

**WEB-BASED PROVIDERS,
ANONYMITY AND THE LEGAL PROCESS**

*Internet and E-Commerce Law in Canada
October 2000*

by
[Andrew Bernstein](#)
Tina Piper

The expectation of anonymity on the Internet is powerful. Internet users with limited technical knowledge write comments on electronic bulletin board services or chat rooms, mistakenly believing their identity is protected, since they have not used their real names. However, each posting leaves an electronic trail which usually leads directly to the poster's identity.

One type of bulletin board that has proven extremely popular, but has caused a number of difficulties, is "stock chatting." Web-based companies such as Yahoo!, have created online bulletin boards dedicated to discussing the financial prospects of specific companies. The comments posted on these message boards focus on factual information about the company and its management, the performance of stocks and trivia about the company. Comments can be posted to bulletin boards "anonymously" since a user can adopt any screen-name he or she chooses.

Often, comments posted to message boards are perceived of as being inflammatory, derogatory and even defamatory of employees and officers of the corporation or of the practices or financial status of the corporation. In addition, some postings may deliberately attempt to circulate false information. If posted comments are serious enough and believed by other users of the message board, they can affect the business interests of a corporation. In some instances, a significant drop in the market price of stock has been attributed to comments posted on a message board. Posted comments have even led to the prosecution of two anonymous posters for securities fraud and conspiracy. Corporations are also concerned that business and trade secrets may be inappropriately divulged by current or former employees on message boards.

Once corporations, businesses or individuals become aware that potentially damaging statements have been made about them online, some attempt to bring an action for defamation or breach of confidentiality. Since these type of comments are inevitably posted anonymously, the potential plaintiff does not know whom to sue. In this situation, frequently the suit will name the defendant(s) as "John/Jane Doe" and then attempt to obtain his or her identity. Identifying an Internet user generally requires information from either or both the website to which he or she posted and the Internet Service Provider ("ISP") to which he or she subscribes.

The ISP provides physical access to the Internet through dial-up modem service or cable links. In exchange for a subscription fee, users are provided with both access to the Internet through the ISP's network and also services such as e-mail, news and entertainment. Web-based companies, such as Yahoo!, canada.com or Lycos, maintain websites on the Internet that are accessible to the public at no charge. The website may host bulletin boards, chatrooms and newsgroups in which the public can participate. In the search for a user's identity, web-based companies can often provide some or all of the e-mail addresses of individuals who access their public site and information the company may have collected during the registration process or the use of the account. Most importantly, web-based companies can provide the Internet protocol ("IP") address of the user and information about the identity of the person who owns the e-mail address, including possibly their name, address, telephone number and billing information. If the website's registration information is incomplete or inaccurate (which is often the case with online defamation), the plaintiff must then attempt to find the ISP who owns that IP address, from whom it then requests the identity of the user.

This attempt at information-gathering by potential plaintiffs creates a tension for companies that provide access to and services on the Internet. To remain competitive, most web-based companies and ISPs must have privacy policies that promise not to disclose information that would reveal their users' identities. Hence, they will rarely do so merely on request. This often results in the plaintiff bringing a motion or application, or serving a subpoena to compel the ISP or web-based company to reveal the IP address and/or identity of the prospective defendant. The ISP or web-based company is then left to decide under what circumstances it should provide the information, whether it should notify its subscriber, and whether notification should occur before or after his/her identity has been revealed. It also raises the question of what

steps companies operating these businesses should take before litigation is commenced to ensure that they are not drawn into the dispute as a litigant for either disclosing or failing to disclose the user's identity.

THE LAW

ISPs and web-based companies have been subject to numerous subpoenas, motions and applications in both the United States and Canada by corporations and individuals seeking to determine the identity of anonymous online posters. As one would expect, the quantity of these requests is growing steadily with the explosion in Internet use.¹ Online businesses will have to strongly consider their user agreements, as well as the still uncertain state of the law, in determining how to react.

Two major U.S. cases demonstrate first, the reluctance of courts to quash a subpoena to compel an ISP to divulge the identity of an online critic and secondly, the potential liability of ISPs if they divulge user information without sufficient notice to those users. In *Hvide v. Does 1-8*² the court rejected the defendant John Doe's motion to quash a subpoena that would require Yahoo! and AOL to disclose his identity. The court decided that requiring the ISPs to reveal the identity of the anonymous online critic did not violate that speaker's First Amendment right to engage in anonymous speech in all media.³

