Reproduced with permission of the publisher from the
Canadian Privacy Law Review, Vol. 8, No. 3, February 2011

CANADIAN PRIVACY LAW REVIEW

Volume 8 • Number 3 February 2011

In This Issue:

What Damages Can Be Claimed Pursuant to the *PIPEDA* by the Victims of Breach of Privacy?

Sidney Elbaz
Associate
McMillan LLP

Éloïse Gratton
Technology Counsel
McMillan LLP

A decision rendered on November 12, 2010, by Justice Phelan of the Federal Court (*Stevens v. SNF Maritime Metal Inc.*, [2010] F.C.J. No. 1410, 2010 FC 1137) sheds some light on the types of damages an applicant can claim following a conclusion by the Privacy Commissioner of Canada (the "Commissioner") that the Applicant had been the victim of a breach of privacy pursuant to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*].

The Facts:

The Applicant, employed by a third party (the "Employer"), was responsible for delivering scrap metal to the Respondents on behalf of the Employer. The Employer became concerned that its sales of scrap metal to the Respondent were below historical norms and, after communicating with the Respondent, the Employer learned that the Applicant maintained personal accounts for the sale of scrap metal to the Respondent. The Respondent provided the Employer with copies of records pertaining to the Applicant's personal accounts, which revealed that the Applicant had been credited with, and received cash for, large quantities of scrap metal. The Applicant was dismissed from his employment.

lead to a future court challenge, and how the *Air Canada* and *State Farm* decisions are dealt with by tribunals and commissioners.

[*Editor's note*: The author would like to acknowledge the invaluable research assistance of Sarah Conroy, Articled Student at Davis LLP.]

1 See protocols for claims of solicitor-client privilege available on the websites of the B.C. and Alberta Privacy Commissioners: <http://www.oipc.bc.ca/advice/SOLICITOR-CLIENT_PRACTICE_NOTE(MAY2009).pdf> and <http://www.oipc.ab.ca/Content_Files/Files/News/Protocol_Adjudication_EXTERNAL_Oct_2008.pdf>. In our view, these protocols are practically useful, but are not entirely consistent with the decision in *Blood Tribe*. There do not appear to be similar protocols in place in the Ontario or Quebec OIPCs (or equivalent offices).

2 Indeed, s. 44(2.1) of *FOIPPA* states that if a person discloses to the Commissioner a record protected by solicitor-client privilege, the privilege is "not affected" by the disclosure. Section 44(3) of *FOIPPA* states that "despite … any privilege of the law of evidence", a public body must produce a document to the Commissioner where the Commissioner has ordered the public body to do so for the purposes of an investigation or audit. Of course, the Supreme Court of Canada has made clear in *Blood Tribe* that solicitor-client privilege is not merely part of evidentiary law but, rather, is a substantive right or presumption of the common law. This was recently confirmed in *Newfoundland and Labrador (Attorney General) v. Newfoundland and Labrador (Information and Privacy Commissioner)*, [2010] N.J. No. 52, 2010 NLTD 31 (see para. 38).

3 Indeed, this article could have been entitled "50 Ways to Distinguish *Blood Tribe*"!

4 A similar result was reached in *Ontario Public Service Employees Union v. Ontario*, [2010] O.G.S.B.A. No. 123 (Ontario Grievance Settlement Board).

5 It should also be noted that there are similar provisions in Alberta *FOIPPA*, RSA 2000, c. F-25 (s. 59(4)), and in British Columbia *FOIPPA* (s. 47(4)) and *PIPA* (s. 41(4)) which indicate that the British Columbia or Alberta Commissioners could also find themselves adverse in interest to an organization or public body before them.

6 There is a pending application for judicial review in the Federal Court of Appeal with respect to the decision in *Quadrini*. The Federal Court of Appeal granted a stay of the PSLRB's order in *Canada (Attorney General) v. Quadrini*, [2010] F.C.J. No. 194, 2010 FCA 47, until a final determination of the issue is made by the Court. A Requisition for Hearing was filed on August 16, 2010, but a hearing date has not yet been set.

7 This decision of the Northwest Territories Commissioner was released after the Federal Court of Appeal decision in *Blood Tribe* but before the Supreme Court of Canada decision in *Blood Tribe*.

