HISCOX

encourage courage™

Making social media work for you.

Eight tips for reducing social media legal risks.

Introduction

Facebook, Twitter, Instagram and other social media applications have become indispensable tools for business, as companies and their employees regularly engage directly with the public (that is, customers, potential customers and even competitors), actively 'sharing' information across various social media platforms. The viral nature of social media makes it a cost-effective and therefore particularly appealing way for businesses to market their products and services, and companies now regularly conduct much – and sometimes all – of their business online. While social media has facilitated many positive changes in the way information is gathered and shared, potential challenges arise in the use of these platforms. The discussion that follows identifies some of the legal risks unique to social media, and offers eight practical tips for minimizing them.

Contents

Tip #1. Think before you post: defamation and Section 230 of the CDA

Issue

The inherent brevity of platforms such as Twitter and Facebook presents a number of advantages, including that readers have virtually immediate access to pithy updates on events, people and topics they are following. These advantages, however, also present a sobering downside: the spontaneity and brevity together create a unique potential for defamation. Statements published to friends, followers, or connections online that arguably harm the reputation of a third-party may result in legal action against the poster of the statement and his or her employer.

And because tweets, Facebook posts and other equally brief online statements inherently provide far less context than would a full-length article or a comprehensive marketing brochure, it may be difficult for the poster to demonstrate that he or she is entitled to the protection of some of the legal privileges and defenses available to a traditional publication. Put simply, while traditional publications often include potentially harmful 'zingers' within longer communications that give them context, tweets and posts often include only the zinger. It therefore is particularly important to 'get the facts right' in social media – to think before one posts. One may not mean to be taken literally when one posts a quick comment on someone else ('He's a crook'), but when the three-word comment has no context, others may take it literally, and the subject may take it quite seriously!

This is particularly so because of the inability to truly 'untweet' or correct a statement once made via social media, even if the tweet or post contained an unintended error. Such posts, even if deleted, can be pulled and re-posted, or re-tweeted by other individuals, and thereby subject the original poster to additional liability.

Caution

There is one legal defense to a claim for defamation available only in the online context, which applies directly to 'user-generated content,' or UGC: Section 230 of the federal Communications Decency Act provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This means that websites or other platforms that allow readers to post comments or retweet third-party content are protected from a range of claims, including defamation, that might otherwise be used to hold them legally responsible for what others say and do on their platforms. This is because the user-generated content – the posted comment, the linked website or the original tweet – is 'information provided by another information content provider'. Significantly, however, this protection can be lost if the publisher (the operator of the website hosting the comment or containing the hyperlink, or the forwarder of the tweet), appears to have adopted or endorsed the original content, rather than merely making it available to others.

Tip #2. Think twice before sharing others' content: copyright and trademark online

Issue

This is a simple legal lesson that is sometimes hard for non-lawyers to accept: just because a photo, graphic or some text has been posted publicly online does not mean that others are entitled to re-post or share it. Copyright law, contract law or both may make that unlawful. It is equally clear, and equally hard for non-lawyers to accept, that giving credit ('Photo by Joe Smith') does not excuse an infringement.

Copyright owners have exclusive rights in their creative works, including the right to control reproduction, distribution, and display of their copyright-protected material. If a social media user copies and reposts or shares the material without permission, he or she could be legally liable to the owner. Some copyright owners give express permission for reuse (a note posted by the owner saying, "feel free to use my photos on your own website"), while some websites state in the terms and conditions (to which a user is often asked to consent by clicking 'I agree') that reuse of material at the site is authorized by the copyright owner. By the same token, however, a website's terms and conditions may prohibit reuse of material, and violating the terms may give rise to a claim for breach of contract. The practical difficulty, of course, is that it is sometimes very difficult to determine the actual owner of the copyright in the original work: once it has been copied and reused by someone else (or by a long string of other people), the identity of the true owner may have disappeared, but this provides no defense to an infringement claim.

Even in the absence of express permission to copy and reuse, however, providing a hyperlink to someone else's work or retweeting it generally have been held not to infringe copyrights. Similarly, there is an emerging consensus that 'in-line links' – the use of a hyperlink to the original item to create a split screen or 'screen within a screen' for the viewer, so that no actual copy of the original item is made – are non-infringing.

Caution

The concept of 'fair use' – the legal right to reuse someone else's content without their permission – is a source of much confusion. This is a fact-specific legal question that involves multiple factors. Two key factors are whether the reuse will have some impact on the market for the original work (will the reuse cause the owner to lose sales?), and whether the reuse is for a different and valuable purpose (a classic example is an art critic republishing an image of a painting for purposes of illustrating a review of the artist's work).