Aquacool_2000 (also known as John Doe) v. Yahoo! raises the stakes. John Doe sued Yahoo! for disclosing his identity to an e-commerce business called AnswerThink Consulting Group Inc. in response to a subpoena. Aquacool allegedly posted messages on a Yahoo! financial information website dedicated to AnswerThink that defamed AnswerThink employees. AnswerThink served Yahoo! with a subpoena to obtain his identity, which Yahoo! complied with. In his complaint, Aquacool claimed Yahoo! does not require that the subpoena be personally served, does not require court approval for out-of-state subpoenas, accepts facsimile service of those subpoenas and does not confirm that the lawsuits pursuant to which the subpoena has been issued comply with state or federal requirements.⁴

In addition to the procedural complaints, *Aquacool_2000* alleges that Yahoo! violated his substantive rights in four ways. First, he alleged that Yahoo! infringed his constitutionally protected reasonable expectation of privacy when it disclosed personal information that Yahoo! had collected when he used its services without his consent, or without notice to him. Second, he claimed that the disclosure of this information breached a written contract of service between himself and Yahoo! by violating an implied covenant of good faith and fair dealing.⁵ Third, he also alleged that Yahoo! negligently misrepresented that it would protect the privacy interests of its members by notifying members before information was transmitted to third parties who would then have the option not to permit the transfer.⁶ Finally, he complained that Yahoo! engaged in unfair competition and false advertising by misleadingly advertising that it provides a high level of protection for its members' personal information.⁷ This claim has been dropped, which is not surprising; it would be quite remarkable if a court found liability for *compliance* with a subpoena. However, this case shows just how strong the expectation of anonymity can be on the Internet, and the extent to which users will hold online businesses to their stated terms and conditions of usage.

There have been no cases analogous to *Aquacool_2000 v. Yahoo!* brought in Canada. However, ISPs have been compelled to release user information. The most high profile case was a suit brought by Philip Services of Canada against John Does 1-26, during the course of which a motion was granted requiring the ISP (Weslink Data Corporation) to provide information regarding the "names, addresses, modem telephone numbers, bills, records and data about the persons sending the messages listed and for all other messages sent by such persons through the Internet providers." Moreover, the court required the disclosure of information

regarding the “names, models, registration numbers, serial numbers, and other identifying information concerning the computers and modems used by the persons.”⁸

Canadian legislative and policy documents fail to clearly address the issue of disclosure and/or notice. Canada’s new private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*, specifically excludes notification of subjects of personal information when the information is sought pursuant to a court order.⁹ However, the recent decision of the Ontario Superior Court of Justice in *Irwin Toy Ltd. v. Doe*¹⁰ gives a strong judicial endorsement to online anonymity while preserving the rights of plaintiffs to proceed with meritorious claims against anonymous critics.

In *Irwin Toy*, Wilkins J. was faced with the typical online defamation situation: a user e-mailed allegedly defamatory material to 75 people (presumably employees of the company). However, this individual could not be traced — all that could be found was an e-mail address and an IP address, which were both traced to iPrimus Canada, an ISP. The plaintiffs contacted the technical administration of iPrimus, who confirmed that the user was an iPrimus subscriber and agreed to preserve the electronic records identifying that user. Not surprisingly, iPrimus refused to volunteer the subscriber’s name, although it did not oppose the court order to provide this information.

There are two notable aspects of Wilkins J.’s decision: first, the framework of analyzing the user to analyze whether to order the ISP to turn over the subscriber’s identity and second, the threshold he sets in applying this framework. His Honour used Rule 31.10 of the *Ontario Rules of Civil Procedure*, permitting oral discovery of non-party as the framework for his analysis. The court will order discovery under Rule 31.10 if (i) there is reason to believe that the party sought to be examined has information relevant to a material issue in the action; (ii) the moving party has been unable to obtain the information from other examinable parties or the party who it seeks to examine; (iii) it would be unfair to require the moving party to proceed to trial without examining that person; and (iv) the examination will not cause delay, undue expense or unfairness. Wilkins J. found that the true identity and address for service for a defendant was sufficiently important, it was apparent that the plaintiffs could not obtain the information elsewhere, it would be unfair to force the plaintiffs to proceed without the defendant’s identity, and there was no unfairness to the ISP. His Honour therefore ordered iPrimus to provide that information. Rule 31.10 is one of the mechanisms in the Ontario Rules for obtaining this type of information. Other alternatives include a summons to witness on a pending motion, or simply bringing an application against the ISP. However, Rule 31.10 may be the most appropriate, given that what is sought is information from a third party.

