

Blakes Bulletin

Intellectual Property – Social Media Series

Enforcing Intellectual Property Rights on Social Media

ANTHONY PRENOL

With the continued growth of social media, it has become increasingly important for businesses to augment their plans to protect their intellectual property (IP) by developing a strategy for addressing violations of IP and other rights that take place on portals, such as FACEBOOK, TWITTER and EBAY, or blogs.

The potential areas of concern are wide ranging. The following are just some examples of the violations of IP rights that can occur in social media:

- copyright infringement, such as the unauthorized use of text, images, videos and audio;
- trade-mark infringement or passing off, through the unauthorized use of a trade-mark for goods or services or a company name in comments on blogs or by impersonating a business;
- violation of personality rights, such as the impersonation of an individual;
- defamation, for example by false postings about a person on blogs;
- trade libel, such as by false postings about a product on blogs; and
- misuse of confidential information, through the disclosure of trade secrets by employees.

MONITORING ABUSES

Before any business can expect to enforce its IP rights on social media, it must develop a plan for detecting and monitoring abuses. Any good plan should involve educating employees and other representatives of the business on the importance of reporting any abuses of the IP rights of the business, and conducting searches on a regular basis for infringing activities.

The sheer volume of postings and other communications on social media has made it extremely difficult to keep pace with violations. For example, infringing copies

of copyrighted works can be accessed and shared by thousands, or even millions, of Internet users.

It is therefore important to bear in mind that not all infringements are of equal concern. For example, many blog postings have a short shelf life, read by only a small number of people before being superceded or buried by more recent postings. Some postings, however, are very influential and are read by many people.

In some cases, a posting may be viewed many times because it is posted on a blog that has a wide readership or is otherwise influential. In other cases, a posting may be made on a site that does not have wide readership but the posting may attract additional readers because other users link to it or forward it to others, or the posting is picked up by traditional media, such as newspapers.

For these reasons, more and more companies are turning to online media monitoring services for help in tracking infringements and other violations of their IP rights. These services not only track references to a business across a wide variety of social media – including hundreds of social networking websites that may not appear in searches conducted on popular search engines – but also provide invaluable information on trends.

For example, a good media monitoring service can detect a sudden surge in comments on a particular company, such as postings to the effect that one of the company's products has been recalled or that the company may be in financial difficulty. Obtaining real-time information can often allow a company to take effective measures to prevent or limit violation of its rights.

COLLECTING EVIDENCE

Monitoring violations of IP rights includes collecting and maintaining evidence of these abuses for use at a later date. The fleeting nature of social media is both a curse and a blessing for rights holders. The blessing is that content that violates rights might be deleted from social media sites before they have been widely viewed, downloaded or shared.

CONT'D ON PAGE 2

CONT'D FROM PAGE 1

The curse is that it can be very difficult to prove, at a later date, a violation that took place in the past but which has left precious little trace in its wake. For this reason, it is crucial that an IP rights holder take immediate steps to record and preserve evidence of infringing activity so that it can, if needed, provide evidence at a later date to establish that a violation occurred.

When a business takes steps to preserve evidence of infringement, it should consider who will likely be in a position to give evidence at a later date. For example, it can be advantageous to centralize the gathering of evidence of infringement so that evidence can, at a later date, be adduced through one or two witnesses rather than requiring a multitude of witnesses, each of whom will only testify as to one or two instances of infringement.

IDENTIFYING INFRINGERS

Once a business determines that its rights have been violated, the next step is to identify the infringer so that appropriate action can be taken. The anonymous nature of social media can make it difficult, but not impossible, to identify infringers.

In the case of a violation by an anonymous person, an IP owner will typically turn to the remedy of an equitable bill of discovery or to federal and provincial rules of civil procedure to obtain a court order requiring a third party, such as an Internet service provider, to disclose identifying information about the infringer. The reaction of Canadian courts to applications of this nature has been somewhat uneven.

In *Mosher v. Coast Publishing and Google*, the chief of the Halifax fire department sought a court order requiring the publisher of a newspaper to disclose information about two respondents that the applicant believed would lead to the individuals who authored allegedly defamatory statements in the newspaper. Both the publisher and Google advised the court that they would not appear in opposition to the application and that they would obey any order issued by the court.

The Supreme Court of Nova Scotia judge who heard the application granted a disclosure order, noting that "the court does not condone the conduct of anonymous internet users who make defamatory comments and

they like other people have to be accountable for their actions."

However, only a month later, in *Warman v. Wilkins-Fournier*, a three-judge panel of the Ontario Superior Court of Justice took a stricter view of an application for a disclosure order. The plaintiff sued for defamation with respect to messages posted by eight defendants, under pseudonyms, on an Internet message board.

