wiley

NEWSLETTER

The CDA, DMCA, UGC, COPPA: Alphabet Soup and Online Legal Basics

January 2011

Traditional radio, television and newspaper outlets are now using multiple platforms to disseminate information to the public, to further stories, and to connect with listeners, viewers and readers. Video-sharing and social network sites feature citizen reporting on news and current events from around the globe, and media organizations are regularly incorporating user-generated content (UGC) in their offerings, and presenting diverse opportunities for their audiences to comment on news stories, provide leads and sources, and offer opinion. New digital platforms, coupled with increasingly participatory media contribute to a complex and, in some respects, uncertain legal landscape.

As our clients ventured forth into the new media realm, we made them aware that there are two key documents or statements that all websites should post. First, the site's terms of use govern the site's relationship with users, allowing you to set boundaries of acceptable on-site behavior and potentially limiting liability. Second, the *privacy policy* informs users of the site's practices relating to private information and helps to avoid liability under a complex array of federal and state privacy laws. *While you may initially have sought legal guidance in preparing these documents, remember that they should be tailored specifically to your operations and revisited frequently*. The same best practice should now apply to your company's social media policy, which governs how your employees communicate in the online world, whether through Facebook or Twitter, for example.

Despite the ongoing technological revolution, bear in mind that the old laws still apply. Defamatory statements are defamatory statements, whether they appear on television or online. As

Authors

Kathleen A. Kirby
Partner
202.719.3360
kkirby@wiley.law

Ari Meltzer
Partner
202.719.7467
ameltzer@wiley.law

discussed in a companion article in this *Mass Media Headlines*, copyright laws apply to material published on the Internet, and to UGC. Privacy issues abound. In short, just about every substantive law previously followed in the "traditional" media realm should be followed in the context of cyberspace.

That said, certain "new" laws have been developed to protect, and in some cases restrict, activities that take place online.

The Communications Decency Act

Section 230 of the Communications Decency Act of 1996 (CDA), for example, provides certain protections for interactive computer service providers (ICSPs) when publishing the statements of another person. It provides that "[n]o 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." Operators of websites often qualify for immunity under the statute. The CDA has been used to protect online content providers against defamation, negligent misrepresentation, breach of contract, intentional nuisance, violations of federal civil rights and other claims. If there is sufficient involvement by the ICSP such that the content can no longer be considered to be provided by a third party, however, it is not likely to be protected by Section 230. The statute should protect online media from liability for comments posted in comments sections and forums. But a number of courts have indicated that active solicitation of content could eliminate Section 230 immunity. If a citizen journalist provides a news story for your website, for example, courts are likely to examine the underlying role of the news organization in soliciting or shaping the story in determining whether immunity can be invoked.

User-Generated Content and the Digital Millennium Copyright Act (DMCA)

The proliferation of UGC has become evident on online video and content services as well as in many forms of advertising. Sites featuring UGC, such as YouTube and Facebook, are some of the most trafficked sites on the Internet. A consortium of leading players in the digital content arena put together a list of principles to follow for those using UGC. They provide that if you are incorporating UGC in your content, you should: (1) provide conspicuous notice in your website terms of use that users may not submit infringing content; (2) implement content-filtering technology to automatically block infringing content that users may attempt to upload to their website; (3) provide content owners with reasonable search capability to locate infringing content on the website; (4) if necessary, conduct manual review of user-submitted content to determine if such content is infringing; and (5) expeditiously take down infringing content and block and/or terminate users who repeatedly submit infringing content.

For certain UGC, the DMCA may offer you some protection. The DMCA provides a safe harbor for ISPs from copyright violation claims provided they follow certain guidelines and promptly remove infringing materials once they receive notice of the infringement from a copyright holder. Your company should have specific guidelines in place for following the DMCA's notice and takedown procedures when a complaint is received.

Where a reasonable review of the relevant UGC should "raise a red flag" that it is potentially infringing, there may be a claim for copyright infringement against an ISP. If you accept submissions of UGC from individuals and, without any type of review or filtering process, post these UGC submissions, you may be liable. For example, where the UGC contains a copyrighted song or other protected work that has been used without permission and it raises a red flag, you could face significant liability for posting the material, particularly where you would receive a measurable gain or benefit from the commercial use of the infringing UGC.

