Web Site Checklist: Minding Your Company's Virtual Storefronts

By Jessica R. Friedman and Paul S. Ellis

Any Web site that your company operates has the potential to be both a blessing and a curse. An attractive Web site can be a significant boost to your company's bottom line. But the same features that make a company's Web sites attractive can also spark a variety of legal claims if they have not been properly vetted. Many of those claims are not unique to the online environment. Defamation or false advertising, for example, can occur in any medium, and counsel should be reviewing all content in any format that might pose a risk of either claim. But Web sites present some unique problems.

First, because it is so easy to post new material online, and because there is such pressure to keep content fresh, people tend to post content without subjecting it to the same legal review to which they would subject print content. Second, user-generated content occurs only on Web sites (and social media pages, which carry some of the same risks). Finally, only Web sites have terms of use and privacy policies, and although the average consumer will probably never read either of them on any Web site, those legal provisions are the first place a sharp plaintiff's lawyer will look when analyzing a potential claim against your company arising from a user's interaction with one of your company's sites.

Many in-house attorneys would be hard-pressed to find the time to review their companies' Web sites on any type of periodic basis, let alone to conduct the daily or even weekly review that would really be required to eliminate all the possible risks. But based on our experience, if you can find the time, checking for the following potential problems will significantly reduce your company's exposure.

1. Trademark Infringement

Even if your company has a policy that requires that the legal department clear each and every trademark before it is used, unless everyone in the company is aware of and adheres to that policy, even a cursory review is likely to reveal trademarks and service marks for your company's products and services that you have never seen before. If this happens, you have to decide whether the mark needs to be removed (is it very clearly likely to be confused with another company's mark? How important is that mark to that other company?), and if so, how fast (immediately, or can it wait until you clear the rights?) and for how long (temporarily while you clear the rights, or permanently?). Not every company, and certainly not every start-up, can afford to conduct complete clearance on each and every mark that some marketing staffer thinks the company should use. Even if you bring a mark that has not been cleared to the attention of the head of the relevant business division, he or she may decide to take a risk and just continue to use the mark. But by at least keeping an eye out for those potentially problematic marks on the Web sites, you will be significantly reducing the company's risk.

Also, every company likes to showcase its existing client list, especially if that list includes heavy hitters or "household names." But not all companies like their names to be used that way. Many companies actually have provisions in their vendor agreements that expressly prohibit clients' use of their names and logos as endorsements without their consent. You should check all of your companies' sites periodically for third-party names and logos. When you find one, you need to check that your company is authorized to display it, or, at least, that your company is not prohibited from displaying it.

2. Copyright Infringement

Many people, and especially the younger people who run many companies' online operations, think that if content can be reproduced, it's perfectly legal to reproduce and display it on another site, either because it's somehow not subject to copyright, or because doing so is "fair use." Both of these assumptions are unfounded.

Under U.S. copyright law, any content that meets a very minimal originality requirement is automatically subject to copyright protection, and only the owner of the copyright in that content has the right to reproduce that content, modify it, create adaptations of it, distribute copies of it (which includes transmit it electronically), display it publicly, and perform it publicly. If anyone other than the owner does any of those things, it is copyright infringement. Since your company's Web sites are accessible all over the world, if your editorial and marketing people are cutting and pasting in articles, photos or other content from other sites, the company is vulnerable to a claim of copyright infringement both in the U.S. and abroad.

Moreover, despite popular misunderstanding, "fair use" is not a magic wand that automatically converts infringing use into non-infringing use, and there are no "bright line" standards that apply to all situations. Fair use is a specific defense to a charge of copyright infringement, pursuant to which a court may excuse certain copying that otherwise would be infringement, after it considers four factors set out in the Copyright Act, together with

whatever else the court considers relevant, as applied to the specific facts at hand.

Even if your company's sites comply with all the requirements of U.S. law, it may still be infringing copyright laws or related laws of other jurisdictions, which could result in the company's being sued in another country. In 2007, a French court held that Viewfinder, the owner of a Web site based in the United States that posts photographs from fashion shows, was liable for copyright infringement under French law for displaying photos from two French fashion houses on its Web site, because while U.S. copyright law does not recognize a copyright in fashion designs, French law does.[1] Viewfinder defaulted, and the French court not only found Viewfinder liable, but awarded the plaintiffs one million francs in compensatory damages in a judgment that the plaintiffs then sought to enforce in court in New York. (That is not the end of the story, but suffice it to say that Viewfinder ended up having to spend a good deal on legal fees just to try to avoid enforcement of that judgment.)

