VENABLE® LLP

Articles

October 5, 2010

The Top Five Technology Legal Traps for the Unwary Association

AUTHORS

Jeffrey S. Tenenbaum

Armand J. (A.J.) Zottola

RELATED PRACTICES

Technology Transactions and Outsourcing

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2010 2006 2002
2009 2005 2001
2008 2004 2000
2007 2003

Related Topic Area(s): Antitrust and Trade Regulation, Copyrights and Trademarks, Electronic Communications, Employment Law, Meeting, Vendor and Government Contracts, Miscellaneous

New technology brings new opportunities for associations to leverage new communication devices, systems and networks. However, incorporating new technology into an association's operations or its external communication, membership or marketing efforts without first considering the potential legal risks can expose the unwary association to potential liability. In order to keep from falling into these legal traps, associations must first be aware of them, and then take proactive steps to avoid them. The following is a non-exhaustive list of some of the top legal traps that can snare an association using new today's new technology.

#1 - The Online/Electronic Contract Trap

Electronic contracts are generally enforceable to the same extent as paper contracts. The Uniform Electronic Transaction Act ("UETA"), which provides that an electronic signature satisfies any legal requirement for a signature on a contract, has been adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Federal legislation, called the Electronic Signatures in Global and National Commerce Act ("ESIGN"), also endorses the use of electronic contracts in interstate commerce. However, even if electronic contracts are generally enforceable, associations that enter into contracts online still have to be mindful of contractual requirements such as showing knowledge of, and assent to, the contract by both parties. Additionally, electronic contracting requires consideration of unique issues, such as maintaining a level of security and authentication adequate to verify reasonably the identity of the parties entering the contract.

Once an association begins to use electronic contracts to make its content, resources and tools available online, the association also should consider setting forth the specific terms and conditions governing the use of such content, resources and tools. These terms and conditions should address common issues such as end-user conduct, permissible use of intellectual property, notice of proprietary rights, disclaimers, limits on liability, the association's role or responsibilities, and other relevant legal issues related to the particular conduct. With respect to posting such terms and conditions, the association should not rely solely on mere notice. Maintaining an enforceable legal document should be accomplished by providing both notice and an opportunity for the end user or other contracting party to review the applicable terms and conditions and subsequently provide some manifestation of assent to the applicable terms and conditions. Recent court decisions suggest that mere notice without a manifestation of assent is not sufficient to make the terms and conditions enforceable. An association also should implement a process by which to document and maintain a record for the online formation and "execution" of an electronic agreement in the same general manner that an association may keep records of the execution of its paper contracts, pursuant to its records and information management policy.

#2 - The Social Media Trap

Associations that operate interactive websites, listserves, blogs, or other interactive online forums, or that utilize online social networks, may encounter user postings with content that infringes or violates the rights of others. For example, with respect to copyrightable works owned by third parties, such as articles written by others, if the posting was made by an association employee, the association may be vicariously liable for copyright infringement if the posting was done without the permission of the copyright owner. If the posting was done by a third party (such as an association member), an association could become liable if it contributes to the posting of the infringing content or alters the material so as to contribute to its content, or if it knew or should have known of the infringement and did not take prompt corrective action. The safe harbor provision of the federal Digital Millennium

Copyright Act ("DMCA") may help shield an association from liability for third-party postings that contain infringing material so long as the organization itself maintains a neutral role, *i.e.*, the infringing material is transmitted at the direction of someone else, is carried out through an automatic process, is not sent to recipients specifically selected by the hosting company, and is transmitted without modification. The federal Communications Decency Act ("CDA") also provides some protection from defamation and other tort liability for postings by third parties, so long as the association does not become the "publisher" of the content. Note that the CDA does not provide protection from antitrust liability or liability for copyright or trademark infringement.

An association should post terms and conditions that govern the behavior of third-party posters as well as the association's own employees, and that clearly identify the type of acceptable content that may be posted to the website or other interactive online forum operated by the association. In addition, associations should maintain a policy governing social media use by association employees, making clear both what is encouraged and what is prohibited, restricted or otherwise subject to regulation by the association.

