Communications Lawyer
Publication of the Forum
on Communications Law
American Bar Association
Volume 25, Number 1, Spring 2007
THE JOURNAL OF MEDIA, INFORMATION, AND COMMUNICATIONS LAW

In this issue

Privilege Paves the Road to Dismissal in Defamation Cases

BY GAYLE C. SPROUL AND JEANETTE MELENDEZ BEAD

Given the pivotal role of truth in a defamation action,[1] it is not uncommon for plaintiffs to resist the full disclosure of evidence bearing on the truth of the statements they challenge. When the information is crucial to the case, courts routinely order plaintiffs to produce it; and, in a typical case, they comply. But sometimes the plaintiff cannot produce the information because it is privileged, its disclosure would violate some law or rule of ethics, or it is not available to either the plaintiff or the defendant. If that is an accurate assessment of the circumstances, how can the case be fairly prosecuted or defended? The answer is that it cannot be. In those instances where the defendant is deprived of evidence that is of central importance to the defense of a defamation action, the action must be dismissed.

Although this proposition may seem Draconian, it is a matter of fairness and the justifiable consequence of a failure of proof. In the normal course of events, courts supervising discovery have the power to dismiss cases in which a plaintiff fails to produce critical evidence. In most jurisdictions, as a matter of rule[2] and precedent,[3] it is well settled that a plaintiff must disclose in discovery information that he himself has put in issue, or the court will dismiss his case. These cases permit dismissal as a sanction for a plaintiff's willful refusal to produce evidence or for a plaintiff's obstruction of the use of such evidence. Simply put, fundamental fairness requires that a defendant be allowed to discover and explore the facts underlying the claims that a plaintiff has put in issue.

Should there be a distinction, though, where the plaintiff can accurately say that his hands are tied, i.e., where a privilege (e.g., state secrets privilege or attorney-client privilege) bars him or another party from disclosing the information, or a law (right against self-incrimination) gives him a constitutional right to refuse to divulge the information? Those courts that have squarely wrestled with the issue say no. Whether a plaintiff willfully or involuntarily refuses to produce evidence, the defendant is deprived of information critical to its defense, and the plaintiff cannot carry the burden imposed by *Philadelphia Newspapers, Inc. v. Hepps*[4] to prove falsity. Dismissal is appropriate when the merits of the controversy at issue are "inextricably intertwined with privileged matters."[5]

State Secrets Privilege

The state secrets privilege, a privilege that protects from disclosure classified government information, has proven the most fertile ground for the test of the principle of dismissal for refusal to produce evidence in defamation actions.[6] Indeed, at our firm we have dubbed a motion to dismiss on this basis a *Trulock* motion, referring to *Trulock v. Lee*,[7] a case in which the Fourth Circuit affirmed the dismissal of a defamation action because factual questions about the truth or falsity of the statements at issue could

(Continued on page 38)

Gayle C. Sproul is a partner in the Philadelphia office of Levine Sullivan Koch & Schulz, L.L.P. Jeanette Melendez Bead is a partner in the firm's Washington, D.C., office. *The authors thank Benjamin Battles of Brooklyn Law School and Aaron Johansen of the George Washington University School of Law for their research assistance.*

FROM THE CHAIR

RICHARD M. GOEHLER

Richard M. Goehler

After you have had a chance to read this edition, I am sure you will agree with me that *Communications Lawyer* is a "must read" for all legal professionals in the communications industry. This edition, like so many of those before it, includes a wide variety of excellent articles on a very broad spectrum of topics impacting the communications bar. As you will see, the contributions include an analysis of cases involving a defamation defendant's inability to obtain privileged information through discovery, and two timely articles on FCC regulatory issues. Also included are cutting edge articles on social networks and Voice over Internet Protocol (VoIP), helping to keep our Forum membership up to date on these evolving issues within the industry. There is also a very creative work of fiction illustrating the use of the First Amendment Due Process argument in criminal actions under the Espionage Act. We also have a very practical practice pointers article—the first in a series on litigation techniques—providing tips and offering insight and concrete suggestions on trial techniques. I hope you find this edition as interesting and enjoyable as I did. Thanks to our editors and contributing authors for a job well done!

As I was reading through the contributions for this edition of *Communications Lawyer*, I received my copy of the Spring 2007 edition of the *Journal of International Media & Entertainment Law*, which the Forum co-publishes with the Donald E. Biederman Entertainment & Media Law Institute of Southwestern Law School. The *Journal*'s table of contents on its cover immediately impressed me. This *Journal* includes a diverse group of articles covering topics on pro-competitive restraints of the trade in women's professional tennis, museums, digitization and copyright law, Internet and wireless license agreements for motion pictures and television programming, and resale royalty works in France. Very impressive.

It strikes me that the depth and breadth of substantive articles that are consistently included in our *Communications Lawyer* and *Journal* mirror the CLE programs that the Forum continues to plan and present. We are only halfway through the year and we have already presented a very successful 12th Annual Conference, along with the 10th Annual Media Advocacy workshop in Key Largo in February.

In March, we presented our 2nd Annual Data Privacy Conference in Washington, D.C. with our co-sponsor, the Federal Communications Bar Association. Planning is already underway for next year's conference, which will surely be as outstanding as our first two programs.

