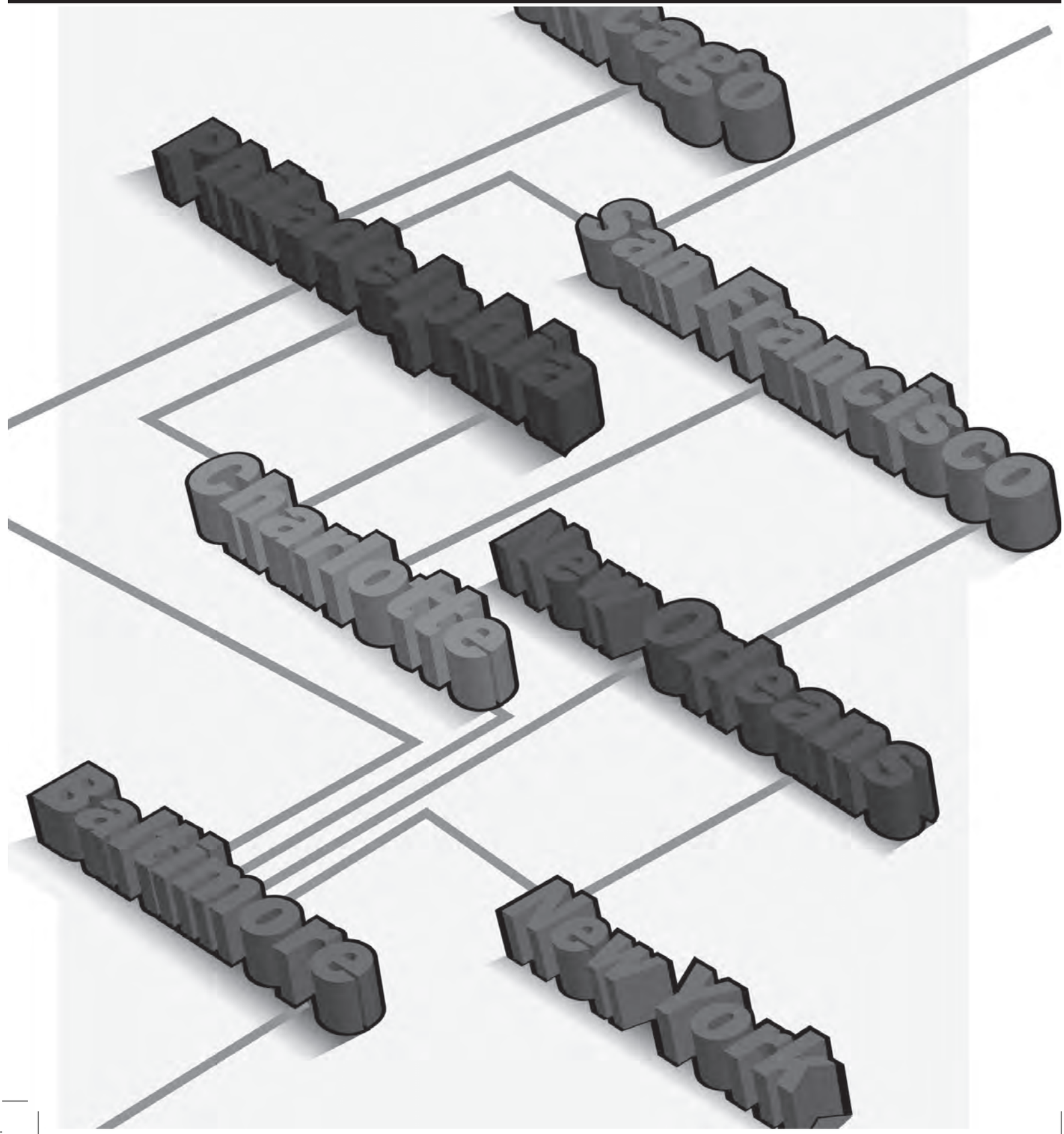
Catching the Tiger By the Tail— Counseling the Burgeoning Government Use of Internet Media

by Carl E. Brody, Jr.[1]