Social media or networking sites also make it easier for someone to masquerade as another person or entity. For example, in *LaRussa v. Twitter, Inc.*, Major League Baseball manager Tony LaRussa sued Twitter after discovering that someone both created an account using his name (www.twitter.com/TonyLaRussa) and posted negative "tweets" about him underneath his name and photo. After contacting Twitter about the account and receiving no response, LaRussa sued Twitter for trademark infringement as well as cybersquatting and misappropriation of his name. Although the suit was later voluntarily dismissed, it provided an example of both the need to monitor and enforce an association's online identity and the risk that can arise from not establishing and identifying for the public an association's official online presence. This is especially critical when an association plans to permit others, even affiliated entities such state and local chapters, to use the association's name online. An association should declare which sites are its own and provide rules for when someone else is using the association's name or trademark outside of the association's official site(s).

#3 - The Trademark Trap

It is easy to misuse third-party trademarks in electronic environments. As a general rule, an association should only use a third party's trademark with permission. In addition, an association should remain vigilant with respect to protecting its own trademarks. Associations should monitor for impermissible use of the association's name or trademarks in or as keyword search terms, user account names, or as the primary variables in unauthorized search engine optimization efforts. To protect against trademark infringement via online advertising or online social networks, associations should consider reserving their own trademarks as user account names and/or as online search keywords with online social networks, ad networks, search engines, and other interactive communities in order to claim rights in the character string equal to an association's full or most recognizable name (s). Associations also should notify and communicate with the appropriate search engine operators or online advertisers if they believe that their trademarks are being improperly used. Associations should make it an express policy to prohibit use by third parties of its name or trademarks as an account name or avatar (*i.e.*, a user or account holder's representation of itself, or the alter ego whether in the form of an image, symbol, icon, logo, username, or text string). Associations should periodically search and enforce such a rule in order to uncover instances when an association's trademark rights are being infringed or misused.

Domain names remain another area where trademark rights can be easily trampled. Associations likely want domain names that are equivalent or similar to their organization's name. As such, associations must remain diligent in their efforts to protect their trademark rights in connection with certain domain name reservation or registration practices. Although registrars now recognize the protection and enforcement of trademark rights in their domain name registration practices, new forms of cybersquatting consistently arise in connection with the increasing number of available top-level domains for domain name registration, such as country- or business-specific domains. For example, "front runners" are domain prospectors who register names immediately after potential brand owners have filed trademark registration applications with the U.S. Patent and Trademark Office. This has the effect of requiring the potential brand owner to purchase the domain name from the domain prospector. To protect against "front-running," associations should consider simultaneously registering for a domain name(s) corresponding to the trademark that is the subject of a new application. Associations also must remain aware of cybersquatters that engage in "drop-catching." In such instances, cybersquatters wait for a registration for a domain name to expire and then "drop-catch" (immediately register the domain name). Cybersquatters profit by building traffic off of the prior

registrants. This is especially true of domains that contain trademarks. Associations can avoid "drop-catching" by being proactive in their efforts to renew their domain names.

#4 - The New Technology Trap

When a new technology gains widespread use and acceptance, it still remains important for an association that may be utilizing the technology for the first time to be aware of the related requirements and potential risks associated with the new technology. This is true even if the association is not one of the early adopters of the technology. For example, more and more associations are conducting business transactions (such as membership dues payments, conference registration fees, and publication sales) and accepting payment through their websites. Associations that utilize credit and debit cards to process payment transactions should ensure that their efforts to protect consumer account information comply with PCI Data Security Standards ("PCI DSS"). PCI DSS is a set of 12 security standards created by the credit card industry that are intended to help organizations protect customer account information from theft and misuse. The standards focus on security management, as well as policies, procedures and protective measures for safeguarding customer account data. Although there are no federal or state laws that mandate compliance with all 12 PCI standards, several states, including Minnesota, have recently enacted statutory requirements similar to PCI DSS. The Minnesota law prohibits merchants from storing sensitive authentication data after payment cards are authorized. As a consequence, associations that process payment card data should validate the association's data security, handling and storage processes and take proactive steps to ensure their compliance with PCI DSS. On many occasions, an association may need to implement and pay for the necessary security programs and measures required to remain in compliance with PCI DSS. Although such PCI compliance may be costly, in the long run, secure payment systems will help associations to preserve member/customer loyalty and brand value.

