Blake, Cassels & Graydon LLP December 2010

Blakes Bulletin

Intellectual Property/Information Technology
Social Media Series

Defamation Risks from User-Generated and Other Online Content

TONY WONG

INTRODUCTION

The Internet provides seemingly endless opportunities for organizations to market and promote their goods and services and to build customer loyalty. An understanding of the law of defamation is vital to ensure that an organization's online activities do not result in real-world legal liability.

Most organizations have an Internet presence, such as a website, FACEBOOK pages, and TWITTER accounts. Some allow their customers to post comments or other user-generated content (UGC) on the organization's website. In taking advantage of these opportunities to engage customers, an organization must keep in mind that the law of defamation applies fully to all its online activities.

ELEMENTS OF DEFAMATION

Defamation is a civil claim available to an individual or organization where each of the following three elements are present.

1. Publication to a third party. The defamatory statement must be communicated to a person *other than* the subject of the statement. Practically speaking, if the statement has been posted online, this requirement will be met. The publication can take a variety of different forms including an article, a press release, an advertisement, a photo, a video, a speech or UGC. Regardless of form, the publication may give rise to liability for defamation.

A "publication" posted on a website need not be prepared or approved by the website operator to give rise to liability for defamation. All those involved in the publication or dissemination of the defamatory statement may be personally liable. What this means is that if a website operator hosts UGC, or allows a user to post a comment, article or video on the website, the operator can be held liable because the operator has been involved in its dissemination.

2. Publication about identifiable individual. A publication must be about an identifiable individual or organization to give rise to liability for defamation. One cannot necessarily avoid a defamation claim by not using a name in a publication. The question in every case is whether the person or organization can be identified in the publication by a reasonable person. Information such as an address, job title, or other publicly known characteristic can be used by a reasonable person to identify an individual or organization even without a name.

3. Publication harms reputation of identified person. A publication is defamatory if it harms the reputation of the individual or organization identified in it. This is a low threshold. For example, it is defamatory to say that someone is incompetent, dishonest, negligent, abusive, greedy or mentally unstable.

If all three of these elements are present, a defamation claim is available and the onus shifts to the person who prepared or disseminated the comment to establish one of the available defences to defamation.

DEFENCES TO DEFAMATION CLAIM

A number of defences are available to a claim for defamation. Some of the defences that are likely to be relied on in the context of online defamation are summarized below.

Truth

Truth is an absolute defence to a defamation claim. If a person can prove that the published statement is substantially true in its natural and ordinary meaning, the person cannot be successfully sued for defamation.

The publisher of a defamatory statement bears the onus of proving that it is substantially true. Proving truth is often difficult, particularly if a person did not prepare or author the statement in issue, i.e., user comments or other UGC. What is generally required to prove truth is evidence of a nature that would be acceptable in a court, such as a witness to an event, a video that can be verified as authentic, a government record, or an admission by the subject of the statement.

CONT'D ON PAGE 2

CONT'D FROM PAGE 1

What is not sufficient to prove truth is a rumour, even if it is widespread in the community. Nor is it generally sufficient to establish truth to say that others have made a similar statement earlier and that one is simply "repeating" what was said earlier – for example, retweeting another's tweet on TWITTER. If rumours or allegations are all that a person has to prove what he/she has published, that person is unlikely to succeed on a truth defence.

Fair comment

Fair comment is a defence that is available to a claim for defamation based on the publication of a defamatory comment or opinion. A defamatory comment or opinion may be protected by fair comment, even if it is not true or reasonable, provided that all of the four following criteria are satisfied.

1. Matter of public interest. The comment or opinion must relate to a matter of public interest. What is a matter of public interest is a very broad concept. A matter is of public interest if it affects people at large so that they may be legitimately interested in what is going on or what may happen to them or to others. A person who comes forward prominently into the public realm may also be a matter of public interest.

2. Based on true facts. The comment or opinion must be based on facts in existence at the time of the publication and either set out in the publication or generally known by the public. These facts must be proven to be true. It is not good enough that the publisher believed the facts to be true.

3. Recognizable as comment. The fair comment defence protects statements of comment or opinion, not fact. To rely on this defence, the statement in issue must be presented as opinion or comment rather than fact. Use of words such as "in my opinion", "it seems to me" or "my view is" will likely be effective in identifying the statement as a comment or opinion rather than fact.