Federal copyright law also gives protection from infringement claims to website owners and operators of similar platforms who agree to remove allegedly infringing content after receiving notice of the claim (referred to as a 'take-down notice'). The law has housekeeping requirements that an owner or operator must follow to obtain this protection, which are described at www.copyright.gov/onlinesp/.

Similarly, unauthorized use of another's trademark on social media may lead to legal liability for trademark infringement or dilution, at least where use of the trademark creates a false impression of endorsement, affiliation or sponsorship. But, as with copyrights, it generally is permissible to mention a company and its product or logo in connection with a review or other post about the company.

Precisely because it is hard to identify the correct owner of online content, and because the copyright, trademark and contract issues governing reuse can be complex, thinking at least twice before repurposing someone else's content is therefore usually prudent.

Tip #3. Think remotely: cloud computing issues and security risks

Issue

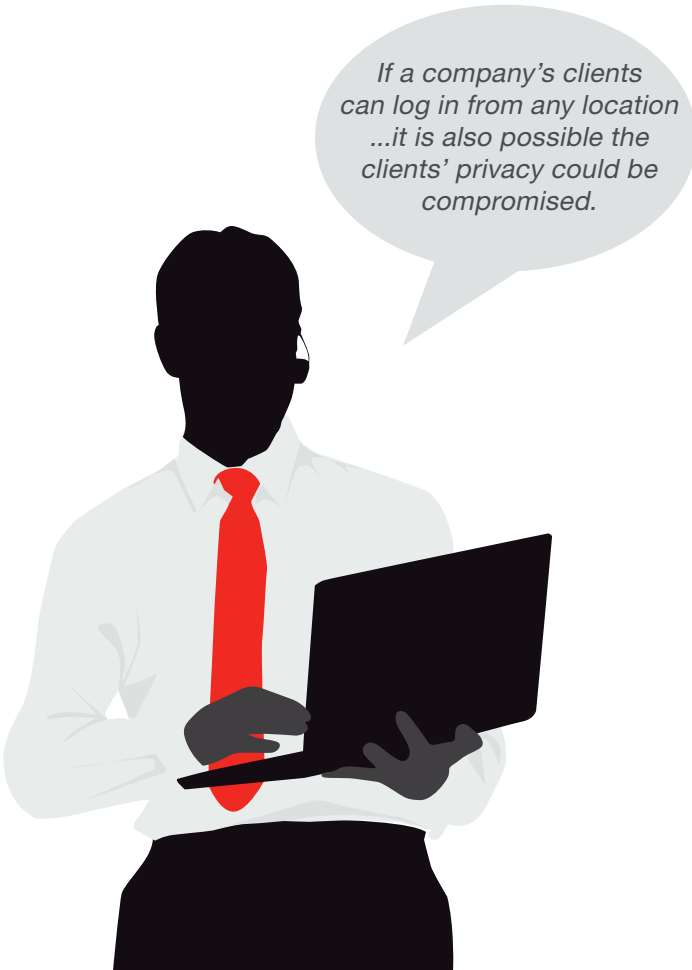
With employees increasingly accessing company applications and data via mobile devices and off-site computers, protecting the information stored on the company's network in the so-called 'cloud' from hackers becomes even more important. In simple terms, cloud computing is the storing of information and programs on remote servers accessed via the internet, instead of on a computer's own hard drive or a company's own server. Some businesses choose to subscribe to applications which allow the company to create custom network storage devices for use by company employees. However, these useful tools may not only attract businesses seeking to expand their remote office capabilities, but also hackers seeking access to confidential company information.

If an attacker gains access to a company's cloud credentials, he or she can potentially eavesdrop on activities and transactions, manipulate data, and falsify information. In addition, if a company's clients can log in from any location to access data and applications, it is also possible the clients' privacy could be compromised.

Caution

To help minimize these risks, proper training of employees who regularly work within the cloud is advisable, and regular refresher training on securely handling data may be helpful. Identifying network applications with highly sensitive information and providing extra protection, encryption and monitoring of them may also be useful.

Not all business owners or managers want to or can become experts in computer security issues. A company that does not have an internal expert can easily find qualified consultants to help properly set up and regularly maintain security. In the press of day to day business, particularly at a start-up or newly expanding company, this is an important 'investment in fundamentals' that can be overlooked.



