacy expectations individuals have in maintaining their online anonymity, and may be reluctant to grant future disclosure orders on the basis of the relatively low threshold established under the Supreme Court Civil Rules.

VIII. Balancing Privacy and Disclosure

In the 2009 Ontario case of *York University v. Bell Canada Enterprises*,⁵⁴ York University sought a *Norwich Pharmacal* order compelling Internet service providers to disclose the identity of the anonymous author of allegedly defamatory emails and web postings that accused York University's president of fraud.

Applying the test set out in *GEA Group AG v. Ventra Group Co.*, Mr. Justice Strathy examined the role of the anonymous author(s) privacy expectations as they related to the interests of justice in granting the application. The court looked at the service agreements and privacy policies of the Bell and Rogers ISPs, both which prohibited use of the internet services for the purposes of posting defamatory material and both of which provided that identifying information could be disclosed by court order. In granting the application, Mr. Justice Strathy found as follows:

A Bell customer can reasonably contemplate, therefore, that his or her identity may be disclosed by order of the court in the event he or she engages in unlawful, abusive or tortious activity.⁵⁵

The courts concern for the privacy interests of the anonymous author was also reflected in the order granted, which included a term requiring the University to serve the author with a copy of the order, once identified. The author could then apply, on notice to the University, to vary or vacate the order.

More recently, a three-judge panel of the Ontario Superior Court of Justice refused to grant an application for disclosure of identifying information under the Ontario Rules of Civil Procedure, citing the privacy interests of the Internet user as identified by Mr. Justice Strathy in *York University*.

In *Warman v. Fournier et al*,⁵⁶ the plaintiff sought an order requiring named defendants to list all documents in their possession relating to the identities of the defendant John Does 1-8 in a defamation action, including their e-mail addresses and IP addresses used by them when making the specific

54 *Supra*, note 35.

55 *Ibid.* at para. 34.

56 *Warman v. Fournier et al*, 2010 ONSC 2126.

postings identified in the statement of claim. This order was granted at the trial level, and on appeal to the Ontario Superior Court of Justice the Canadian Civil Liberties Association was granted intervenor status to argue the importance of protecting the privacy of Internet users on behalf of the anonymous defendants.

The Court noted at the outset that this application involved the balancing of conflicting privacy interests:

Privacy interests arise for consideration in the present case in favour of both the plaintiff and the John Doe defendants. As the Supreme Court ruled in *Hill*, the good reputation of an individual is intimately connected to his right to privacy, and thus the right to privacy of the plaintiff may be affected by the allegedly libelous postings. At the same time, the John Doe defendants who made the allegedly libelous postings arguably had a reasonable expectation of privacy, having expressly elected to remain anonymous when they did so.⁵⁷

Although that the application was brought under the Rules of Civil Procedure, the Ontario Superior Court of Justice found that, because the Rules of Civil Procedure have the force of a statute, they must be interpreted in a manner consistent with *Charter* rights and values.⁵⁸

According to the court, interpreting the Rules of Civil Procedure in accordance with the *Charter* involved consideration of more than the mere relevance where privacy concerns are raised:

In circumstances where *Charter* rights are engaged and therefore courts are required to take such interests into consideration in determining whether to order disclosure, the case law indicates that the *Charter* protected interests are balanced against the public interest in disclosure in the context of the administration of justice by a combination of (1) a requirement of an evidentiary threshold, (2) fulfillment of conditions establishing the necessity of the disclosure sought, and (3) an express weighing of the competing interests in the particular circumstances of the litigation. In order to prevent the abusive use of the litigation process, disclosure cannot be automatic where *Charter* interests are engaged. On the other hand, to prevent the abusive use of the internet, disclosure also cannot be unreasonably withheld even if *Charter* interests are engaged.⁵⁹

After finding that there was no case law that specifically addresses relevant *Charter* considerations in an application under the Rules of Civil Procedure, the Ontario Superior Court of Justice turned to the *Norwich Pharmacal* jurisprudence. According to the court, “the fundamental premise of *Norwich Pharmacal* is that, where privacy interests are involved, disclosure is not automatic even if the plaintiff establishes relevance and the absence of any of the traditional categories of privilege.”⁶⁰

Given the competing privacy interests at stake in a defamation action, as well as the importance of freedom of expression, the court held that something more was required than the mere relevance test under the Rules of Civil Procedure (essentially the same test as that under BC’s Rule 7-1(18)) for the court to order disclosure of the identity of anonymous online authors:

... because this proceeding engages a freedom of expression interest, as well as a privacy interest, a more robust standard is required to address the chilling effect on freedom of expression that will result from disclosure. It is also consistent with the recent pronouncements of the Supreme Court that establish the relative weight that must be accorded the interest in freedom of expression. In the circumstances of a

57 *Ibid.* at para. 18..