Unmasking Anonymous Defendants in Internet Defamation Cases: Recent Developments and Unresolved Issues

Matthew Nied
Student-at-Law

Introduction

Jane Doe was a law student at the top of her class. Despite interviews with more than a dozen employers, she failed to receive an articling position at the end of law school. Jane was perplexed. It wasn't until weeks later that she ventured to conduct an internet search of her own name. What she found was alarming. Among the search results was a website containing false and offensive postings about her character, morals, and sexuality. Horrified, Jane sent an email to the website operator requesting that the postings be removed. The operator ignored her request, and the postings remained visible for the world to see.[1]

While the internet provides users with an environment in which socially valuable speech can flourish, it also provides users with an opportunity to defame others behind a shield of anonymity. If these users can be identified, they may be held liable for defamation. Unfortunately for plaintiffs, the identities of these users are usually known only by the website or internet service provider ("ISP") through which the statements were made, and these third parties generally decline to disclose a user's identity in the absence of a court order compelling them to do so.[2] Faced with a growing stream of applications for such orders, courts have sought to consistently assess them in a way that strikes an appropriate balance between the freedom of expression and privacy interests of anonymous defendants and the reputational interests of plaintiffs.

Currently, there are two ways for plaintiffs to compel third parties to disclose the identity of anonymous defendants: by seeking an equitable remedy of discovery known as a "*Norwich* order", or by seeking pre-action discovery or production under the applicable rules of civil procedure. Although courts have developed these approaches to strike a more appropriate balance between the competing interests, two unresolved issues remain to threaten that balance. First, while the approaches are similar, they differ with

respect to the protection that they afford to the privacy and freedom of expression interests of anonymous defendants. Second, neither approach requires that anonymous defendants be informed of applications for the disclosure of their identities in order to enable them to represent their interests. This article surveys the two approaches, discusses the unresolved issues, and considers how courts may address them.

The *Norwich* approach

Plaintiffs may seek disclosure of the identity of anonymous defendants from third parties by way of an equitable remedy of pre-action discovery known as a "*Norwich* order". *Norwich* orders were introduced in *Norwich Pharmacal Co. v. Customs and Excise Commissioners*[3] in which it was held that where a third party becomes involved in the tortious acts of others, that third party has a duty to disclose the identity of the tortfeasor.[4]

Five factors apply to the determination of whether to grant a *Norwich* order in the internet defamation context. These factors were set out by the Ontario Superior Court of Justice in *York University v. Bell Canada Enterprises:*[5]

- whether the applicant has provided evidence sufficient to raise a valid, *bona fide* or reasonable claim;
- 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 involved in the acts;
- whether the third party is the only practicable source of the information;
- whether the third party can be indemnified for costs to which it may be exposed because of the disclosure; and
- whether the interests of justice favour obtaining the disclosure.

In *York University*, the plaintiff sought a *Norwich* order to compel ISPs to disclose the identity of the anonymous author of allegedly defamatory emails and web postings that accused a university president of committing academic fraud. After concluding that the first four factors were met, the court proceeded to consider the fifth factor which, in the court's words, required it to "balance the benefit to the applicant of revealing the desired information against the prejudice to the alleged wrongdoer in releasing the information."[6] The court concluded that the interests of justice favoured the disclosure of the author's identity, primarily because the author could not have had a reasonable expectation of privacy with respect to their identity due to the terms of their ISP's privacy policy. Significantly, while the court concluded that the plaintiff had demonstrated a *prima face* case under the first factor, it did not require the plaintiff to demonstrate more than a *bona fide* case.

The same approach was taken in the earlier case of *BMG Canada Inc. v. John Doe*,[7] albeit in a different context. In that case, the plaintiffs, a group of music recording industry companies, commenced action against internet users who were alleged to have engaged in illegal file sharing. The trial court applied the *Norwich* order analysis and concluded that the application should be denied. In doing so, the court held that the plaintiffs were required to demonstrate a *prima facie* case under the first *Norwich* factor. Although the Federal Court of Appeal affirmed the trial court's decision, it clarified that the first *Norwich* factor only requires plaintiffs to demonstrate a *bona fide* belief of wrongdoing. The court expressed the concern that the imposition of the higher *prima facie* standard would effectively strip the plaintiff of a remedy because the plaintiff could not know the case that they wished to assert against the defendants until they knew of the identity of the persons that they wished to sue and the nature of their involvement in the file-sharing activities.[8]