4. Honestly based on facts. To succeed on a fair comment defence, the publisher must prove that the comment or opinion is one that any person could honestly hold based on the proven facts. This is a low threshold. It is not necessary to prove that the comment or opinion is "fair" or "reasonable" because not all persons hold opinions that are fair or reasonable.

Innocent Dissemination

The "innocent dissemination" defence may potentially be available to protect a website operator against liability for UGC posted on its website in certain limited circumstances.

The "innocent dissemination" defence has traditionally been available as a defence to a defamation claim where a person has played a subordinate role in the publication of defamatory material if that person can prove that: (i) it did not know or suspect that it was distributing defamatory content; and (ii) it ceased distributing, or removed, the defamatory material upon being put on notice of the alleged defamation.

In the context of the Internet, it has been argued that the innocent dissemination defence is available to protect against a defamation claim relating to UGC on a website where: (i) the website operator does not review comments prior to posting on the website; and (ii) the operator removes the UGC immediately upon being put on notice that it may be defamatory.

The two requirements for relying on the innocent dissemination may appear easy to satisfy in practice but carry with them significant reputational risks. Absent review of user comments prior to posting, the operator loses control of what content appears on its website, which is commercially risky. Further, removing user comments too quickly may expose the operator to complaints of censorship. Because of these risks, many organizations that open their websites to user comments choose to forego the steps necessary to qualify for the innocent dissemination defence, even if it might be available.

There is no statutory recognition of the innocent dissemination defence as there is in the United States' *Communications Decency Act*. The British Columbia Court of Appeal appears to have implicitly accepted this defence in *Carter v. B.C. Federation of Foster Parents Association,* which related to defamatory user content in a forum or chatroom. However, the availability of the innocent dissemination defence to protect against defamation claims arising from user comments has not yet been recognized in other provinces.

CONCLUSION

If a business uses a website, a blog, a social networking website such as FACEBOOK or TWITTER, or any other social media to market its goods or services, it is vital that it do so with knowledge of the law of defamation. Without such knowledge, a promising marketing opportunity can quickly turn into a costly and time-consuming defamation claim.

Blakes Bulletin
December 2010
Intellectual Property/Information Technology
Social Media Series

Copyright Issues in User-Generated Content and Scraping

DAPHNE MARAVEI

User-generated content (UGC) has become one of the key components of the Web 2.0 environment. UGC raises a number of issues and risks relating to copyright and screen scraping.

UGC includes content contributed by users on wikis, blogs, discussion forums and social networking websites (see our September 2010 *Blakes Bulletin on Intellectual Property*). UGC includes text, such as product reviews and blog comments, photographs, videos and music, as well as combinations, or "mash-ups", of any one or more of such media. The widespread and increasing popularity of Web 2.0 has led many organizations to promote or permit the posting of UGC on their own websites and their pages on social networking websites.

The proliferation of frequently accessible and easily navigated websites that simplify the posting and sharing of content from a wide range of sources has lead to heightened concerns for copyright owners and may expose website operators to risks of copyright infringement for the posting of UGC on their websites.

COPYRIGHT INFRINGEMENT

Not all content is subject to copyright. The minimum standard that must be met for a work to qualify for copyright protection is "originality". Originality has different standards in different jurisdictions. By way of example, in Canada, for a work to be considered original and therefore attract copyright, it must be the product of the author's exercise of skill and judgment. Creativity is not a condition of originality.

Assuming that copyright subsists in a work posted by a user, ownership of copyright in the work may be owned:

- entirely by the user based on authorship and/or the acquisition of title by the user;
- by both the user and one or more other parties as a result of authorship and/or acquisition by one or both;
- by the user as the result of the adaptation of content owned by a third party into a new original derivative work; or
- by one or more third parties and not at all by the user.

While each category raises legal concerns, the last two pose the most risks for copyright infringement in the Web 2.0 context given that a person other than the user may have rights in the posted work or a work from which the posted work is derived.

If neither the user nor the website operator owns, or has an applicable licence to, the copyright in UGC, the posting or transmission of the content may constitute infringement of copyright resulting from the violation of one or more component rights. Depending upon the jurisdiction, these may include the rights of reproduction, communication to the public, making available, public performance, and distribution. Posting UGC may also infringe neighbouring rights related to performers' performances, sound recordings and broadcasts.