The second important aspect of Wilkins J.’s decision is his comments about the way in which the test for forcing an ISP to reveal user information should be applied in the future. His Honour recognized that “implicit in the passage of information through the Internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed.”¹¹ He further states:

In keeping with the protocol or etiquette developed in the usage of the internet, some degree of privacy or confidentiality with respect to the identity of the internet protocol address of originator of a message has significant safety value and is in keeping with what should be preserved as being good public policy. As far as I am aware, there is no duty or obligation upon the internet service provider to voluntarily disclose the identity of an internet protocol address, or to provide that information upon request.¹²

This is a strong endorsement of anonymity for Internet users. Wilkins J. supports this by inserting another step in the analysis of determining whether the plaintiff is entitled to the defendant's identity. He states: "In the circumstances of the case at bar, the moving party has demonstrated on the affidavit material filed before me that it has a *prima facie* case as against Joe Doe in respect to the allegations of claim made in the Statement of Claim.

In my view, that is the appropriate test for the court to apply in determining whether or not to order a non-party internet service provider to disclose the identity of an internet protocol address."¹³ (emphasis added)

Justice Wilkins' decision appears to be a reasonable compromise. The court scrupulously protects the defendant's identity until the plaintiff can establish a *prima facie* case. This ensures that Internet users cannot be identified merely because someone dislikes what they are saying, but protects plaintiffs' access to the judicial process when they have a legitimate claim.

CURRENT ISP PRACTICE

ISPs that operate and web-based providers in Canada generally prohibit the use of Internet accounts for unlawful purposes that may incur civil liability, such as defamation. Many provide explicit privacy policies which pledge to protect the personal information of their users by refraining from transmitting this information without a user's knowledge or consent. However, most policies include the caveats that this information will be released if required by court order or subpoena or if the ISP is legally obligated to provide information, that the ISP will co-operate with legal authorities, or that the ISP will release information if it is required to identify or bring a legal action against a person. Other ISPs and web-based companies specify that they will not divulge personal information unless they "believe in good faith that the law requires it."¹⁴

LESSONS FOR INTERNET SERVICE PROVIDERS AND WEB-BASED COMPANIES

Hvide and *Aquacool* in the United States and *Phillips* and *Irwin Toy* in Canada demonstrate that, at a minimum, it is inadvisable for ISPs and web-based companies to disclose the identity of their members until they are served with a legally sufficient subpoena, court order or the third party discovery order. In addition to avoiding liability, this policy makes sound business sense: a company that provides little or no anonymity for its members will not be popular, as Internet users put a premium on privacy.¹⁵ This approach also respects the terms of privacy policies or contracts of service of most ISPs and web-based companies, reducing exposure to claims for breach of contract, false advertising or negligent misrepresentation (as alleged in *Aquacool*).

When a subpoena is issued or a motion is brought, another issue that arises is whether the ISP or web-based company should provide notice to its user before revealing his or her identity. This can be a vexing problem since the person seeking the information will often wish the fact of their subpoena or order to remain confidential. This is particularly true in the criminal context, where the police have a strong interest in maintaining confidentiality. However, it is equally true in civil cases, where the defendant may have physical evidence which the plaintiff may wish to obtain with an *Anton Pillar* order. On the other hand, there is a growing sentiment that it is unfair for the ISP or web-based company to disclose a subscriber's name without notice. Anonymity is considered by many in the Internet community to be a substantive right. Since the company generally has no interest in litigating to preserve a user's anonymity, the subscriber should have the right to do so him or herself. Hence, a prudent ISP or web-based company should provide notice to its users before releasing their identity, both to enhance its

relationship with its users, and to avoid a lawsuit such as the *Aquacool* litigation. The practice of the major Internet businesses (such as AOL¹⁶, Yahoo!¹⁷ and MSN) in the United States is to provide notice and allow 14 days for a member to attempt to bring a motion to quash a subpoena or bring a motion to prevent his or her identity from being disclosed. This approach was recently endorsed in the United States, where a court (for the first time) refused to automatically grant Dendrite International a subpoena to obtain user information from the ISP. Instead, the court required that the plaintiff company post legal notice on the same message board as the alleged defamatory comments had been posted to allow the online posters an opportunity to present arguments in court to block the subpoena.¹⁸

In circumstances where notice may undermine the purpose of the order (as would be the case for a search warrant or an *Anton Pillar* order), an option that could be considered is to advise the party seeking its subscriber's identity that its ordinary practice is to give the subscriber notice of the subpoena or proceeding, and give the plaintiff the opportunity to request an order that notice not be given. This allows the court, not the ISP or web-based company, to make the determination of whether notice is appropriate or inappropriate in the circumstances. Ultimately, a court order precluding the company from giving notice ought to be sufficient to protect ISPs in a subsequent legal action by a subscriber.

Finally, since there are no absolute requirements, the contracts between the company and its subscribers will be crucial in determining their respective rights. Hence, whatever the ISP or web-based company chooses to do when requests emerge, it should ensure that the promises made on their websites, in their privacy policies and in their contracts for service are consistent and realistic as to the level of protection the provider will provide for personal information.