The takeaway here is that you need to check for third-party articles, photos, graphics, and any other content on the company's sites. If you are told that particular content is licensed, you should review the license to make sure it covers Internet usage and has not expired.

Learning that a particular image has been licensed from a stock photo house should not end your inquiry. If your company uses a stock image on a Web site under a license that does not cover Internet use, or if it had a license for Internet use that has expired, sooner or later you can expect a letter from the stock house that demands that the company pay not only a license fee but a penalty fee that your company "agreed" to pay when the license was signed, or else face a copyright infringement suit. Often, these kinds of demands can be settled for less than $5,000, but if your company is small, is a start-up, or is just not doing well in this economy, even that amount can be more than you want to spend. The best way to avoid this is to tell your marketing department (or whoever is responsible for what appears on the Web sites) exactly which versions of the major stock licenses are acceptable.

If you spot any material that turns out not to be licensed at all, try to find out where it came from, or at least try to make sure that it is not the result of "scraping" other sites, which is especially common on real-estate industry sites and other listing sites.

3. Right of Publicity Violations

Displaying a person's name or photo, or using a recording of someone's voice, to advertise your company's products or services without that person's permission may violate that person's so-called "right of publicity." Not every state recognizes the right of publicity, and of the states that do, some have specific statutes and some only enforce it through judicial decisions, and the penalties vary from state to state. But as a general rule, even if Madonna is using your company's products, the company may not say so on its site or social media pages without Madonna's permission. So check for anything that looks like a celebrity endorsement—even a "candid" photo of a celebrity using your product. The fact that a celebrity was actually wearing your company's sunglasses does not mean that the celebrity consents to the use of her image to advertise those same sunglasses. In some states, one's right of publicity survives death, so that even using the name or photo of a deceased celebrity can result in a legal challenge. So if you happen to see a photo of Rosa Parks as part of a branding campaign designed to indicate that your company is "revolutionary," take it down immediately.

Just looking for celebrity names and photos is not enough, though, because one doesn't have to be famous to bring a right of publicity claim. In 2011, a group of users brought a class action against Facebook in which they alleged that Facebook was violating their rights of publicity by displaying the fact that they had "liked" certain products.[2] Facebook moved to dismiss the claim, but the court denied the motion because Facebook itself had admitted that an advertisement with that kind of testimonial attached to it was twice as valuable as an ad without one. (The case eventually settled.) So if any consumer-facing page includes a testimonial of a real person, even if that person is not famous, check whether the company has permission to use that person's name for that purpose.

4. Outdated Privacy Policies

Your consumer-facing privacy policies should be customized for the businesses that they represent. There is no one-size-fits-all. The online policy for each company Web site has to say what personal information *your* company collects on that site, what *your* company does with that information, and with whom *your* company shares that information. The language in which you articulate these policies should be clear and the graphic presentation should make them conspicuous.

But even if you are sure that each of your online privacy policies was drafted specifically for the business it reflects, you need to revisit them every couple of months to make sure that they are still accurate. If the company has actually changed its privacy practices in some material way—for example, if it has decided to sell its e-mail lists even though it initially did not do that—it may not be enough to simply rewrite the online policies. The company will need to notify users of the changes *separately from* its company's terms of use and privacy policy, and

preferably *before* it starts to sell the information, so that users who do not want their information handled according to the new policy have a chance to opt out. One effective way to notify users is to send out an e-mail to all your users that contains a link to the impending new policy. Needless to say, if you propose this, you are likely to get some serious pushback from the head of your marketing department. But one good antidote to that pushback would be to describe the burdensome FTC consent decree that Google was forced to enter into in 2011 after it violated its own privacy promises when it rolled out its "Google Buzz" service.[3]

Although many privacy policies don't have it, your policy should include a provision that is required by California law that says that if a California resident asks to be told with whom your company is sharing his or her personal information, you will provide that information within thirty days.