Internet media has grown exponentially, and many local governments are taking advantage of the benefits of social networking. "Internet media," as the term is used here, consists of Web sites operated by governmental entities or elected officials, including public sites, social networking sites (e.g., Facebook, Twitter, YouTube), sites initiated by the public body or its agencies, and weblogs ("blogs") maintained by the public body or its agencies. Through Internet media, local governments are able to advertise and market themselves, give notice to constituents, and provide information to residents and others, world-wide. Elected officials are using these tools as a way to interact more directly with the public and promote their individual political positions. Because Internet media use is outpacing the legislative ability to create standards and protections for the use of these new forms of communication, it's easy to inadvertently create liability for governments and their agencies. The power of this technology assures that liability and compliance concerns will need to be addressed by government attorneys now and in the foreseeable future. This article will look at some of the federal legislation that affects the use of Internet media.

The DMCA

In 1998, Congress passed a law[2] as a part of the Digital Millennium Copyright Act (DMCA), seeking to create a conditional "safe harbor" to shield Internet service providers (ISPs) from being held liable for the actions of their users. The service-provider designation applies to both primary and secondary providers, so long as the ISP is not responsible for the posting of infringing material. A primary provider is an ISP that creates a Web site that interacts with the public and allows public comment or posting; a secondary provider uses outside Web providers (e.g., Facebook, YouTube or Twitter) to network. The DMCA protects both categories of provider when the potentially infringing content is posted by a user, without modification of the content by the ISP.[3] The intent is to protect providers from the misdeeds of others in order to foster the free and open exchange of information; therefore, the DMCA apportions blame to the person or entity actually responsible for infringing on a copyright through an Internet posting. Strict compliance with the terms of Section 512 is required, though, to retain the protections of the Act.

Title 17 U.S.C. § 512(a) limits the liability of ISPs in copyright infringement challenges based on the provider's transmission, routing, or providing connections for material through its system or network, but only if the transmission was initiated by a content user and automatically transmitted to the Web, without selection of the recipients, without making a copy that is retained, and without modification of the material.[4] What this means is that, when a governmental body operates an Internet media site that allows users to view and post comments, it will not be found liable for the content provided by a user, so long as transmission of the content is automatically released by the provider's computer system. This will afford protection in almost all social networking circumstances, as the purpose of these applications is to be open and interactive with outside users. Provider computer systems automatically release content consistent with the legislative intent of allowing open and free discourse through the Internet. Alternately, an ISP may block responses and postings by outside users, but this option is inconsistent with the reason for social networking and, though it may cure potential copyright claims, it is not generally consistent with a desire to create open and robust social networking.

Further subsections of § 512 expand Internet media protections,[5] but the exemption does not apply where the service provider has specific knowledge that certain content on its site infringes the copyright of another and takes no action to remove the material.[6] Consistent with this, there is no liability to an ISP for removing user content if the action is taken in a good faith belief that the content violates copyright. On the other hand, if the content is provided by a subscriber, the ISP must take the extra step of providing notice of the removal.[7] Subscribers must also be informed of the ISP's policy prohibiting repeat infringers.[8] Subscribers receive extra protection because they are essentially secondary providers and may not be directly responsible for postings made by their users which affect the primary provider. Finally, an ISP must provide a designated agent to receive claims of infringement.[9] This can be satisfied by including basic information about a contact person on the Web site.

To protect providers from potential liability for the removal of content, as directed above, any misrepresentation that material is copyright protected when, in fact, it is not violates the Act, and subjects the violator to damages, costs, and attorneys' fees.[10] Assertion of this provision is similar to frivolous lawsuit prohibitions.

The application of the Act is currently under review by the courts, but some basic outlines and standards have been set. For example, in *Corbis Corp. v. Amazon.com, Inc.*,[11] the court determined that an ISP would receive copyright protection under § 512 so long as it complied with the requirements of subsection (i). To satisfy this requirement, the ISP needed to have a policy to address copyright violation claims. Amazon, the defendant, attempted to comply with this mandate by a participation agreement establishing guidelines for use of the site, and prohibiting the posting of material that the user knew to be in violation of copyright law. The plaintiff claimed that the language in the agreement was too vague. The court disagreed, holding that even vague language was sufficient to satisfy the statutory standard, as Congress was not specific in drafting the provision and, as such, intended service providers to have some measure of leeway in protecting themselves through the exemption.[12] This suggests that, so long as a government ISP provides language similar to that in

continued on page 8



Carl E. Brody, Jr. is a Senior Assistant County Attorney with the Pinellas County Attorney's Office in Clearwater, Florida, representing County Communications, along with several other County departments. Mr. Brody began his career as a Legal Counsel for the Illinois State Senate Minority Leader and as a litigation attorney for the Chicago firm of Evans & Lowenstien. A graduate of Howard University and the University of Oregon Law School, he is also a member of the Illinois and Florida Bars.