Tip #4. Protect your trade secrets: employees and disclosure of confidential information

Issue

Equally worrisome for companies is the disclosure of confidential business information. The prevalence of Twitter accounts and other social media channels through which employees discuss their personal and work lives may raise concerns about whether an employer can and should place limits on what an employee can share online. For example, is it appropriate for an employee to tweet about a new business plan ("Being sent to Tampa to launch new office next month – Competitor X here I come!")? Not unless that tweet is actually part of the business plan. The traditional lines between work and personal life become blurred when employees use the same technologies (and sometimes the same accounts or profiles) in the office and at home. Additionally, the spontaneity and sense of familiarity created on social media sites such as Facebook, LinkedIn, and Twitter tends to result in people more inclined to share more information than they might at a formal conference or a business meeting.

Caution

Accordingly, some companies have adopted written policies making clear to their employees the scope of protected information, or what the employer considers to be confidential and inappropriate for sharing outside the company. In addition, when confidential business information is shared with employees, it may be appropriate to label the document or email message, 'not for distribution outside company' or 'not for comment on social media'. Most employees want to do the right thing in this regard, and giving them clear guidance often can, by itself, avoid harmful disclosures.

Tip #5. Decide who owns what: control of social media accounts

Issue

As noted, the distinction between personal and professional use of social media, and even between personal and professional profiles or accounts, is often blurred, the emphasis of Facebook in comparison to LinkedIn notwithstanding. Typically, what an employee tweets, blogs, or posts on the company's social media accounts as part of his or her duties is fully the company's business, and its legal responsibility. But a company may also be held responsible for what an employee posts off duty, at least if it is not clear to the reader whether the employee is speaking for the company or only personally.

Similarly, companies sometimes struggle with the issue of who owns a social media page or account. For example, does a popular food writer and blogger for a food business own the Twitter page that she regularly uses to post comments or other information about the company and its specialty food products, including the recipes she has created using those products, or does the company own the page and its content? What happens if the blogger leaves to work for a different food company? In the absence of an agreement between the blogger and the first company, the law may impose default answers to these questions with surprising results.

Caution

Therefore, depending on the nature of the business and whether employees are required to use social media for work purposes, it may be helpful to establish policies on maintaining separate work and personal profiles or accounts, requiring the use of disclaimers on personal accounts ("I work for XYZ, but my blog reflects my personal views only"), and whether the employer may monitor or access its employees' online profiles or other social media accounts. And to the extent engaging in social media is affirmatively part of an employee's job, it may be useful to address ownership of the accounts and content in question in the employment agreement. Certainly, businesses and employees alike can benefit from having social media policies that are realistic and not overly complex.

A company may be held responsible for what an employee posts off duty, at least if it is not clear to the reader whether the employee is speaking for the company or only personally.

Tip #6. Be prepared for discovery: electronic discovery of social media information

Issue

Although the concept of electronic discovery and the need to preserve relevant files when litigation is anticipated is by now familiar to most businesspeople, courts have also begun to grapple with issues of discoverable information online beyond the typical emails, text messages, and scanned documents. Postings on social media sites, like paper documents and emails, are generally subject to production during the discovery process in a lawsuit and can be used as evidence. Moreover, even if it is not itself 'evidence' relevant to the lawsuit, the information on a social media page is subject to production in discovery if it might reasonably lead to the discovery of other admissible evidence, such as the identity of witnesses. This is particularly so if the information in question has been posted publicly. At least one federal court has precluded discovery of social media information on privacy grounds, however, finding that information posted online that was shared only with a limited group, rather than the general public, could be considered private, and therefore not discoverable in the particular lawsuit in question.

Caution

This begs the question of who 'controls' the social media account or page in question (see Tip #5), since it is the party who possesses or controls the information who has an obligation to preserve and produce it. Given that employees often access and post to social media sites using both personal and company-owned devices, and some of those sites may be company-owned and some not, a company may wish to develop a social media discovery strategy. This would typically be an electronic document retention policy that specifies which communications and platforms are company property, and which are the personal property of the employee. It is also important that companies and employees understand how each social media site functions, the information likely to be shared on the site, and the various ways to access that information. This will allow a company to determine what information could potentially be relevant in litigation and how that data can be retrieved. Such planning could prove useful to the company if and when an actual legal proceeding is threatened.

Tip #7. Advertise with care: marketing on social media

Issue

Social media platforms have become increasingly appealing to companies wishing to expand their advertising reach. Social networks like Facebook and Twitter are regular destinations for millions of consumers. Increasingly, advertisements featured on these sites offer targeting to specific demographics, social connections, and interests. In addition, platforms such as Snapchat — a mobile app that allows users to send photo messages that self-destruct after a period of ten seconds or less — and Facebook's rival app Poke, are growing in popularity as companies look for ways to take advantage of users' desire to share and receive short-term visual messages. Like many social media platforms, however, privacy and security are concerns. Although applications like Snapchat are considered 'privacy-protective,' in that they delete content immediately upon sending, there is the possibility that the data can still be retrieved. Indeed, some of these applications have been the targets of hackers.