The *Rules* approach

Plaintiffs may also identify anonymous defendants by seeking pre-action discovery or production of information under the applicable rules of civil procedure. Although the rules of civil procedure in most provinces impose a low threshold for plaintiffs to meet before disclosure will be ordered,[9] recent decisions have held that the *Charter* requires courts to strike a balance between the competing interests by requiring plaintiffs to:

- meet an evidentiary threshold;
- establish the necessity of the disclosure sought; and
- demonstrate that disclosure is favoured by a weighing of competing interests.[10]

These requirements were set out by the Ontario Divisional Court of Justice in *Warman v. Wilkins-Fournier*.[11] In that case, the plaintiff commenced an action against the operators of an internet message board and eight anonymous participants. The alleged defamation arose from a series of postings that contained offensive comments about the plaintiff. At the document production stage, the operators of the internet message board refused to disclose documents that contained the identity of the anonymous defendants, due to privacy concerns. In response, the plaintiff brought a motion for an order compelling the operators to comply with the *Rules of Civil Procedure* which required the production of those documents.[12] Because the *Rules* did not require the plaintiffs to satisfy the court that they had met an evidentiary threshold, the motions judge concluded that such disclosure was mandatory and automatic upon the issuance of a statement of claim. This result stood in stark contrast with earlier cases that offered protection to the privacy of internet users beyond that provided by the *Rules*.[13]

The Divisional Court unanimously allowed the appeal, recognizing that the anonymous posters' privacy and right of freedom of expression under the *Charter* must be taken into account in considering a request for disclosure under the *Rules*. The court held that, because the *Rules* have the force of statute, they must be interpreted in a manner consistent with the *Charter*. In rejecting the notion that disclosure is mandatory and automatic, the court expressed concern for the ease by which "a plaintiff with no legitimate claim" could "misuse the *Rules* … by commencing an unmeritorious action for the sole purpose of revealing the identity of anonymous internet commentators, with a view to stifling such commentators and deterring others from speaking out on controversial issues."[14]

The court set out four considerations, aimed at respecting the privacy of internet users, that should be considered by courts in deciding whether to order disclosure:[15]

- whether the unknown alleged wrongdoer could have a reasonable expectation of anonymity in the particular circumstances;
- whether the plaintiff has established a *prima facie* case against the unknown alleged wrongdoer and is acting in good faith;
- whether the plaintiff has taken reasonable steps to identify the anonymous party and has been unable to do so; and
- whether the public interests favouring disclosure outweigh the legitimate interests of freedom of expression and right to privacy of the persons sought to be identified if the disclosure is ordered.

In concluding that plaintiffs should be required to meet a *prima facie* standard rather than the lower *bona fide* standard, the court emphasized that the "more robust standard is required to address the chilling effect on freedom of expression that will result from disclosure."[16] The court noted that the *prima facie* standard "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."[17] The court also distinguished *BMG Canada* where the Federal Court of Appeal expressed the concern that the imposition of the *prima facie* standard would effectively strip the plaintiff of a remedy because the plaintiff could not know the case that they wished to assert against the defendants until they knew of the defendants' identities and the nature of their involvement in the file-sharing activities. The court in *Warman* held that this concern does not arise in internet defamation cases because plaintiffs will inevitably know the details of the allegedly defamatory acts at issue.[18]

Courts in other provinces have followed *Warman*. In *A.B. v. Bragg Communications Inc.*,[19] the plaintiff sought an order from the Nova Scotia Court of Queen's Bench requiring an ISP to disclose the identity of an anonymous user that created a fake Facebook profile. The profile contained the plaintiff's picture, a variation

of her name, personal information, and offensive sexual commentary. The plaintiff's application was made pursuant to the Nova Scotia *Civil Procedure Rules*.[20] In the course of finding that disclosure was appropriate, the court applied the considerations set out in *Warman*.[21] The New Brunswick Court of Queen's Bench adopted the same approach in *Doucette v. Brunswick News*.[22] In that case, the plaintiff sought an order requiring newspaper publishers to disclose the identity of a person that posted allegedly defamatory comments on their website. The plaintiff sought disclosure under both approaches by bringing a *Norwich* application under a provision in the New Brunswick *Rules of Court*.[23] The court engaged in an analysis under both approaches before concluding that disclosure was appropriate.