 continued from page 7

Amazon's agreement and obtains the user's acknowledgment of the prohibition against downloading copyright-protected material, the §512 protections will remain in place.[13] Based on this interpretation, a disclaimer including the requirements in subsections 512(c)(2) and (i) of the Act should be sufficient to satisfy the demands of § 512.

The courts have also addressed how a complaint for copyright infringement is to be raised. Subsection 512(c)(3) provides two basic requirements: notice to the ISP of the copyrighted work that has been infringed and is currently being displayed on the provider's site, and a good faith belief that the display constitutes an infringement. The notice requirement is straightforward but very specific, and will be satisfied only upon sufficient information being provided to the ISP to identify the complainant and material allegedly being infringed. Failure to strictly comply with these requirements will allow an ISP to ignore the complaint.[14] The good faith element has been interpreted to apply a subjective standard, based on the complainant's belief that the displayed material infringes on his or her copyright,[15] but the complainant must do more than just identify the allegedly infringing material.[16] After receipt of a good faith complaint, the provider must remove the allegedly infringing material. Prompt removal will retain immunity,[17] even if it is later determined that the removal was in error. As long as the provider informs the subscriber whose material was removed, there will be no liability to the ISP.[18]

Section 512 provides full immunity for local government ISPs, but strict compliance with its rules is required. To retain these protections, create written policy statements consistent with § 512(c)(2), (g)(2) and (3), and (i). Include a disclaimer section on the Web site that at least recognizes the ISP's compliance with § 512, and requires a user or subscriber to acknowledge awareness and agree to comply. Finally, members of the public body designated to manage the Web site must be trained in how to respond to complaints in compliance with the Act. Taking these steps will assure that the liability protections of § 512 are retained.

The CDA

In a landmark decision, *Reno v. Am. Civil Liberties Union*,[19] the U.S. Supreme Court held that the Communications Decency Act (CDA), 47 U.S.C. §§ 223(a) and (d), violated the First Amendment right to free speech. However, the lesser known 47 U.S.C. § 230, which provides general liability protection for service providers, was not challenged and remains in effect. Section 230(c)(1) (the "Good Samaritan Law") provides immunity for ISPs publishing material on the Web,[20] and exempts them from liability for information posted by users or for any actions taken in good faith to restrict access to obscene, lewd or otherwise objectionable postings.[21] This exemption extends to preempt all state and local laws that may be in conflict with the Act.[22] Excluded from protection, though, are challenges based on intellectual property rights.

The CDA distinguishes between "interactive computer services"— an ISP that allows access by multiple users — and an"information content provider," an ISP that retains responsibility for the creation or development of information provided through the Internet. The former receives the exemption because it lacks the necessary control element, while the latter is unprotected. Local government sites can fall under either category, depending on their level of direct control over content posted on their site; therefore, this is the first issue to address in reviewing a social networking site.

In *Doe v. Sexsearch.com*,[23] a user sued an Internet dating service after he was introduced to, and had sex with, an underage partner, resulting in criminal proceedings against him. The plaintiff's action was based on his allegation that Sexsearch.com warranted that the participants on the Web site were all 18 years of age or older.[24] In its analysis, the court noted that a site like Sexsearch.com could simultaneously be both an interactive computer service and an information content provider. The critical issue was whether the site "acted as an information content provider with respect to the information that [Plaintiff] claim[s] is false." [25] Based on the facts, the court found the § 230 exemption applied because, even though Sexsearch.com reserved the right to modify the content of profiles on its site, Doe did not allege that it specifically modified the profile at issue; therefore, the control element was missing.[26] This allowed the site to retain its designation as an interactive computer service.