Another potential issue for companies turning to social media for marketing is the awkwardly named 'Controlling the Assault of Non-Solicited Pornography and Marketing Act,' or CAN-SPAM. This federal law generally requires that electronic commercial messages include accurate sender identification information, effective opt-out tools, and a physical address where the advertiser can be located. Although originally understood as limited to email, a recent federal court decision appears to expand the reach of the CAN-SPAM Act to electronic messages sent via social media as well. This means that companies that send advertising messages to individual users through social media sites may need to ensure that the messages meet all the requirements of the CAN-SPAM Act. This likely also would apply to automatic, unsolicited messages sent to social media users telling them about content available on a more traditional website.

Caution

Endorsements are an equally important tool for advertisers to attract consumers. Companies using social media to convey endorsements should be mindful that FTC guidelines provide that endorsements must be truthful and not misleading. For example, posting unrepresentative testimonials may be misleading if they are not accompanied by information describing what consumers can generally expect from use of the product or service. The FTC regularly posts guidelines on its website, www.ftc.gov, designed to help companies ensure that their online endorsements and testimonials meet these standards.

Tip #8. Beware the giveaway: contests and sweepstakes on social media

Issue

While there is nothing new about prize promotions such as sweepstakes and contests, merging such promotions with social and mobile media can be a particularly efficient and effective way of engaging consumers. However, conducting a prize promotion through social media can sometimes raise unanticipated legal issues. For example, does offering a user the chance to win a free prize in exchange for liking a company's Facebook page, following the company on Twitter, or joining the company's LinkedIn group, amount to giving consideration (i.e., an exchange of something of value), which could transform a simple contest into an illegal lottery? The case law in this area is not settled. In the meantime, companies may wish to ensure that any contest or sweepstakes it is offering is really free to enter – even if participants also have the option to 'like' or 'follow' the company.

Verifying the age of participants in contests is also difficult, and can raise legal issues if information about the winners – for example, extracts from the winners' Facebook pages – will be used in announcing the results or otherwise promoting the contest or the company sponsoring it.

Caution

Companies should also be aware that social media websites generally have terms and conditions in place that specifically govern advertising, including sweepstakes, contests, and giveaways. Thus, before launching or promoting a contest through a third-party site (such as Facebook), careful scrutiny of the website's user agreement is prudent.

Conclusion

Social media brings significant potential benefits to businesses, but also a number of potential legal pitfalls. Companies should be sure to have adequate insurance coverage in place to address social media activities and to carefully review coverage afforded by existing insurance policies, as their commercial general liability policies may not cover online content. Because risk extends beyond the company's own website to content placed elsewhere on the internet, such as Facebook, LinkedIn, etc., coverage needs to match the risk.

Social media – and the internet generally – have become fundamental tools of trade throughout the global economy. While the significant change associated with these developments is likely to continue for the foreseeable future, the accompanying distribution of risk is becoming a known quantity for businesses throughout the world. As the laws regulating social media continue to develop, prudent managers will stay abreast of developments and continue to implement appropriate safeguards and policies.

About the authors

Jay Ward Brown and Shaina Jones Ward are, respectively, a partner and associate in Levine Sullivan Koch & Schulz, LLP, a national firm specializing in representation of media and related companies in litigation arising from content and the production and distribution of it. Their clients include newspapers and magazines, digital media platforms, film studios, broadcasters and cable companies, book publishers, non-profit entities and consumer products manufacturers and retailers. The firm as a whole is ranked as one of the leading First Amendment defense firms in the country, and Mr Brown was named by Best Lawyers as the Media Law Attorney of the Year for 2014 in Washington, D.C., while Ms Ward was named a Rising Star in Media Law by the same publication. Mr Brown has previously taught media law at Trinity College and the University of Maryland. Mr Brown holds a J.D. degree from N.Y.U. and Ms Ward's J.D. degree is from Vanderbilt. Both worked as journalists prior to law school.

Contact information

Insurance brokers are welcome to contact us. Two ways to find your regional contact:

hiscoxbroker.com/contact-us/

Northeast: 646 452 2353
Southeast: 404 410 2800
Midwest: 312 380 5555
Northwest: 415 814 1455
Southwest: 213 412 1210