Evidentiary standards

Although the approaches go some way to assist courts with the process of striking an appropriate balance between the freedom of expression and privacy interests of anonymous defendants and the reputational interests of plaintiffs, two unresolved issues remain to threaten that balance. First, while the approaches are similar,[24] they differ with respect to the evidentiary threshold to be met by plaintiffs before disclosure will be ordered. Whereas the *Rules* approach requires plaintiffs to demonstrate a *prima facie* case due to the applicability of the *Charter*, the *Norwich* approach permits plaintiffs to seek disclosure by demonstrating merely a *bona fide* case. The concern is that the *Charter* protection afforded to defendants under the *Rules* approach is threatened if plaintiffs can circumvent it by seeking disclosure under a less onerous approach.

Courts have recognized that the *prima facie* standard is required to address the chilling effect on freedom of expression that results from disclosure.[25] The unmaking of an anonymous defendant may subject them to ostracism for expressing unpopular ideas, or invite retaliation from those who oppose their views.[26] The problem with the *bona fide* standard is that it may permit unjustified breaches of privacy and the right to freedom of expression by allowing for the unmasking of defendants by plaintiffs that do not have a meritorious case, as long as they honestly believe that they do.[27] It may also allow plaintiffs who did not intend to pursue a claim to deprive defendants of their anonymity solely for the purpose of pursuing extra-judicial forms of relief.[28]

To resolve this issue and harmonize the law, courts may adapt the *Norwich* approach to preclude plaintiffs from unmasking anonymous defendants on the basis of the lower standard. While *Norwich* jurisprudence has traditionally applied the *bona fide* standard,[29] courts may not consider themselves bound to do so in internet defamation cases. As the court in *Warman* noted, *Norwich* orders are equitable remedies with principles that should be applied flexibly, and the question of whether a plaintiff must satisfy a *bona fide* or *prima facie* standard is an issue to be resolved on a case-by-case basis.[30] Moreover, although the *Charter* does not apply to *Norwich* orders because they are made under common law authority, the principles of the common law must develop in a manner consistent with *Charter* values.[31] There is no reasonable justification for maintaining different standards when the same *Charter* rights are at stake.

Notice requirement

Second, neither approach requires that plaintiffs or third parties make reasonable efforts to inform anonymous defendants of applications to compel the disclosure of their identities in order to enable them to represent their interests. This is a concern because there is generally no affinity of interest between anonymous defendants and third parties, who would rather decline to challenge applications for disclosure in order to evade the cross-fire of litigation as rapidly and cheaply as possible.[32] As a consequence, a defendant may be stripped of their anonymity and subjected to embarrassment, social stigma, harm to their career prospects, or risk to their personal safety without notification that they have the opportunity to represent their interests by anonymously opposing the application.

Despite these concerns, courts have held that the determination of whether to give notice should be made on a case-by-case basis.[33] In *York University*, the court noted that it "may be appropriate, in a given case, to require that the unknown publisher of the offending

material be given notice of the proceedings" but declined to do so because it did "not appear to have been done as a matter of course in other *Norwich* order cases" and the court "did not consider it necessary to do so in [that] case".[34] The court in *Warman* agreed that the determination of whether to give notice should be made on a case-by-case basis and commented that "little would generally be added by such a step, because any defences that might be raised are not relevant to a determination as to whether a *prima facie* case has been made out." Nevertheless, the court stated that a notice requirement might be necessary in cases where a defendant has "compelling reasons for wishing to remain anonymous that are not immediately obvious, such as a risk to personal safety, and such grounds could not be put before the court absent notice."[35]

Courts may question the validity of this position in future cases. The factors to be considered on an application for disclosure under either approach involve far more than a simple determination of whether a *prima facie* or *bona fide* case has been met. Both approaches involve arguable issues, such as whether the anonymous defendant could have a reasonable expectation of anonymity in the particular circumstances, and whether the public interests favouring disclosure outweigh the legitimate interests of the defendant's freedom of expression and right to privacy. Moreover, where a defendant has a legitimate reason for wishing to remain anonymous that is not immediately obvious, a possibility that the court in *Warman* contemplates, it is difficult to see how that reason could come to the court's attention in the absence of notice to the defendant.