Finally, even if the facts stated in your consumer-facing privacy policies have not changed, the laws that govern what those policies have to say may have changed. It is beyond the scope of this article to talk about worldwide privacy law developments, but you should either have outside privacy counsel or a few good sources you can turn to for the latest developments.

5. Out-of-Date and/or Unenforceable Terms of Use

Like consumer-facing privacy policies, your terms of use need to be written specifically for your company. But even if your company was smart enough to start out with terms of use that were drafted specifically to fit its operations, if the company has changed the way that it does business, those terms of use may no longer be accurate. Maybe the company has changed its refund policy or the way its auctions work or its rules concerning the posting of user-generated content.

Equally important, if up to now your company has not been requiring users to agree to its terms of use, consider changing that policy by making them actually click on an "I agree" icon, either when they enter the site or at some crucial point, such as when they buy an item or click on an article (even if it's free). Just displaying a statement somewhere on the site that by browsing the site, a user is bound to the site's terms of use—which is sometimes inaccurately called a "browsewrap" agreement—has been held to be ineffective in many cases. If your company has been lucky enough not to experience any serious user disputes, the difference between a browsewrap agreement and a clickthrough agreement may not be immediately obvious. For example, if your user agreement says that the company will only give refunds within the first 30 days after a purchase, and someone seeks a refund six months later, not being able to enforce the 30-day limitation may not be a big deal (and unless the product was very expensive, the chances of anyone's actually initiating legal action are very low to start with). But if your company is unable to enforce a disclaimer of warranty, or a limitation on the company's liability for an expensive defective product to the price that the user paid for it, or a requirement that any claims against the company be subject to arbitration in Miami, the costs may be very high, especially if you are trying to fend off multiple lawsuits or a class-action suit by disgruntled users.

Zappos learned this the hard way in 2012 when it sought to enforce a clause in its terms of use that required users to submit all disputes to arbitration in Las Vegas.[4] Although a link to the terms of use appeared on every page of the Zappos site, the court found that those links were "inconspicuous, buried in the middle to bottom of every Zappos.com webpage among many other links, and the website never direct[ed] a user to the Terms of Use." Because the plaintiffs had never assented to the terms, no contract existed, so they could not be compelled to arbitrate. This past May, a court held that Yahoo! could not enforce a requirement that any litigation be brought in California.[5] On the other hand, in a 2011 case, the court held that Zynga's terms of use were enforceable even though users were not actually required to click "I agree" before accessing the application at issue, because "the terms were presented right underneath the button which allowed [the plaintiff] to access the application."[6] It's okay if your terms of use are in a "scrollbox," which a user would have to scroll through to read, as long as assent to them is mandatory.[7]

Another reason that the court held that Zappos could not enforce its terms of use is that those terms provided that Zappos had the right to change them at any time. Many terms of use include such unilateral amendment provisions, but well before the Zappos decision, courts had held that such a provision converts any agreement that otherwise might be formed into an "illusory" contract, which is not enforceable. If your company's terms of use include such provisions, consider removing them.

Last but not least, make sure that the information about your DMCA agent—your agent for receiving claims of online copyright infringement under the Digital Millennium Copyright Act—is up to date. If you never appointed an agent in the first place, you should do so at http://www.copyright.gov/onlinesp/agent.pdf, or else the company will not be eligible for the safe-harbor protections of Section 512 of the DMCA.

6. "Creation and Development" of Offensive User-Generated Content

If your company's sites allow the posting of user-generated content, you are probably aware of Section 230 of the Communications Decency Act.[8] Section 230

immunizes an "interactive service provider," which includes a Web site operator, from most federal and state liability[9] arising out of user-generated content (and other third-party content) as long as the Web site operator is not "responsible in whole or in part for the creation or development of the offending content."

