Robinson+Cole

Intelligence

TRENDING

ADA Website Compliance

There has been a recent surge of lawsuits and demand letters alleging company websites are violating the Americans with Disability Act (the “ADA”). In the first six months of 2018, there were at least 1,053 lawsuits alleging websites are not in compliance with the ADA, many of which are class actions. This is compared to 814 lawsuits in all of 2017.

Most recently, an individual, Dennis Haynes, who is blind, sued Dunkin’ Donuts, claiming that the company’s website was in violation of the ADA because it was not compatible with the screen-reading software he uses. This left Mr. Haynes unable to locate physical Dunkin’ Donuts store locations, purchase gift cards, or utilize other features of the website. While the lower court dismissed Mr. Haynes' complaint, on appeal the court ruled in his favor. [To read the court’s decision see *Haynes v. Dunkin’ Donuts LLC*, No. 18-10373, 2018 U.S. App. LEXIS 21126 (11th Cir. July 31, 2018)]. This follows a lawsuit by an individual in Florida who is blind and could not access a supermarket chain’s website to order a prescription or look up the store’s hours. A Florida court held that the supermarket’s website was in violation of the ADA because it was inaccessible to blind and visually impaired users. [To read the court’s decision see *Gil v. Winn Dixie Stores, Inc.*, 257 F.Supp. 3d 1340 (2017)].

Title III of the ADA (the “Act”) prohibits discrimination based on disability in places that are open to the public and requires companies to make reasonable accommodations to eliminate barriers to accessibility. However, the Act is a bit behind the times, as there are no laws that say private websites must be ADA compliant. Despite the lack of express language in the Act related to website compliance, based on recent court decisions it appears that the courts are taking the position that the Act is meant to be applied online. One court has said that the prohibition of discrimination is not limited to tangible barriers that disabled persons face, but can extend to intangible barriers as well.

So, without any formal regulations, how do you know if your company’s website is in compliance? Many courts have been considering whether a website is ADA compliant by applying the Web Content Accessibility Guidelines 2.0 (“WCAG 2.0”) to that determination. WCAG 2.0 is a set of guidelines for making websites accessible to all. The focus is on ensuring that the website is

Q3 2018

FEATURED TOPICS

FEATURED AUTHORS

Alaine C. Doolan
Jacqueline Pennino Scheib

perceivable, operable, and understandable for those with impairments. This includes, for example, providing text alternatives to any non-text images, providing captions for audio content, using adequate text sizing, text contrasting, and the use of animation. WCAG 2.0 is split into three levels of conformance — Level A, Level AA, and Level AAA — with Level A being the minimum requirements and Level AAA being the maximum requirements. Many courts have taken the position that Level AA provides an adequate level of web accessibility without being too burdensome or expensive. Please note though that on June 5, 2018, the WCAG 2.0 guidelines were expanded to add 17 new criteria. The new criteria, which are known as WCAG 2.1, are not a replacement for WCAG 2.0 but rather are "add-ons" to the WCAG 2.0 criteria. [For more information on WCAG 2.0 and WCAG 2.1, visit W3C's website].

Based on the increasing number of lawsuits on this issue, although specific compliance rules are not mandated by law, companies may want to review their websites to confirm whether they are compliant under WCAG 2.0 and if they will be compliant under WCAG 2.1. If the answer to this statement is "no," then the company may want to consider a website update or redesign.

GC SURVIVOR KIT

Navigating the DMCA Safe Harbor Provisions

When the Digital Millennium Copyright Act (DMCA) was signed into law in 1998, it implemented numerous significant changes to U.S. copyright laws. Among other things, a key area of the DMCA is the adoption of mechanisms for protecting certain types of businesses that provide internet services from secondary liability associated with copyright infringement that may occur through the use of their services by others. In particular, the DMCA provides that service providers who provide transitory communications, system caching, storage of information on systems or networks at the direction of users, or information location tools (each, an ISP) could follow certain requirements and qualify for a "safe harbor" from liability. The requirements were outlined in 17 U.S.C. §512 and provide that:

a) the ISP must adopt and enforce a policy for terminating subscribers that are repeat infringers;
b) the ISP may not interfere with technology that helps identify infringers and protect copyrighted works; and
c) in the case of ISPs engaged in the storage of information on a system or network at the direction of a user, the ISP must:

> **(i)** have a system for notification of infringing activity and then act swiftly to remove content that it has been informed is infringing; and
> **(ii)** have a system for counter-notice to reinstate content that a subscriber believes has been wrongly removed.

Earlier this year, the case of *BMG Rights Mgmt. (US) LLC v. Cox*

Communications, Inc., No. 16-1972, No. 17-1352, No. 17-1353, 2018 U.S. App. LEXIS 2487 (4th Cir. 2018) considered the question of the appropriate scope of the safe harbor requirement to adopt and enforce a policy for terminating repeat infringers. The procedural background of the case was that Cox was appealing a jury trial decision that found Cox liable for willful infringement of music copyrights and awarded BMG $25 million in statutory damages. Cox appealed on the grounds that the district court should have granted Cox's motion for summary judgment on the basis of the DMCA safe harbor provisions and failed to properly instruct the jury on contributory infringement. The Fourth Circuit rejected Cox's claim that it met the safe harbor requirements, but remanded to district court on the issue of jury instructions. This article focuses only on the safe harbor elements of the decision.