The next issue that courts examine is whether an ISP operates as only a publisher or speaker, because the exemption applies only to these categories. In *Barnes v. Yahoo!, Inc.*,[27] an estranged boyfriend posted nude pictures of Barnes, his ex-girlfriend, on a membership directory run by Yahoo, Inc. The ex-boyfriend conducted discussions in Yahoo's chat rooms posing as Barnes and directed male correspondents to fraudulent profiles he had created. These included the actual contact information for Barnes. Barnes followed Yahoo's procedures to have the profiles/photos removed, but they remained. During this time, she received an assurance from Yahoo's Director of Communications that the posts would be removed.[28] Barnes sued, relying on negligent undertaking and breach of contract. Yahoo responded with motions to dismiss based on its immunity under § 230. The U.S. Court of Appeals for the Ninth Circuit focused on when a plaintiff's theory of liability would treat an ISP as a publisher or speaker.[29] Examining the definition of "publisher," the court determined that all acts of removing content from the site were consistent with that general definition; therefore, § 230 immunity applied.[30] Conversely, the court found that Yahoo was not entitled to immunity on the contract claim (promissory estoppel, based on its employee's failure to follow through on the promise to remove the offending material), as the promise was not consistent with the act of publishing or speaking.[31] This case provides an abject lesson to warn clients not to correspond directly with users or other third parties regarding actions that will be undertaken by the government ISP on their behalf. Otherwise, the client runs the risk of acting outside of the publisher or speaker rule and forfeiting the protections of § 230.

The rule to be gleaned from the foregoing is to retain the limited role of a "publisher of an interactive computer service" status. Current technology allows a service provider to maintain

an arm's length approach to the day-to-day operation of Internet media, thereby supporting entitlement to immunity as the "control over content" element is missing. Simultaneously, the provider must comply with the removal provisions of the Act in order to retain the "publisher" role. Creating a policy in compliance with these limits will assure that the protections of § 230 remain in place.

The SCA

The Stored Communications Act (SCA)[32] prohibits a party from intentionally accessing an electronic communication service and then obtaining or altering communications found therein without authorization. In one SCA case, *Van Alstyne v. Electronic Scriptorium, Ltd.*, [33] the Fourth Circuit reviewed a jury verdict for statutory and punitive damages against an employer found liable for accessing the personal e-mail account of a former employee, even though the account was on the company's computer system. The e-mails were held in an electronic communications service, a service providing users with the ability to send or receive electronic communications.[34] Because the account originated with an outside service, accessing it from the home site or any other computer was a violation of the Act, and subjected the employer to a minimum $1,000.00 fine.[35] Yahoo, AOL, and other personal e-mail services are protected from outside access; conversely, an employer's internal service might not be subject to this rule as it is not within "electronic communications services" in the SCA. This distinction allows government employers to access their internal systems without fear of reprisal, but this should be undertaken carefully and according to any internal rules and policies of your client. The final holding in *Van Alstyne* is instructive as it interpreted the SCA to require a plaintiff to prove actual damage in order to receive the statutory minimum damages award.[36] However, punitive damages and attorneys' fees were available to a plaintiff without proof of actual damages if the violation of the Act was willful or intentional.[37] What this means is that an Internet media policy must make employees aware of the potential liability created through the SCA in similar situations.

The ADA

Local governments are required to comply with the Americans with Disabilities Act[38] (ADA) and, if the government entity receives federal funds, Section 508 of the Rehabilitation Act of 1973, as amended.[39] This compliance can be achieved by providing qualified individuals with disabilities with equal access to programs, services, or activities through the Internet Web site. The only exception to this allows non-compliance if compliance would fundamentally alter the nature of the provider's programs, services, or activities, or would impose an undue burden.[40] Alternatively, the government may employ alternatives in providing information to disabled individuals regarding government programs or services, such as a staffed telephone information line. Unfortunately such alternatives will likely not provide an equal degree of access, as compared to online access; therefore, their use should be limited and justified by the undue burden standard referred to above. In order to fully comply with these rules, most attorneys will need the assistance of their client's Web developer or other information technology specialist. Providing alt tabs, long descriptions, and captions, as well as posting alternate options for obtaining information posted on the Web site, will go a long way toward compliance, as will a policy that acknowledged the entity's Web site will be accessible. The U.S. Department of Justice provides information online to assist localities with the technical aspects of complying with the ADA rules.[41] Following these directions in conjunction with a qualified technical expert should be sufficient to protect government clients from liability for non-compliance.

