# Electronic remarks may not be as anonymous as authors would like

By David Crerar

With a few keystrokes, a reputation can be ruined, a confidence broadcast to the world or sudden violence threatened, all under the cloak of electronic anonymity. As noted recently by the Ontario Court of Appeal in *Barrick Gold Corp. v. Lopehandia* [2004], O.J. No. 2329, the pervasive, instantaneous and yet permanent nature of Internet communications make the potential for damages caused by Internet mischief especially acute. Forensic techniques, coupled with logical extensions of discovery jurisprudence, allow the injured party to discover the identity of the anonymous sender, from nonparty sources.

The best source of discovery will be the Internet Service Providers, or ISPs, such as Bell, Telus, Shaw or Rogers. These companies maintain subscription information, as well as records of all e-mails sent on their servers. Companies that provide e-mail accounts, such as Yahoo!, AOL, and Hotmail, are another potential source of information. As these companies do not generally charge a fee for e-mail accounts, do not maintain billing records and do not verify customer names, they are less likely to be useful or reliable sources of information. The third source of information is the host website on which the offending communication has been posted. The hosts of chat-rooms, bulletin boards and similar web pages will often have information about the source of the postings on their sites; the available records and retention policies vary widely.

An offending e-mail or posting contains a wealth of hidden information. The header information of an e-mail, for example, reveals the sender's IP (for "Internet protocol") address (e.g. "24.71.223.140"), the accounts sending and receiving the e-mail, the server via which the e-mail was delivered, and the time the e-mail was sent and received. As each server that handles the message appends its own "trace field" to that message, the header information may reveal the entire path of the e-mail.

The IP address allows the next step of sleuthing. Various Internet reverse look up utilities, such as the WHOIS database at www.arin.net, can identify the company and server (usually an ISP) that has been assigned the given IP address. Because most ISPs dedicate specific IP addresses to specific geographic areas, it may be possible to determine the geographic location of the e-mail sender by city or town, or even as precisely as a radius of only a few blocks.

**"Canadian courts have thus practically and robustly applied paper-based discovery principles to new electronic spheres."**

The next step is contacting the ISP. A party should contact the ISP as soon as possible to ensure that the electronic records are preserved, for two main reasons. First, some ISPs, such as Shaw, retain their backup records with respect to specific e-mail communications for only a few weeks, after which the logs and backup tapes may be erased. Second, as with injunctions, a delay in applying to court will undermine the plaintiff's claim that the actions in question are a serious and urgent threat requiring judicial intervention.

Once one has obtained the header information, it is sensible to contact the ISP's in-house counsel, describe the concern and urgency, and forward the header information. The ISP is usually able to determine from the header information which customer sent the e-mail. An ISP does not assign each customer a unique IP address, but lends each customer a given IP address for a short period of time, usually between one week and six months. Thus the date and the IP address allows the ISP to cross-reference its records and determine which of its customers sent the e-mail at the specific time and date. The ISP's engineers can readily determine whether records exist concerning the communication in question. The ISP will usually be willing to confirm whether the records still exist and whether there is a name attached to the transaction. As ISPs are restrained by privacy legislation from divulging information concerning their customers, an ISP will almost always require a court order compelling it to release the information.

The next steps are thus legal. An applicant may unmask a John Doe through two possible procedures. First, one may seek a *Norwich Pharmacal* order, in which the ISP or non-party is the named defendant. Second, one may name John Doe as the defendant and proceed by way of non-party discovery rules (such as British Columbia Rules 26(11) or 28, or Ontario Rules 30.10 and 31.10). The John Doe route is the preferable procedure, as it does not require suing the ISP directly, it does not require multiple actions, and the legal test is usually simple to meet in the case of Internet tort.

Although such orders are now issued on a regular basis, reported decisions for Internet discovery are scarce, even after 15 years of widespread Internet and e-mail use. The leading decision comes from Ontario: *Irwin Toy Ltd. v. Joe Doe* [2000] O.J. No. 3313 (S.C.J.). There, the e-mail contained confidential files and defamatory comments. Justice Wilkins, in granting the remedy to the applicant, set down a general test. The applicant must show that the communication was *prima facie* tortious; that the applicant will likely be without a remedy unless provided the name of the holder of the IP address; and that the applicant has been unable to obtain the information from other persons. In the more recent decision in *BMG v. John Doe* [2005] F.C.J. No. 858, the Federal Court of Appeal set out a more relaxed test: the applicant need only prove a *bona fide* rather than *prima facie* case. Both courts took pains to emphasize that while the Internet confers no right of anonymity, courts must tailor orders such as to minimize the violation of privacy of non-party sources and their customers.

Note that a successful John Doe application does not always lead to the unmasking of the tortious sender. A sender can "piggyback" onto a nearby wireless server that the user has failed to secure; the IP address will lead back to the hapless piggybackee. Another dead end arises where the sender of the e-mail uses a public terminal, such as a library or an Internet café. Even here, however, further sleuthing may be possible through surveillance cameras or credit card records or user logs.

David Crerar

Canadian courts have thus practically and robustly applied paper-based discovery principles to new electronic spheres. A person posting a defamatory advertisement in a newspaper would enjoy no immunity from disclosure if the newspaper were compelled through discovery rules to reveal his identity; the same principle applies to a person who defames via the Internet. So long as a plaintiff acts swiftly and takes technical care in seeking redress through the means set out above, the judicial processes set out above offer a potential remedy and hope to an aggrieved plaintiff.

*David Crerar practises corporate and commercial litigation at Borden Ladner Gervais LLP, and serves as an adjunct professor at the University of British Columbia's faculty of law.*