58 *Ibid.* at para. 22.

59 *Ibid.* at para. 24.

60 *Ibid.* at para. 27.

website promoting political discussion, the possibility of a defence of fair comment reinforces the need to establish the elements of defamation on a *prima facie* basis in order to have due consideration to the interest in freedom of expression. On the other hand, there is no compelling public interest in allowing someone to libel and destroy the reputation of another, while hiding behind a cloak of anonymity. The requirement to demonstrate a *prima facie* case of defamation furthers the objective of establishing an appropriate balance between the public interest in favour of disclosure and legitimate interests of privacy and freedom of expression.⁶¹

This case has since been cited with approval by the Supreme Court of Nova Scotia.⁶² In light of this ruling, it may be the test for disclosure of identifying information under the Supreme Court Civil Rules becomes more onerous and complicated. At the very least, one should consider the privacy interests of the anonymous authors when bringing an application for disclosure, either under the Rules of Court or by way of *Norwich Pharmacal* order.

IX. Conclusion

Not only have Canadian courts adapted to the electronic frontier, but they have managed to thrive. Ancient common law remedies such as the *Norwich Pharmacal* order have been repurposed for the information age, questions of limitation periods and jurisdiction have mostly been settled, and while there remains tension between the competing privacy interests of Internet users and plaintiffs, it is generally possible to obtain orders for the disclosure of the identity of anonymous authors.

Further, Canadian courts appear quite willing to award aggravated and punitive damages against those who sought to make use of the Internet to “spray libellous graffiti.”

By way of example, in the case of *Vaquero Energy Ltd. v. Weir*,⁶³ the Alberta Court of Queens Bench awarded \$25,000 in punitive damages against a defendant who had posted defamatory material about a mining company and its CEO on a stock bulletin board, citing the anonymity and ubiquity of the Internet as reasons for doing so:

E-mails are easy to send and can be sent anonymously in the sense that readers cannot know who the author is and that person’s motives for sending the e-mail. To take an example, if a defamatory article is published about someone in a newspaper with a well-known political bias, a reader can take that into account. Because an e-mail is anonymous, a reader is not readily able to discount comments that are made. There is a greater risk that the defamatory remarks are believed. That aggravates the defamation.

...

He said Mr. Waldner was insane, called him a moron, equated his conduct to that of Hitler, Saddam Hussein and Osama bin Laden, all under the protection of anonymity. Finally, it was published literally to the world. That conduct deserves sanction.⁶⁴

More recently, in March of 2010, the BC Supreme Court awarded \$75,000 in punitive and \$75,000 in aggravated damages against an online publisher who used the internet to anonymously defame.⁶⁵ While lawlessness may once have reigned, the sheriff has come to town.

61 *Ibid.* at para. 42.

62 *A.B. v. Bragg Communications Inc.*, 2010 NSSC 215.

63 *Vaquero Energy Ltd. v. Weir*, 2004 ABQB 68.

64 *Ibid.* at paras. 17 and 26.

65 *Hunter Dickinson Inc. v. Butler*, 2010 BCSC 939.

X. Model Disclosure Order

The affidavit in support of an application for disclosure should include the following:

1. It should set out the defamatory postings, to establish that a *bona fide* claim exists against the unknown wrongdoer. Print outs of the defamatory publications can be attached as exhibits.

On October 22, 2008, a user identified as "ANONYMOUS" posted a message on the Forum, an online bulletin board service hosted by the Respondent, as part of a message thread concerning the Plaintiff. Attached as **Exhibit "A"** to this my affidavit is a copy of the October 22, 2008 posting by ANONYMOUS.

2. It should set out that, in order to proceed with the action/a proposed action against the anonymous defendant, the information being sought is required.

I am informed by the Plaintiff and verily believe to be true that the Plaintiff does not know the identity of the author or authors responsible for the forum postings. I understand that in order to proceed with a lawsuit against the author or authors, it is necessary for the Plaintiff to ascertain the identity of the author or authors of the above messages.