Cox argued that it had met the requirements of the applicable DMCA safe harbor provisions. Specifically, Cox argued that it had a policy, as required, and that it enforced that policy. Cox also argued that the DMCA's use of the term "infringers" was intended to apply to infringers who were adjudicated as infringers by a court of law. The court quickly concluded that the plain language of the DMCA did not require a narrow reading of the term "infringers" such that they need to have been *adjudicated* infringers by a court of law. In assessing whether Cox had implemented a policy that provided for termination in appropriate circumstances, the court determined that while a policy did exist, it did not meet the requirements for either terminating repeat infringers or swiftly removing infringing content.

The facts of the case reflected that Cox had a 13-strike process for receipt of notifications of infringement, which included numerous additional chances and reactivation standards. The evidence also showed that the process rarely resulted in termination of infringers and, in those instances where infringers were terminated, Cox routinely reinstated the terminated user after a very brief period. Cox's internal email traffic referred to these reactivations as a "start over" and, as one email stated, their general perspective was that "DMCA = reactivate." In addition, the trial record showed that Cox engaged in a practice of blacklisting certain persons such that their notices of infringement were never acted upon. For example, the trial produced evidence that Cox decided to automatically delete notices received from BMG's agent, Rightscorp and, therefore, that all notices of music copyright infringement originating from Rightscorp on behalf of BMG were never acted upon despite the existence of a DMCA-related policy. Not surprisingly, in light of these facts, the court held that the trial court had not erred in concluding that Cox did not meet the safe harbor requirements.

The DMCA-granted safe harbor is designed to insulate ISPs from liability over which they have minimal control, and also to encourage ISPs to be a part of the solution to help stop infringing uses. The Cox case illustrates how quickly the basic requirements of the DMCA can get overwhelmed by business revenue goals. Stick to the basics with a simple notification process and meaningful action to both remove content that is infringing and, subsequently, to terminate users that repeatedly infringe. The risk of losing the safe harbor protections can quickly outweigh the minimal revenue that is saved by not removing infringing content and not terminating repeat infringers.

DID YOU KNOW?

Managing the Labeling Requirements of Prop 65

Do you manufacture, distribute, or supply consumer products that are sold in California? If yes, do your products contain warnings that are Proposition 65-compliant and are the warnings compliant with the Amended Proposition 65 rules that went into effect on August 30, 2018?

What is Proposition 65?

In 1986 California approved an initiative to address concerns about exposure to toxic chemicals. That initiative became the Safe Drinking Water and Toxic Enforcement Act of 1986, which is better known by its original name, Proposition 65. Proposition 65 requires (i) the State to publish a list of chemicals that the California Office of Environmental Health Hazard Assessment (OEHHA) has determined to cause cancer or birth defects or other reproductive harm; and (ii) businesses with 10 or more employees to notify Californians about significant amounts of chemicals in the products they purchase. In addition, Proposition 65 also prohibits California businesses from knowingly discharging amounts of listed chemicals into sources of drinking water. Proposition 65 does not ban or restrict the sale of chemicals on the OEHAA list. Rather, the warnings are intended to help Californians make informed decisions about their exposures to these chemicals from the products they use and the places they go.

Rules under Amended Proposition 65

Proposition 65 was amended in September 2016, and on August 30, 2018, the amended rules went into effect. The amendments do the following:

- Require the addition of new “tailored” warnings that provide more specific information for certain kinds of exposures, products, and places.
- Provide for website warnings for products purchased over the Internet.
- Provide for warnings in languages other than English in some cases.
- Help to clarify the roles and responsibilities of manufacturers and retailers in providing warnings. Manufacturers have the primary responsibility for providing Proposition 65-mandated warnings. This can be done by putting warning labels on the products, providing notices to distributors, importers or retail outlets, or entering into written agreements with retailers to modify the allocation of responsibility.

Warning Label Requirements

Some, but not all of the requirements for the warning labels are as follows:

- The warning must be “clear and conspicuous.”
- The warning will say the product “can expose you to” a Proposition 65 stipulated chemical rather than saying the product “contains” the chemical.
- The warning must contain the ⚠ symbol.
- (The symbol can be found at https://www.p65warnings.ca.gov/warning-symbol)
- The word “WARNING” must appear to the right of the warning symbol and be in all capital letters and bold print. The symbol must be in a size no smaller than the height of the word “WARNING.”

An example of a warning notice under the amended rules is as follows:

⚠ **WARNING:** This product can expose you to chemicals including arsenic, which is known to the State of California to cause cancer. For more information, go to www.P65Warnings.ca.gov.

The Safe Harbor provisions under Proposition 65 do allow for long-label form and short-form warnings. Information on both can be found here.

Enforcement of Proposition 65

The California Attorney General’s Office enforces Proposition 65. Any district attorney or city attorney (for cities whose population exceeds 750,000) may also enforce Proposition 65. In addition, any individual acting in the public interest may enforce Proposition 65 by filing a lawsuit against a business alleged to be in violation of this law. Penalties for violating Proposition 65 by failing to provide warnings can be as high as $2,500 per violation per day.

Note: This article does not cover all of the requirements or exceptions to Proposition 65 or its safe harbor provisions. For more information on these warning label requirements please visit https://oehha.ca.gov/proposition-65/law/proposition-65-law-and-regulations.

Contributors:

Jacqueline Pennino Scheib | Alaine C. Doolan

Nathaniel T. Arden | Kelly Frye Barnett | William J. Egan

Benjamin C. Jensen | Andrew W. Monthey | Brian E. Moran | James R. Nault

Kathleen M. Porter | Melissa (Lisa) Thompson

For additional information, please contact one of the lawyers listed above or another member of Robinson+Cole's Intellectual Property + Technology Group. For insights on legal issues affecting various industries, please visit our Thought Leadership page and subscribe to any of our newsletters or blogs.