PRE-LITIGATION PRACTICE

An important way for an ISP or web-based company to avoid litigation (or, at least liability) is to ensure that the terms and conditions of usages are set out clearly, well-known to its users, and as fair as possible. Hence, blanket statements such as "we will protect your personal information" or "we will not disclose your identity" should be tempered with words such as "unless we believe it to be required by law" or "subject to legal process or compulsion." It is also a good idea to ensure that notice provisions, whatever they may be, are clear to users. If the company is going to reveal identity without notice, they should say so. An attempt to give the impression of strict privacy controls can engender expectations and can create liability. Conversely, clear terms and conditions are the best protection against future liability.

Factors such as when the company will reveal information, what confidentiality obligations it will seek, whether it will give notice, how it will give notice, and whether notice will be given before or after the identity is revealed should be clearly specified. Needless to say, once a privacy policy has been established, it should be rigorously observed.

CONCLUSION

The expectation of anonymity on the Internet is powerful. As the issue of rights to anonymous speech play out in the courts, businesses in possession of information that can remove the cloak of anonymity will come under increasing pressure to either disclose or conceal that information. Since the business typically has no interest in either revealing or hiding the information, its primary concerns will be maintaining its reputation as a fair and safe place to be on the Internet, and avoiding subsequent liability. Every situation will ultimately depend on its particular facts, and net-based businesses are well-advised to consult their advisors when these issues arise. However, an excellent first step is a clear privacy policy that is fair, well-publicized and consistently observed.

[*Editor's note:* Andrew Bernstein is a litigation lawyer and member of the Technology Practice Group at Torys in Toronto. Tina Piper is a third-year law student at Dalhousie University.]

¹ This survey was conducted in the criminal context: in 1997 AOL was served with 33 search warrants and by 1999 that number had increased to 301 (an 800% increase) (Will Rodger, "Search warrants for online data soar," July 28, 2000, online: *USA Today* <www.usatoday.com/life/cyber/tech/cti289.htm> (date accessed: August 15, 2000)).

² The judgment became effective June 14, 2000, No. 99-22831-CA01, Fla. Cir., Miami-Dade Co.

³ C. S. Kaplan, "Judge Says Online Critic Has No Right to Hide" (2000) *Cyberlaw Journal*, online: New York Times <www.nytimes.com/library/tech/00/06/cyber/cyberlaw/09law.html> (date accessed: June 12, 2000).

⁴ Factum for the plaintiff in *John Doe, also known as Aquacool_2000 v. YAHOO! Inc., a Delaware corporation, and DOES I-9*, online: American Civil Liberties Union <www.aclu.org> (date accessed: June 10, 2000) at 6.

⁵ *Ibid.*, at 11.

⁶ *Supra*, note 4 at 12.

⁷ *Supra*, note 4 at 13.

⁸ Order to Weslink Data Corporation, *Philip Services Corp. v. John Doe I-26*, Wednesday June 24, 1998, Court File No. 4592/98.

⁹ S.C. 2000, c. 5, s. 7(3).

s. 7 (3) For the purpose of clause 4.3 of Schedule I, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(b) for the purpose of collecting a debt owed by the individual to the organization;

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

¹⁰ [2000] O.J. No. 3318.

¹¹ *Ibid.*, para. 10.

¹² *Ibid.*, para. 11.

¹³ *Ibid.*, para. 18.

¹⁴ See, for example, Yahoo!'s Privacy Policy, online: Yahoo! <<http://docs.yahoo.com/info/privacy/>> (date accessed: May 17, 2000) at 5.

¹⁵ ACLU amicus brief in *Hvide v. Does I-8*, online: American Civil Liberties Union of Florida <www.aaaclufl.org/body_hvideamicus.html> (date accessed: June 12, 2000).

¹⁶ AOL notifies members once a subpoena is received in a civil case who then have 14 days to attempt to block the subpoena. This practice is not specified in AOL's terms of service (*supra*, note 8).

¹⁷ Yahoo! has specifically stated, however, that it does not resist subpoenas issued to determine a member's identity. (M. Hedges, "Bad-mouthing businesses on the Internet can be risky," online: CJ Online Business News <www.cjonline.com/stories/072599/bus_badmouthbiz.shtml> (date accessed: June 19, 2000).

¹⁸ Aaron Elstein, "Dendrite International to Use Web as Post for Legal Notice", August 11, 2000, *The Wall Street Journal*, online: <<http://interactive.wsj.com/articles/SB965925940877307004.htm>> (date accessed: August 15, 2000).