Note that the DMCA's protections appear to be shrinking. Section 512(c) of the DMCA provides that an ISP will not have liability for the infringing activity of a user if the following criteria are met: (1) the service provider must not have the requisite level of knowledge of the infringing activity, (2) it must not receive a financial benefit directly attributable to the infringing content, and (3) it must act expeditiously to take down or block access to infringing content. The *Grokster* decision out of the Southern District of New York (SDNY) made clear that a service provider may have liability if the primary purpose of the service is to disseminate infringing content. The ongoing *Viacom/Paramount Pictures v. YouTube* case in the SDNY presents another opportunity for the court to narrow the applicability of the DMCA safe harbor.

Children's Online Privacy Protection Act

COPPA prevents commercial website operators from collecting online (via website registrations/clubs, email, chatrooms, tracking or cookies) any Personally Identifiable Information (PII) from children under the age of 13, unless there is advance "verifiable parental consent." Federal Trade Commission regulations specify how verifiable parental consent may be obtained. PII includes a child's name, address, email address, telephone number, social security number or other information, including cookies or other "persistent identifiers," that makes identification possible. COPPA applies to two categories of commercial websites: (1) those that are "directed to" children (*e.g.*, through subject matter, or the use of cartoons), or (2) those that have actual knowledge of PII collected online from children. Actual knowledge exists, even if unsolicited, whenever a child discloses his or her age, grade level or primary school name online, such as in a chat room or message board, and the website operator either monitors, or is made aware of, the content.

COPPA is the subject of recent review by the FTC and scrutiny by advocacy groups, with an eye toward expansion. FTC enforcement actions have resulted in sizable fines for COPPA violations, including in excess of $1 million. If you plan to collect information from children, it is critical that you seek legal counsel and craft a thoughtful, well-balanced privacy policy that complies with COPPA and reflects your actual practices.

In the Newsroom

For all its benefits, the relative ease with which anyone can post information online should cause every journalist to question and then question again. When considering information derived from the Internet, don't forget the basics. Use original sources and documents when possible, attribute information gathered to published sources, use multiple original sources of information, and check every fact reported.

Many people believe that anything published on the Internet is in the public domain or that anything can be incorporated into news reporting as a fair use. Wrong.

You should subject material you obtain from the Internet and incorporate in your reporting to the same copyright analysis you would otherwise use. Second, the inclusion of citizen journalists in the process of finding, publishing and propagating news may make it difficult to determine "ownership" of a story ultimately produced. Treat your amateur contributors as you would freelancers, with rights clearly outlined.

Material you obtain from listeners or viewers also may raise potential liability for newsgathering torts (like violation of wiretapping laws, fraud, trespass or conversion). Generally speaking, the news media will not be held liable for publishing lawfully obtained information on matters of public concern, even if they knew or had reason to know that the material itself had been obtained unlawfully by a third party. But you might be held liable if you participate, directly or indirectly, in the unlawful conduct through which the information was obtained. If you solicit input or source material from listeners and viewers, you should be mindful of any actions that could be construed as encouraging illegal behavior and recognize that third parties invested in a collaboration may be more apt to cross certain lines than would seasoned journalists. You should also take care not to promote risky behavior.

It is also wise to implement procedures to correct substantive errors on the Internet. You may reduce potential liability from defamation claims by publishing corrections or retractions that respond to legitimate demands from persons who claim they have been libeled online. Internet search engines are also spawning requests to correct, update or remove articles archived online. You likely have no legal duty to remove or update outdated material, and courts are holding that statutes of limitations do apply to online publications and run from the first publication of the material in a mass medium. If the statute of limitations has not run out, you may avoid potential liability by correcting or updating information, but you should proceed carefully and seek legal advice about whether you face the risk of lawsuit by republishing the allegedly false content, if only by correcting or updating it.

Of course, the proliferation of online publications and the ease with which almost anyone can publish "news" begs the question of who is a "journalist." This has obvious implications in the context of state (and proposed federal) laws that protect "journalists" from disclosing certain information during government proceedings. Whether or not you qualify as a journalist entitling you to invoke a privilege against testifying about or revealing your sources or other confidential information may have far-reaching implications for you and your reporting.

Conclusion

These are just some of the basic legal issues to keep in mind as your business evolves in today's media marketplace. Others are discussed throughout this newsletter. As the law attempts to catch up to technology, we'll keep you apprised of developments.

*District of Columbia Bar (pending, supervised by principals of the firm)