Requiring parties to provide notice to anonymous defendants would impose a relatively light burden while providing defendants with the opportunity to defend their anonymity. While it may be appropriate for plaintiffs to pay the cost of providing notice, they should not bear the burden of doing so. Unlike third parties, plaintiffs are in a relatively poor position to give reliable notice because they lack access to the defendant's contact information.[36] As a result, third parties are in the best position to provide notice.

[*Editor's Note*: Matthew Nied, B.Comm. (Alberta), LL.B. (Victoria) is currently clerking at the Supreme Court of British Columbia. He will commence articles in Vancouver in September 2011. The views expressed in this article are his personal opinions and not those of the judiciary.]

---

1 This fact pattern is based on *Doe I v. Individuals,* 561 F. Supp. 2d 249 (D. Conn. 2008).

2 Federal and provincial privacy legislation may prevent third parties from disclosing information without a court order. See s. 7(3)(c) of the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5. For an example of provincial legislation, see s. 18 of British Columbia's *Personal Information Protection Act,* S.B.C. 2003, c. 63.

3 [1974] A.C. 133 (H.L.).

4 *Ibid.* at 175.

5 [2009] O.J. No. 3689*,* 311 D.L.R. (4th) 755, 99 O.R. (3d) 695 (S.C.J.) at para. 13 [*York University*]. The factors relevant to the determination of whether to grant a *Norwich* order were recently confirmed by the Ontario Court of Appeal in *GEA Group AG v. Ventra Group Co.*, [2009] O.J. No. 3457, 2009 ONCA 619. For authority in British Columbia, see *Kenney v. Loewen*, [1999] B.C.J. No. 363, 64 B.C.L.R. (3d) 346, 28 C.P.C. (4th) 179 (S.C.) and *College of Opticians of British Columbia v. Coastal Contacts Inc.*, [2010] B.C.J. No. 130, 2010 BCSC 104. For authority in Alberta, see *Alberta (Treasury Branches) v. Leahy*, [2000] A.J. No. 993, 270 A.R. 1 (Q.B.), aff'd [2002] A.J. No. 524, 303 A.R. 63 (C.A.), leave to appeal refused [2002] S.C.C.A. No. 235.

6 *York University, supra* note 5 at para. 30. The court added at para. 30 that, at this stage, considerations may include the nature of the information sought, the degree of confidentiality accorded to the information by the party against whom the order is sought, and the degree to which the requested order curtails the use to which the information can be put.

7 [2004] F.C.J. No. 525, 2004 FC 488, aff'd [2005] F.C.J. No. 858, 2005 FCA 193 [*BMG Appeal*].

8 *BMG Appeal*, *ibid*. at para. 34.

9 See *e.g.* Rules 30.06, 30.10, 31.10, and 76.03 of the Ontario *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194 [*Ontario Rules*]. See also Rules 7-1(18) and 7-5 of the *Supreme Court Civil Rules*, B.C. Reg. 168/2009.

10 *Warman v. Wilkins-Fournier*, [2010] O.J. No. 1846, 2010 ONSC 2126 at para. 24 (Div. Ct.) rev'g, [2009] O.J. No. 1305, 309 D.L.R. (4th) 227, 76 C.P.C. (6th) 155 (Ont. S.C.J.) [*Warman*]; see also *A.B. v. Bragg Communications Inc.*, [2010] N.S.J. No. 360, 2010 NSSC 215 at paras. 12, 17 [*Bragg Communications*].

11 *Warman*, *ibid.*

12 Rules 76.03 and 30.06 of the *Ontario Rules*, *supra* note 9.

13 Previous cases required plaintiffs to demonstrate a *prima facie* case of defamation before ordering disclosure. In *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318, [2000] O.T.C. 561, 12 C.P.C. (5th) 103 (S.C.J.) the plaintiffs brought a motion pursuant to Rules 30.10 and 31.10 of the *Ontario Rules*, *supra* note 9 for an order that an ISP produce material identifying the sender of an allegedly defamatory e-mail message. The Ontario Superior Court of Justice concluded that the disclosure of the identity of the anonymous defendant should not be automatic. Rather, the plaintiff first had to demonstrate a *prima facie* case. The court was satisfied that the plaintiff had done so, and concluded that disclosure was appropriate. See also *Latner v. John Doe*, [2010] O.J. No. 3806, 2010 ONSC 4989, which, although decided after the Divisional Court's decision in *Warman*, follows the analysis in *Irwin Toy*.