CANADIAN COPYRIGHT REFORM

United States and European law provide website operators with immunity from, or safe harbours for, copyright infringement for UGC in certain circumstances. Canadian copyright law does not currently provide the same protection (see *Risks of User-Generated Content to Website Operators*, on page 6 of our November 2010 *Blakes Bulletin on Intellectual Property*).

The proposed 2010 amendments to the *Copyright Act* in Bill C-32 (see our June 2010 *Blakes Bulletin on Intellectual Property*) would immunize Internet users and website operators for UGC in certain circumstances.

The Bill proposes that it would not be copyright infringement to use the work, combine it in a new work, or authorize dissemination by an intermediary, such as a website operator, provided that:

(i) the name of the author is referenced, if reasonable to do so;

(ii) the person who deals with the work has reasonable grounds to believe that the existing work or a copy of it does not infringe copyright;

(iii) such activity is done solely for non-commercial purposes; and

(iv) the activity does not have a substantial adverse effect, financial or otherwise, on the exploitation of the existing work or a market for it.

CONT'D ON PAGE 4

CONT'D FROM PAGE 3

Examples of permissible activities provided on a Government of Canada website about the Bill include the making of a home video of a friend dancing to a popular song or creating a "mash-up" of video clips and posting them online.

It would also not be infringement merely to provide digital memory in which another person stores a work for the purpose of allowing its telecommunication through the Internet. However, immunity would not be available if the person providing the digital memory knows of a court decision holding that the person who stored the work infringes copyright by making the copy or using the work.

SCREEN SCRAPING

"Web scraping" or "screen scraping" is the extraction of data from another person's website by way of a computer program and the aggregation of such data in a commercially valuable form. Some web-scraping software is very sophisticated and essentially simulates clicks to drill down through a web page and collect data from a website in a very short period.

Typically, a screen scraper accesses the website of the target, electronically reads and copies information from the displayed web page, and then aggregates and redisplays the information on its own website. The aggregator may provide price comparisons, be a competitor of the target, or be a reseller of the target's products or services. A screen scraper attempts to leverage the compiled data to profit from the increased traffic.

Scraping is popular among price comparison and other intermediary websites, such as in the travel or consumer goods industries, whose operators find it a quick and inexpensive method of collecting large amounts of data that are subject to constant, and often daily, fluctuations.

However, scraping may not be permissible in all situations. Website operators have sued, and in some cases prevailed against, third parties that use scraping software to extract pricing or product information, claiming that such actions constitute copyright infringement, trespass to the website operator's computer systems, violation of computer misuse statutes, and breach of the operator's terms and conditions.

For example, a discount airline, Ryanair, sued German defendants in an Irish court in response to what it alleged was unauthorized scraping and "mis-selling" of tickets from Ryanair's website. The defendants argued that the Irish court did not have jurisdiction.

Ryanair argued that, by reproducing content from its website without permission, the defendants violated the terms and conditions which prohibit third parties from using its website for commercial purposes. Ryanair also argued that the defendants' conduct breached its intellectual property rights, including its copyright and database rights.

The court held that a contract existed between Ryanair and the defendants because the latter agreed to the terms and conditions which were prominent on the website. The relevant terms and conditions stated that the Irish courts alone had exclusive jurisdiction to deal with any dispute between the parties. The consideration provided by Ryanair for the contract was making the information available on its website.

In contrast, a claim under the United States *Computer Fraud and Abuse Act* based on the scraping of data failed because the court said that the scraped data was not protected by restrictive password access, restrictive terms and conditions of service or in any other manner that would make access to the data unauthorized.

These decisions highlight the importance for website operators to have appropriate terms and conditions in place.

TERMS AND CONDITIONS

Scraping and UGC copyright issues raise the question as to how a website operator can protect the data available on its website and protect itself from copyright claims from third parties. No single solution will eliminate all risks, however, there are some strategies available to a website operator. An operator should consider the following in adopting terms and conditions:

- include a notice that copyright and other intellectual property rights, such as trade-marks and, in some jurisdictions, database rights, are proprietary to the website operator;
- include a provision requiring that users own, or at least have an appropriate licence in, the copyright in the content they post;