Conclusion

Internet media will be with us for the foreseeable future, and governmental entities will rightly desire to take advantage of the benefits inherent in the varied structures that are being created. Now is the time to establish policies and procedures for governmental clients to ensure, to the greatest extent possible, that the government employees and officials involved, either personally or on behalf of the government, are aware of their responsibilities and the potential liabilities that may arise. This is also the time to become more comfortable with the rights and protections that have been enacted to allow the free and open flow of information through the various media. Understanding the problems and protections that are implicated in this arena is the first step toward providing competent advice, but remain engaged — the technology and legal issues are continually evolving, and require attorneys to be aware and adaptable.

Notes

1. A longer version of this article was first published in *The Florida Bar Journal* (December 2009, Vol. 83, No. 11).
2. Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, 112 Stat. 2877 (1998).
3. 17 U.S.C. § 512(k)(1) (West 2009).
4. 17 U.S.C. § 512(a); *see* Parker v. Google, Inc., 422 F. Supp 2d 492, 497 (E.D. Pa. 2006) (when an ISP automatically and temporarily stores data without human intervention so that the system can operate, the necessary element of volition is missing for a copyright infringement claim).
5. 17 U.S.C. § 512(b) to (e), providing protection for system-caching, storage of content, linking, and limitation on liability of nonprofit educational institutions.
6. 17 U.S.C. § 512(c) (1).
7. 17 U.S.C. § 512(g).
8. 17 U.S.C § 512(i).
9. 17 U.S.C. § 512(c)(2).
10. 17 U.S.C. § 512 (f). *See* Online Policy Group v. Diebold, Inc. 337 F. Supp 2d 1195 (N.D. Cal. 2004) (plaintiff violated DMCA misrepresentation provision by attempting to shield non-copyright material from being posted on Web site through copyright claim).
11. 351 F. Supp. 2d 1090 (W.D. Wash. 2004).
12. *Id.* at 1100-01.
13. *Id. See also*, Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) (DMCA's infringement policy requirement has three prongs, requiring a service provider to: (i) adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances; (ii) inform users of the service policy; and (iii) implement the policy in a reasonable manner).

continued on page 36

Government Use of Internet

cont. from page 9

14. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Serv., Inc. 351 F. 3d 1229, 1236 (D.C. Cir. 2003); Perfect 10, Inc. v. CCBill, LLC, 488 F. 3d 1102, 1112 (9th Cir. 2007).
15. *See* Rossi v. Motion Picture Ass'n of Am., Inc., 391 F. 3d 1000, 1004 (9th Cir. 2004).
16. *See* Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150 (N.D. Cal. 2008) (copyright owner is required to consider any fair use doctrine defenses prior to issuing DMCA notice).
17. Io Group , Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1150 (N.D. Cal. 2008) (company's policy of removing content within days of receiving DMCA complaint protected it from liability for publishing copyrighted material).
18. 17 U.S.C. § 512(g) (West 2009).
19. 521 U.S. 844 (1997).
20. Until recently, immunity was thought to be limited to torts, specifically defamation and libel, but the Ninth Circuit, in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 489 F.3d 921 (9th Cir. 2007) *aff'd en banc,* 521 F. 3d 1157 (9th Cir 2008), closely examined the language of the statue and determined that immunity was absolute.
21. 47 U.S.C. §§ 230 (c)(1) - (2) (West 2009).
22. 47 U.S.C. § 230(e)(3).
23. 502 F. Supp. 2d 719 (N.D. Ohio 2007).
24. *Id.* at 723-24 (plaintiff alleged 14 claims in tort and contract).
25. *Id.* at 725, quoting *Anthony v. Yahoo! Inc.*, 421 F. Supp.2d 1257 (N.D. Cal. 2006).
26. *Id.* at 727-285.
27. 570 F.3d 1096 (9th Cir. 2009).
28. This occurred just before a local news program was to broadcast a report on the incident. The posts were not removed until after Barnes had filed her lawsuit. *Id.* at 1098-99.
29. *Id.* at 1102-03.
30. *Id.* at 1103 ("the duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles").
31. *Id.* at 1109. Because that issue had not been fully considered by the district court, the Ninth Circuit remanded.
32. 18 U.S.C. §§ 2701-2711 (1986).
33. 560 F. 3d 199 (4th Cir. 2009).
34. U.S. v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003).
35. 18 U.S.C. § 2707.
36. 560 F. 3d at 208.
37. *Id.* at 209.
38. 42 U.S.C. § 12101 *et seq*. (1990).
39. 29 U.S.C.A. § 794d (electronic and information technology accessibility guidelines).
40. 28 C.F.R. § 36.104. This defines "undue burden" in part, as meaning "significant difficulty or expense."
41. U.S. Dept. of Justice, Civil Rights Division, *Accessibility of State and Local Government Websites to People with Disabilities* (June 2003) at http://www.ada.gov/websites2.htm (providing local government IT specialists with information about making government Web sites comply with the ADA). *See* the website for information on the DOJ's toll-free ADA Information Line that provides access to ADA specialists during business hours. ML