14 *Warman*, *supra* note 10 at para. 33.

15 *Ibid*. at para. 34.

16 *Ibid.* at para. 42.

17 *Ibid.*

18 *Ibid*. at para. 41. Moreover, at para. 39, the court distinguished the considerations that it set out from those relevant to *Norwich* orders. In particular, the court noted that the second and fourth *Norwich* factors are not relevant to the *Rules* approach because they apply only to third party respondents rather than co-defendants. The other *Norwich* factors are, however, practically identical to the considerations set out in *Warman*.

19 *Bragg Communications*, *supra* note 10.

20 Rules 14.12 and 18.12.

21 In *Bragg Communications, supra* note 10 at para. 21 the court noted that the "reasonableness of an expectation of anonymity must be assessed on a case-by-case basis" and that in the "absence of any suggestion of a compelling interest that would favour anonymity (such as fair comment), the expectation of anonymity … is not a reasonable one." See also the decision of the Nova Scotia Supreme Court in *Mosher v. Coast Publishing*, [2010] N.S.J. No. 348, 2010 NSSC 211. In that case, the plaintiffs sought disclosure of information identifying individuals who authored allegedly defamatory comments published in a newspaper owned by the defendants. The court held that Rule 14.12(1) of the Nova Scotia *Civil Procedure Rules* was appropriate. Although the court considered *York University, supra* note 5 in passing, it did not engage in an analysis of whether the plaintiffs had established a *prima facie* or *bona fide* case.

22 [2010] N.B.J. No. 235, 2010 NBQB 233.

23 Rule 32.12 of the New Brunswick *Rules of Court*, N.B. Reg. 82-73. The factors to be met under the provision are similar to the *Norwich* factors, except that the former requires plaintiffs to demonstrate a *prima facie* case rather than a *bona fide* case.

24 See *supra* note 18.

25 *Warman, supra* note 10 at paras. 41-42.

26 *Doe No. 1. v. Cahill* (2005)*,* 884 A.2d 451 (Del. S.C.) at 457 [*Cahill*]; see also *Krinsky v. Doe 6*, 159 Cal. Rptr. 3d 231, 241(Ct. App. 2008) [*Krinsky*]: "[the *bona fide* standard] offers no practical, reliable way to determine the plaintiff's good faith and leaves the speaker with little protection."

27 *Re Richard L. Baxter,* No. 01-00026-M, 2001 US Dist. LEXIS 26001 (WD La. Dec. 19, 2001).

28 *Cahill, supra* note 26 at 457.

29 See s*upra* note 5.

30 *Warman*, *supra* note 10 at para. 28.

31 *Retail, Wholesale and Department Store Union, Local 580 [R.W.D.S.U.] v. Dolphin Delivery Ltd*., [1986] S.C.J. No. 75, [1986] 2 S.C.R. 573, 33 D.L.R. (4th) 174.

32 *York University, supra* note 5 at para. 21. For a discussion of the relationship of dependence that exists between internet users and third parties, see Ian Kerr, *Personal Relationships in the Year 2000: Me and My ISP, in Personal Relationships of Dependence and Interdependence in Law* (Law Commission of Canada ed., 2002) 78.

33 Conversely, numerous American courts have required plaintiffs or third parties to provide notice to anonymous defendants in internet defamation cases: *Dendrite International, Inc. v. John Doe No. 3,* 775 A.2d 756 (N.J. App. Div. 2001); *Cahill, supra* note 26; *Mobilisa, Inc. v. Doe 1,* 170 P.3d 712 (Ariz. Ct. App. 2007)*; Krinsky, supra* note 26; *Solers, Inc. v. Doe,* 977 A.2d 941 (D.C. 2009).

34 *York University, supra* note 5 at para. 24.

35 *Warman, supra* note 10 at para. 43.

36 Although plaintiffs could be required to provide indirect notice (by posting on the ISP's pertinent message board, the same website used by the defendant to publish the statements at issue, or, if the statements originated in an email, by sending notice to the defendant's email address) there is no guarantee that a defendant will check these sources, or that the website or medium will still exist by the time that the plaintiff commences the action.