The operators of the message board permitted registered users to post messages on various political and social topics. The plaintiff sued not only the eight posters, whom it named as John Does in its Statement of Claim, but also the administrators and moderators of the message board.

The plaintiff sought from the operators of the message board the Internet Protocol addresses for the allegedly defamatory postings made by the John Doe defendants as well as the email addresses with which they registered as users of the message board and any subscriber data that they provided at the time of registration.

The plaintiff took the position that it needed this information so that it could identify the John Doe defendants and serve them with the statement of claim. The judge who heard the application for a disclosure order at first instance granted the requested order.

On appeal, the court considered submissions not only from the appellant operators of the message board but also from two intervenors, the Canadian Civil Liberties Association and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. The primary issue before the court on appeal was whether, and to what extent, the court should consider privacy concerns when faced with a request for a disclosure order.

The court had no difficulty in concluding that an individual's right to privacy was protected under the *Canadian Charter of Rights and Freedoms*. The court then went on to hold that, in order to prevent the abusive use of the litigation process, disclosure should not be automatic where Charter interests are engaged. At the same time, the court also commented that, even if Charter interests are at stake, disclosure cannot be unreasonably withheld if it is required to prevent the "abusive use of the internet."

CONT'D ON PAGE 3

CONT'D FROM PAGE 2

The court then held that the judge who heard the plaintiff's application for a disclosure order should have considered the following factors:

- whether the unknown alleged wrongdoer could have a reasonable expectation of anonymity in the circumstances;
- whether the plaintiff had established a *prima facie* case against the 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.

Going forward, a plaintiff seeking a disclosure order would be well advised to ensure that its evidence meets the stricter standard imposed by the *Warman* decision.

CONCLUSION

Enforcing IP rights on social media might at first blush appear daunting. However, with the development and implementation of a monitoring strategy for infringements on social media and by remaining familiar with the standards being imposed by Canadian courts for disclosure orders, an IP owner will be better positioned to enforce its rights.

Use of Social Media in Dispute Proceedings

ALAN AUCOIN

Whether one “tweets,” “friends” or otherwise communicates on any of the many social networking websites available for personal or business communications, you should realize that what is said, posted or received may be used in the course of court or arbitral proceedings.

Social networking is now an integral part of our communication tool box and has greatly facilitated the exchange of information. However, it has also expanded the scope of accountability in a way that paper trails seldom do. Depending upon the importance of the issues or money at stake, these are trails that litigation will inevitably explore and expose.

This article briefly considers the way in which core aspects of dispute resolution have been affected by social media, namely notice; preservation, production and discovery of documents; and the use of documents in a court or arbitral proceeding.

NOTICE OF LEGAL PROCEEDINGS

Historically, notice of an originating legal proceeding had to be served personally or by a limited number of alternatives to personal service. Depending upon the facts and the need for immediate court response, any method of bringing the proceeding to the recipient’s attention is acceptable if it can be demonstrated that there is a high probability of the notice being received. The reason for these procedural safeguards is to ensure fairness and provide the recipient with an opportunity to be heard.

In the event that the proceeding goes forward in the absence of the recipient, the result can be set aside if it can be demonstrated that the notice had not come to the recipient’s attention through no fault of the recipient.

Canadian courts have always had jurisdiction to order service by a non-routine method, called substituted service, where it was impractical to effect prompt personal service or where it was necessary in the interests of justice to do so.

Even if an order for substituted service is not obtained in advance, courts can always validate service, provided that it can be established that the recipient

received such notice and was attempting to evade service. However, even where evasion has not been an issue, courts have validated service where it can be demonstrated that notice came to the attention of the recipient.

As technology evolved, alternatives to personal service began to include the postal system, facsimiles and couriers. Recent case law in Canada, the United States, the United Kingdom, Australia, New Zealand and other countries demonstrate how quickly the courts have moved from the traditional methods of notice to the point where social networking sites are now seen as a reasonable alternative to providing notice in legal proceedings.

Given the manner in which social media sites are rapidly becoming the modern version of the town square or village meeting place, it is not surprising that the courts have recognized service via such sites in appropriate cases. For example, one U.K. court recently allowed a plaintiff to serve a summons on a debtor through substituted service via FACEBOOK.

PRESERVATION OF DOCUMENTS AND E-DISCOVERY

The failure to maintain documentary evidence that could have a bearing on a dispute has attracted much attention in the age of electronic evidence. The consequences of being found to have not protected relevant documents can be disastrous and, in some cases, may result in a court taking an adverse inference towards the party at fault.

When the only records were “hard copies”, it was relatively easy to identify, segregate and preserve documents for the purposes of litigation. The volume, speed and variety of ways of transmission of electronic messages make it a daunting task for litigants when it comes time to identifying, preserving and producing such information.