3. The affidavit should set out the involvement of the ISP or email service provider.

I understand that in order to post messages to the Forum, it is necessary for an individual to set up an account with Example.com. To set up an account with Example.com, an account holder must provide an e-mail address to Example Corp.

Example Corp. may also be in possession of other personal information about ANONYMOUS, including but not limited to the internet protocol ("IP") address(es) of the computer(s) utilized by ANONYMOUS to send the postings.

4. It should set the defendant is the only practicable source of the information, and set out the previous steps that have been taken to obtain the information.

Under cover of letter dated October 30, 2009, counsel for the Plaintiff wrote to Example Corp., requesting that Example Corp. disclose information necessary to aid in the identification of the author(s) of the defamatory communications, including any and all registration data, internet protocol addresses ("IP addresses"), and e-mail addresses associated with the ANONYMOUS account. Attached as **Exhibit "B"** to this my affidavit is a copy of the October 30, 2009 letter.

By way of email dated November 1, 2009, John Doe, Senior Editor of Example Corp., wrote to counsel for the Plaintiff and stated that Example Corp. would not turn over the requested information without a court order. Attached as **Exhibit "C"** to this my affidavit is a copy of the November 1, 2009 letter.

5. It should include the terms of use of the ISP or email service provider. The terms of use typically include a term that the user will not use the services provided to defame, harass or conduct criminal activity.

I understand that by signing up for a Forum account, Forum users agree to be bound by the Example.com Service Agreement. The Example.com Service Agreement includes a "Code of Conduct", which states the following:

You will not upload, post, transmit, transfer, distribute or facilitate distribution of any content (including text, images, sound, video, data, information or software) or otherwise use the service in a way that:

...

incites, advocates, or expresses pornography, obscenity, vulgarity, profanity, hatred, bigotry, racism, or gratuitous violence.

...

threatens, stalks, defames, defrauds, degrades, victimizes or intimidates an individual or group of individuals for any reason; including on the basis of age, gender, disability, ethnicity, sexual orientation, race or religion; or incites or encourages anyone else to do so.

Attached as **Exhibit "D"** to this my affidavit is a copy of the Example.com Service Agreement and Code of Conduct.

6. Finally, the affidavit should set out the privacy policy of the service provider. The privacy policy will typically inform the user that personal information can be disclosed pursuant to a court order.

The privacy Example.com affords its customers is outlined in Example.com Privacy Policy, which states "Example.com collects personal information to provide you with the best and most personalized experienced possible." It goes on to state that:

Example.com will not disclose any personally identifiable information about individual users, except as described in this Privacy Statement... As for individually identifiable information, we may disclose it only under the following circumstances:

...

We may disclose your personal information as required by applicable law, or in response to legal process, to protect the rights or property of Example.com, or to protect the safety of Example.com, our users, or others.

Attached as **Exhibit "E"** to this my affidavit is a copy of the Example.com Privacy Policy.

It is important to include the Terms of Use and Privacy Policy. Together, these documents may provide a basis for arguing that the privacy rights of the anonymous author are limited, and further, that it should be within the anonymous author's contemplation that their identifying information may be turned over pursuant to a court order.

In light of the decision in *Warman v. Fournier et al.*, 2010 ONSC 2126, we have drafted a model order that takes into account the privacy interests of an anonymous author by including as a term of the order a term permitting the anonymous author to apply to vary or vacate the order.

Before bringing an application, the ISP or internet company should be contacted, and proposed terms of the Order set out in advance. A standard order under the BC Supreme Court Civil Rules/*Norwich Pharmacal* order can be drafted as follows:

THIS COURT ORDERS that:

1. Google Inc. disclose to the Plaintiff/Petitioner email address(es), name(s), IP address(es), and any other identifying information of the account holder(s) associated with the email addresses "abc@gmail.com";
2. The Plaintiff pay to Google all reasonable costs incurred by Google for the retrieval, production, inspection and delivery of the identifying information forthwith in the agreed amount of \$150.00; and
3. This Order shall be served by the Plaintiff/Petitioner on the account holder(s) identified by Google Inc. and those person(s) and any person(s) affected by this order may apply on two days notice to the Plaintiff/Petitioner to vary or vacate this Order.