CONT'D ON PAGE 5

CONT'D FROM PAGE 4

- specify the nature of the licence in posted content that is granted to the operator by the user and providing that such licence covers all uses that the operator foresees that it and other users will make of the content;
- alternatively, depending on the circumstances, provide that copyright in the UGC vests in the operator. However, this may not be sufficient to effect an assignment of copyright in some jurisdictions. This may also expose the website operator to liabilities and reduce or eliminate the availability of certain defences;
- stipulate that only non-commercial use of information posted on the website is permitted and that users of the website are deemed to be bound by a licence agreement prior to making use of website information;
- prohibit or limit screen scraping or any other unlicensed activities by expressly stating that the use of a robot, spider, scraper or any other fully automated means of accessing the website for any purpose, including screen scraping, is prohibited;
- ensure that the terms and conditions are clearly worded, clearly visible and brought to the attention of users before they access the UGC or commit to buying goods or services; and
- review the terms and conditions regularly to ensure that they are current and relevant to the content posted on the website.

CONCLUSION

A website operator should carefully consider terms and conditions on its website to reduce the risks of copyright infringement for UGC and the right of others to scrape and reuse valuable data.

Blakes Bulletin
December 2010
Intellectual Property/Information Technology
Social Media Series

Risks of User-Generated Content to Website Operators

SHELDON BURSHTEIN

User-generated content (UGC) on websites raises many legal concerns because of its sheer volume and numerous sources. Canada does not afford the same protection to website operators for UGC as other major jurisdictions.

UGC includes not only content on video-sharing sites such as YOUTUBE, but also product reviews and contest submissions on business websites (see our September 2010 *Blakes Bulletin on Intellectual Property*). UGC may be immediately responsive and is usually not subject to journalistic or organizational filtering. Often, the source of UGC is anonymous or is falsely identified.

Therefore, the operator of a website which enables the publication or dissemination of UGC may be exposed to risks relating to UGC, including UGC posted by persons with whom it may have no connection. These risks include intellectual property infringement, defamation, misleading advertising and other torts.

Currently, there is no specific statutory protection available to website operators for UGC liability in Canada, except in the province of Quebec, but proposed amendments to the Canadian *Copyright Act* contemplate immunity from copyright infringement. The legislative immunities and safe harbours available to website operators for UGC liabilities in the United States and Europe highlight the risks to website operators in Canada.

In the United States, where a website operator acts passively, it may be immunized by the *Communications Decency Act* (CDA) against all claims except the infringement of federal intellectual property rights. The operator may be protected against copyright infringement claims by the *Digital Millennium Copyright Act* (DMCA) safe harbour.

In Europe, the *E-Commerce Directive* exempts certain website operators from liability for UGC where the operator has neither knowledge nor control over the content transmitted or stored.

UNITED STATES DIGITAL MILLENNIUM COPYRIGHT ACT

Section 512 of the DMCA provides a safe harbour from copyright infringement for a qualifying website operator with respect to content stored on its website at the direction of a user.

To qualify, a website operator must be a "service provider" (SP), as defined in the DMCA. Based on the definition, SPs include classic Internet access service providers, web-hosting providers, operators of search engines, online auction sites, wikis, blogs, social networking sites, virtual worlds and more conventional websites that allow the posting of UGC.

An SP is not liable for monetary relief or, except in limited circumstances, for injunctive or other equitable relief for the infringement of copyright by reason of the storage, at the direction of a user, of material, such as UGC, that resides on a system or network controlled or operated by or for the SP. As preconditions to qualify for this safe harbour, an SP must:

- designate, and post contact information for, an agent to receive notification of alleged infringement;
- provide the agent's contact information to the United States Copyright Office;
- implement and disclose a copyright infringement policy and "notice and takedown" procedures;
- establish and disclose a repeat offender policy, whereby the SP terminates the accounts of users who repeatedly infringe copyright; and
- accommodate, and not interfere with, standard technical protection measures used by copyright owners to identify or protect copyrighted works.

In addition, with respect to particular material which is alleged to infringe copyright, the SP must:

- have no actual knowledge that the material, or any activity with the material, on its system or network infringes copyright and not be aware of facts or circumstances from which the alleged infringing activity is apparent;
- receive no financial benefit directly attributable to such activity, where the SP has the right and ability to control such activity; and
- expeditiously remove, or disable access to, the material upon obtaining knowledge or becoming aware of such activity, or receipt of notification of an infringement claim.