Associations also must protect against the risks that accompany employee use of employer-issued mobile communication devices. More and more associations permit use of, or even provide their employers with, mobile devices to facilitate their work. As the capacity and sensitivity of data that mobile communication devices can hold continues to expand, employers should make every effort to protect the information managed or stored through such devices in the same manner that the association manages the information on its own internal computer network. For example, the use of third-party applications on mobile communication devices is now a prevailing norm (*e.g.* ringtones, games, etc.). As a result, the risk of malware for mobile devices continues to increase (*e.g.*, there were some 300 to 500 known versions of mobile malware in 2008). Although most mobile operating system vendors require third-party applications to be tested for approval and certification, this often is not enough protection to avoid viruses or other forms of malware. Associations should therefore work to protect both their own internal computer networks and systems and their external networks and mobile devices by purchasing anti-malware programs and measures that address both kinds of networks. Additionally, employers should implement proactive processes to protect information on employee mobile devices that are lost or stolen. Beyond password features, associations should invest in remote data deletion software that would allow an association to remotely delete sensitive information on lost or stolen devices.

#5 - The Employee Use Trap

As more and more information is stored electronically and new technology makes it easier to access and disseminate information, trade secret protection becomes harder to manage and enforce. Trade secret owners therefore must take extra precautions for the use, handling and transmission of their valuable or proprietary information in digital form. Associations should implement policies directed specifically against disclosure that may occur online or through mobile communication devices. These policies should focus on restricting and controlling employee access to and disclosure of trade secrets through these newer forms of communication. For example, associations should prohibit employees from storing confidential information on unauthorized digital devices or posting confidential information on unaffiliated websites (e.g., social media sites, blogs, etc.). Additionally, associations should actively promote security compliance to their employees, and require that employees promptly report any security breaches. Finally, upon termination of employment, associations should require employees to delete any association information that has been stored on personal electronic devices.

In addition to remaining mindful of trade secrets in connection with mobile communication devices, the capabilities of remote access are increasingly expanding the traditional notion of the workplace. This expansion has ramifications on both controlling and monitoring employee conduct. According to the U.S. Supreme Court's recent decision in *City of Ontario v. Quon*, employers can monitor employee

text messages on employer-issued mobile phones or pagers – if done in the appropriate manner. In that case, the City reviewed an employee's text messages (and those of two fellow co-workers) after the employee exceeded his texting limit. In conducting its review, the City discovered many of the employee's text messages to be personal and sexually explicit. The Court held that the search did not violate the employee's Fourth Amendment rights to reasonable search and seizure. While *Quon* involved a government employer and thus posed different legal standards than most associations face, it serves as an important reminder that associations should consider adopting policies that explicitly address the ability to monitor employee conduct outside an association's own offices (*e.g.*, on personal computers linked to the associations network and personal mobile communication devices linked to the association's email system) – and that specifically make clear to employees that they have no reasonable expectation of privacy when using these facilities. In addition to safeguarding confidential information and maintaining productivity, monitoring can be justified as necessary to help protect associations from vicarious liability for employee conduct. Courts have regularly held employers liable for their employees' inappropriate use of employer-provided mobile communication devices. For example, in *Ellender v. Neff Rental, Inc.,* an employer was held vicariously liable for the negligence of an employee who caused an accident in his personal vehicle while conducting business on his employer-provided cell phone. Therefore, to protect themselves from potential liability, associations should establish written policies that work to monitor and deter inappropriate use of association-related facilities both in and outside of the office.

* * * * *

Jeff Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. A.J. Zottola is a partner at Venable in the Business and Technology Transaction Groups and focuses his practice on intellectual property, computer, Internet, new media, and technology law. For more information, please contact ***jstenenbaum@venable.com*** *or* ***ajzottola@venable.com****, or 202-344-4000.*