Unfortunately, despite one court's statement that "[i]f you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune,"[10] Section 230 is not self-enforcing. There seems to be no shortage of creative plaintiffs' lawyers—and even plaintiffs who themselves are lawyers—who will allege that just by making it technologically possible to post content, a Web site operator is responsible for the creation of that content.[11] Plaintiffs also continue to bring cases that allege that newspapers are responsible for reader comments on account of their having moderated those comments to make sure that they were not abusive, obscene, profane or otherwise in violation of the newspaper site's own terms of use, even though it is well-established that this is not the case.[12] And despite the seemingly clear protection that Section 230 literally provides, once in a while, a court will refuse to dismiss a claim that clearly should be dismissed under Section 230.[13] Moreover, ever since the Ninth Circuit held in *Fair Housing Council v. Roommates.com* that by requiring subscribers to include certain information in their profiles, Roommates.com in effect became the developer "at least in part" of that information,[14] many plaintiffs make sure to include allegations to the effect that the defendants have created or developed the allegedly offensive content "in part," which is sometimes enough for the court to permit discovery on the issue of how the offending content was created.[15]

Although there is no way to completely insulate your company against lawsuits over user-generated content, you still may be able to reduce your company's risk of liability by making sure that whoever runs your company's forums or message boards is not doing any more than "moderating" user comments and that the interactive features of your company's sites are not structured so as to somehow solicit content that is illegal or that reasonably can be anticipated to be harmful or offensive.

Endnotes

1. *Sarl Louis Feraud Int'l v. Viewfinder, Inc.* 489 F.3d 474 (2nd Cir. 2007).
2. *Fraley v. Facebook, Inc., et al.*, no. 111-CV-196193 (Cal. Super. Ct.).
3. The settlement (i) bars Google from misrepresenting the privacy or confidentiality of individuals' information or misrepresenting compliance with the U.S.-EU Safe Harbor or other privacy, security, or compliance programs, (ii) requires Google to obtain users' consent before sharing its information with third parties if it changes its products or services in a way that results in information sharing that is contrary to any privacy promises made when the user's information was collected, (iii) requires Google to establish and maintain a comprehensive privacy program, and (iv) requires that for the next 20 years, the company have audits conducted by independent third parties every two years to assess its privacy and data protection practices. See http://www.ftc.gov/opa/2011/03/google.shtm for a summary and http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf for the actual consent decree.
4. *Id.*
5. *Ajemian v. Yahoo!*, 12-P-178 (Mass. Ct. App. 2013).
6. *Swift v. Zynga*, 2011 WL 3419499 (N.D. Cal. 2011).
7. *Scherillo v. Dun & Bradstreet, Inc.*, 2010 WL 537805 (E.D.N.Y. 2010).
8. 47 U.S.C. § 230.
9. Section 230 does not apply to liability arising out of the use (or misuse) of intellectual property, federal criminal prosecutions, or liability arising under the Electronic Communications Privacy Act or analogous state laws.
10. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 2008 WL 879293 (9th Cir. 2008).
11. *See, e.g., Barnes v. Yahoo!*, 2005 WL 3005602 (D. Or. 2005), in which the plaintiff claimed that Yahoo! was responsible for profiles posted by her ex-boyfriend that included nude photos of her and her contact information, because Yahoo! provided the tools to create the offending profiles.
12. *See, e.g., Gains v. Romkey*, 2012 IL App (3d) 110594-U (Ill. App. Ct. 2012); *Delle v. Worcester Telegram & Gazette Corp.*, 2011 WL 7090709 (Mass. Super. Ct. 2011).
13. *See, e.g., Jones v. Dirty World Entertainment Recordings, LLC*, 2012 WL 70426 (E.D. Ky. 2012).
14. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 2008 WL 879293 (9th Cir. 2008). The inclusion of information such as user gender and sexual preference was held to violate the federal Fair Housing Act and California housing discrimination laws by making it possible for potential roommates to discriminate against people based on the contents of their profiles.
15. *Chang v. Wozo LLC*, 2012 WL 1067643 (D. Mass. 2012).

Jessica R. Friedman has practiced copyright, trademark, e-commerce and publishing law in New York City for over 20 years. Her clients include technology, publishing, and entertainment companies. In addition to conducting her own private practice (www.literarypropertylaw.com), she serves as counsel to the Paul Ellis Law Group.

Paul Ellis is the principal of the Paul Ellis Law Group LLC (www.pelglaw.com), a 6-lawyer firm that represents small and midsize companies in corporate, intellectual property and general operational matters. Paul is a founding board member of the New York Technology Council, a trade association dedicated to supporting and promoting the technology industry, and is a frequent speaker on legal issues for technology companies.