The rules of civil procedure of Canadian courts recognize wide definitions of “documents” for the purposes of disclosure and production to the other side. For example, the Ontario *Rules of Civil Procedure* provide that a “document” includes a sound recording, videotape, film, photograph, chart, graph, map, plan, survey, book of account, and *data and information in electronic form*.

CONT'D ON PAGE 5

CONT'D FROM PAGE 4

The Ontario Rules also provide that a document shall be deemed to be in a party's power if that party is entitled to obtain the original document or a copy and the party seeking it is not so entitled. This has wide-ranging consequences for users of social media where the content is relevant to a legal proceeding. For example, a document posted by a third party on one's FACEBOOK page may have to be produced.

E-discovery has spawned an entire industry of service providers and software products to deal with the identification, production and examination of relevant electronic documents. In many cases, the indiscriminate and wide use of emails and messaging systems has made it next to impossible for a litigant (let alone their lawyers) to "sift the wheat from the chaff."

Several Canadian decisions have ordered the disclosure and preservation of information from social networking sites. Such disclosure is dependent upon the probative value of the information being requested, provided that disclosure does not infringe reasonable expectations of privacy. For example, a plaintiff claiming to be suffering from chronic pain may be faced with contradictory FACEBOOK pictures.

A person who posts something on an unrestricted social networking page has no reasonable expectation of privacy. There have already been several Canadian decisions in which courts have ordered the disclosure and preservation of information from social networking sites, such as FACEBOOK pages.

Disclosure has been ordered where the probative value of the requested information would not violate a reasonable expectation of privacy. However, this requires an examination of the reasonable limits of each request. Even where the information is contained in the "private" portion of a profile, numerous friends may have access to see and further disseminate the information so that such private portions may be subject to discovery.

There is a movement in Canadian dispute proceedings to limit the scope of discovery by imposing notions of proportionality. In other words, there are reasonable limits that will be imposed on requests for information of any type, including pictures, records, messages that might be found on social networking sites.

Even though proportionality values may ultimately rule out the use of many electronic documents, a litigant is still responsible for determining the existence of relevant documents and ensuring that such documents are not destroyed pending such a determination.

INTERNET EVIDENCE

Most websites are dynamic, both in content and operation. In some cases, reference to a live website is better evidence than a print copy. A court can see the contents, including documents as they exist, or may have existed, on the Internet and can see features such as hyperlinking, metatagging, and interactive streaming that cannot be realistically reproduced on paper.

There is no particular magic in information obtained on the Internet. If the information would be admissible on a rule of evidence, the fact that it is obtained on the Internet is not determinative. Online articles, websites and definitions are admissible as evidence of information which is available to the general public. Information on foreign websites that are accessible domestically may also be admissible.

On the other hand, the mere fact that the information is publicly available on the Internet and readily producible does not make it reliable. Such information must still satisfy the normal tests for admissible evidence. The weight given to such evidence must be carefully evaluated because the source is often unknown or the credibility untested. Courts must view evidence located on the Internet warily, and the record of such evidence must be sufficiently developed to provide an adequate factual underpinning.

In litigation relating to Internet activities, it is often necessary to provide evidence as to the content of a website at a particular point in time. The caching and archiving of websites result in evidence being recorded and available long after content is deleted from a live website.

A commonly used source for historical views of websites is the WAY BACK MACHINE, located at «www.archive.org», which contains a library of archives of Internet websites. Canadian decisions have not been uniform on the admissibility or reliability of evidence from the WAY BACK MACHINE, although some cases have accepted such evidence without comment.

CONT'D ON PAGE 6

CONT'D FROM PAGE 5

The issue of whether counsel can access content on social networking websites in the context of a dispute has been considered by various bar committees in the United States. A lawyer may not be permitted to cause a third party to access the social networking website pages of an individual to obtain information that might be useful for impeaching that individual's testimony at a trial where those pages are generally accessible only with the permission of the individual through a "friend". This would constitute of a false statement to a third party for which the lawyer would be responsible.

However, a lawyer representing a client in pending litigation may access the public pages of another party's social networking website for the purpose of obtaining possible impeachment material for use in the litigation, provided that the lawyer does not employ deception in any way, such as by becoming a member of the target's network or in "friending" the person.

CONCLUSION

In the same manner that e-mails may become relevant as documents and must be preserved in litigation, one must expect that information posted on social networking sites is potentially just as relevant. The lines between "public" and "private" information can be erased if relevance can be shown or inferred by the court or arbitrator.

Go to blakes.com/english/subscribe.asp to subscribe to other Blakes Bulletins.

NEW YORK CHICAGO MONTRÉAL LONDON OTTAWA BAHRAIN TORONTO AL-KHOBAR* CALGARY BEIJING VANCOUVER SHANGHAI* blakes.com
* Associated Office