The Fourth Amendment

cont. from page 13

30. By contrast, apprehension by the use of deadly force would constitute a seizure, as established by *Tennessee v. Garner,* 471 U.S. 1, 7 (1985) ("[A] pprehension by the use of deadly force is a seizure subject to the reasonableness requirement of the Fourth Amendment"). *See also* Carr v. Tatangelo, 338 F.3d 1259, 1268 (11th Cir. 2003) ("Officer Fortson had shot to kill to save the life of Officer Tatangelo, and it is his intent and the physical contact of the bullet from his gun that governs our Fourth Amendment, seizure analysis. Although Carr was not immediately stopped ... by the bullet from Officer Fortson's gun, he nevertheless was seized within the meaning of the Fourth Amendment when the bullet struck or contacted him").
31. 240 Fed. Appx. 104 (7th Cir. 2007).
32. *Id.* at 111.
33. *Id.* at 127.
34. 341 F.3d 600 (7th Cir. 2003).
35. *Id.* at 603.
36. *Id.* at 605. In *Croal v. United HealthCare of Wisconsin, Inc.*, No. 07-CV-837, 2009 WL 913641, *15 (E.D. Wis. Mar. 31, 2009), police responding to a domestic violence complaint used a taser on a family member. Other relatives came outside to protest, and were knocked down by the officers trying to arrest a different individual. The court ruled that the alleged intentional conduct of a police officer arresting a different individual was not a seizure of the plaintiffs under the Fourth Amendment. *Compare Acevedo v. Canterbury*, 457 F.3d 721, 725 (7th Cir. 2006) (distinguishing *McCoy* where officer responded to call of a disturbance and punched plaintiff in the face, causing him to fall to the ground; after plaintiff was treated at hospital, he was brought to police station where he was arrested for assault. "Not only did [the officer] knock him to the ground in a location far away from his home under the general control of the police (the auto pound); the force of that blow caused Acevedo to black out momentarily. Even after he regained consciousness, he claims that he remained in a daze for a time[.]").
37. 50 Fed. Appx. 300 (6th Cir. 2002).
38. *Id.* at 302.
39. No. 05-73244, 2007 WL 1768767, *3 (E.D. Mich. June 15, 2007).
40. *Id.*
41. No. 02 C 6248, 2005 WL 3359124, *3 (N.D. Ill. Dec. 08, 2005).
42. *Id.*
43. *See* County of Sacramento v. Lewis, 523 U.S. 833, 843 (1998) (where there is no search or seizure, the use of force is unconstitutional only if it shocks the conscience under the Fourteenth Amendment). Excessive force claims under the Fourth Amendment are analyzed under a "reasonableness" standard. *See* Graham v. Connor, 490 U.S. 386, 395 (1989). ML

Defending Title II

cont. from page 17

rights-of-way are reserved.
15. 28 C.F.R. § 35.151.
16. Kinney v. Yerusalim, 9 F.3d 1067, 1073 (3d Cir. 1993). *See also* Reichenbach v. City of Columbus, No. 2:03-CV-1132,