CONT'D ON PAGE 7

CONT'D FROM PAGE 6

Viacom v. You Tube illustrates the application of the DMCA safe harbour. You Tube regularly removed videos from its website upon the receipt of takedown notices under the DMCA for particular works. However, the court held that You Tube was not liable for copyright infringement for the tens of thousands of videos available on its website which allegedly infringed the copyright of the plaintiffs but which had not been specifically identified in notices. The court held that a website operator is entitled to safe harbour protection in the absence of notice of specific and identifiable infringing works because the actual knowledge requirement is applicable to each work.

UNITED STATES COMMUNICATIONS DECENCY ACT

Section 230 of the CDA stipulates that no provider of an "interactive computer service" (ICS) shall be treated as the publisher or speaker of any information provided by another "information content provider" (ICP).

To qualify for such immunity, a website operator must be an ICS, namely an information service, system or access software provider that provides or enables computer access by multiple users to a computer server. A website operator whose site permits the posting of UGC is an ICS.

An ICP is a person who is wholly or partially responsible for the creation or development of information provided through the Internet.

Eligibility for immunity under the CDA depends on the source of the information. If a website passively displays content that is created entirely by third parties, the CDA protects the operator from liability that would otherwise apply as a result of such publication, including in cases alleging defamation, fraudulent and negligent misstatement, misleading advertising and other torts.

Immunity is generally available where the ICS restricts its activities to traditional editorial functions or merely forwards content without making a material contribution. Immunity is also available to website users who post content from another source.

The CDA excludes immunity for the infringement of federal intellectual property rights, such as trade-mark and copyright infringement. However, immunity may be available for related claims, such as the violation of state trade-mark rights and rights of publicity.

An ICS does not enjoy immunity for content which it wholly or partially creates or for which it is responsible. *Doctor's Associates v. QIP Holder* illustrates that it is not always easy to draw the line between active and passive involvement.

In an advertising campaign for the QUIZNOS restaurant chain, QIP Holder (Quiznos) invited consumers to post videos on a dedicated website demonstrating "why you think QUIZNOS is better" by comparing the amount of meat in a particular QUIZNOS sandwich to a similar SUBWAY sandwich. QUIZNOS posted four sample videos created by its agency to assist the contestants.

When Doctor's Associates (Subway) sued for false advertising, QIP unsuccessfully moved for dismissal on the basis that it was immune under the CDA. The court said that it was "unclear" whether Quiznos went beyond the role of a passive publisher by actively soliciting the videos and shaping their content. The case was settled shortly after.

EUROPEAN E-COMMERCE DIRECTIVE

In Europe, the *E-Commerce Directive* exempts a website operator that qualifies as an "information society service" (ISS) from liability for UGC where the ISS has neither knowledge nor control over the content transmitted or stored. An ISS is defined similarly to an ICS under the CDA. To benefit from the limitation on liability, the ISS must comply with the Directive.

A website operator is exempt from liability where the operator does not play an active role of a kind which gives it knowledge of, or control over, the data stored on its system. However, if its role becomes more than technical, automatic and passive, liability may attach. An ISS must act expeditiously to remove, or disable access to, content upon receipt of actual knowledge or becoming aware of illegal activities.

CANADA

There is no Canadian federal legislation that corresponds to the CDA or DMCA. However, the proposed 2010 amendments to the *Copyright Act* in Bill C-32 (see our June 2010 *Blakes Bulletin on Intellectual Property*) would provide limited immunity in respect of copyright infringement (see also *Copyright Issues in User-Generated Content and Scraping* on page 3 of our November 2010 *Blakes Bulletin on Intellectual Property*).

CONT'D ON PAGE 8

Blakes Bulletin
November 2010
Intellectual Property/Information Technology
Social Media Series

CONT'D FROM PAGE 7

QUEBEC

Quebec is the only Canadian province which provides statutory protection to a website operator for UGC. The Quebec *Act to Establish a Legal Framework for Information Technology* provides that a service provider who acts as an intermediary in providing content storage services on a communication network is not responsible for the activities of the service user with documents stored by the user or at its request.

The provider is not immune from liability for such storage if, upon becoming aware that the documents are being used for an illicit activity, or of circumstances that make such use apparent, the provider does not act promptly to block access to prevent the activity. However, a provider is not required to monitor content stored or communicated on the network or to identify circumstances indicating that the content is used for illicit activities.

CONCLUSION

The risks to website operators for UGC in Canada may require operators to exercise vigilance over UGC postings on websites that may be governed by Canadian law.