Our 26th Annual "Representing Your Local Broadcaster" program was held in Las Vegas at the Bellagio on April 15, 2007. Kudos to Guylyn Cummins and her program committee, who planned and presented a very practical seminar covering daily issues facing broadcast lawyers. The Vegas program was a daylong conference packed with substantive presentations on regulatory compliance, advertising, privacy in the digital age, newsgathering, and intellectual property issues impacting the broadcast industry. If you have not been a regular attendee to our Las Vegas program in the past, I would strongly encourage you and your colleagues to consider attending next year. The program is always held on the Sunday immediately preceding the National Association of Broadcasters Annual Convention. We continue to value and benefit from our "co-sponsorship" of this annual program with our partners, the NAB and the FCBA.

We intend to complete our 2007 ABA year with some new substantive CLE programs. Planning is under way on the development of our new teleseminar initiative. We are expecting to present two to three "hot topic" teleseminars, and we are confident that these seminars will further enhance our CLE offerings and programs for our membership.

Next year's annual conference, our 13th, returns to the Boca Raton Resort & Club on February 14-16, 2008. The planning committee has begun its work, and any input on program ideas and workshop topics is, of course, always welcome.

We encourage each of you to make your Forum membership as worthwhile as possible. Take advantage of the benefits of Forum membership. Our *Communications Lawyer* and *Journal* editors are always looking for content and articles for our publications, and the planning committees for our programs and conferences are always happy to receive feedback and input. Feel free to contact me at any time if I can be of assistance to you on Forum matters.

Richard M. Goehler (rgoehler@fbtlaw. com) is a partner in the Cincinnati office of Frost Brown Todd LLC representing clients in all aspects of media law, advertising, promotions and sweepstakes law, and litigation of trademark and copyright matters.

Communications Lawyer (ISSN: 0737-N7622) is published quarterly by the Forum on Communications Law of the American Bar Association, 321 North Clark St., Chicago, IL 60610-4714. POSTMASTER: Please send address corrections to ABA Service Center, 321 North Clark St., Chicago, IL 60610-4714.

Communications Lawyer is aimed at attorneys and other communications specialists. It provides current practical information, public policy, and scholarly articles of professional and academic interest to its members and other readers.

Doe v. MySpace, Inc.: Liability for Third Party Content on Social Networking Sites

MICHAEL D. MARIN AND CHRISTOPHER V. POPOV

MySpace is a Web 2.0 phenomenon. In less than four years, it has become one of the most visited sites on the Web, boasting over 150 million user profiles and wielding unprecedented potential for collaboration and marketing power. The MySpace concept, often referred to as online social networking, is simple. MySpace users create online profiles, or personal webpages, on which they post photographs, videos, and information about themselves. These profiles serve as a platform for users to network with an online community of people with common interests. This simple concept has revolutionized online advertising, politics, news, music, and ordinary Internet chatter.

But the tremendous popularity of social networking has been tarnished by a parallel public outcry over sexual predators who use the Internet to meet and seduce minors into having sex. This outcry has captured the attention of both politicians and plaintiffs' lawyers.

In June 2006, a fourteen-year-old girl and her mother filed a highly publicized lawsuit in Austin, Texas, against MySpace and its parent, News Corp., after the girl was sexually assaulted by a man she allegedly met on MySpace. The plaintiffs' suit, *Doe v. MySpace, Inc.*, sought $30 million in damages and alleged that MySpace and News Corp. were negligent and grossly negligent for failing to implement age verification procedures and to protect the fourteen-year-old from sexual predators. If successful, the suit would have been a significant, if not fatal, blow to social networking.

Last February, however, Judge Sam Sparks of the Western District of Texas dismissed the *Doe* case.[1] Relying upon the immunity afforded to "interactive computer services" under the Communications Decency Act (CDA) and upon Texas common law, the court held that MySpace could not be required to implement age verification procedures nor be held liable for claims flowing from its users' online communications.

Although the *Doe* case allowed MySpace and other social networking sites to breathe a temporary sigh of relief, it is unlikely to end attempts to hold such sites liable for their users' conduct. The *Doe* case is on appeal, and four new sexual predator suits have been filed against MySpace in Los Angeles.[2]

Political pressures continue to mount as well. A coalition of forty-four state attorneys general are pushing for laws that would require social networking sites to verify the age and identity of their users and to implement various protections for minors who use the sites, and at least one state legislature is currently debating such a bill.[3]

This article sets forth the legal defenses available to social networking sites faced with private lawsuits stemming from the criminal or tortious conduct of individuals who use the sites to harm another person. The article also discusses why proposed state statutes aimed at holding these websites liable for third party conduct are unlikely to survive legal scrutiny.

Defending Private Lawsuits

Social networking websites are not the first entities to encounter lawsuits based upon third party conduct. For years, plaintiffs have sought to hold traditional e-mail and Internet service providers liable for publishing defamatory or otherwise actionable content generated by third party users. Even before the advent of the Internet, parties sought to hold defendants with deep pockets liable for the tortious or criminal acts of a third person. Furthermore, social networking sites are not the first sites to face demands for online age verification; Congress has tried for nearly a decade to impose such a requirement on Internet sites offering pornography.

Claims based on these theories of liability have been largely unsuccessful and have given rise to well-established legal defenses. First, in light of the Communications Decency Act of 1996, courts have been virtually unanimous in their holdings that websites cannot be held liable for publication of third party content or for real world injuries that flow from the publication of third party content. Second, well-established common law principles provide that a person typically has no duty to protect another from a third party's criminal or tortious acts. Finally, the Supreme Court has made clear that requiring websites to institute online age verification violates the First Amendment because age verification is an ineffective means of protecting minors from harmful content and is an overly restrictive limitation on constitutionally protected speech.

As discussed below, these defenses apply with equal force in the social networking context and work to shield websites from liability for the criminal and tortious acts of their users.

CDA Immunity

The first line of defense against any claim based on content generated by a website's users, or based on its users' related offline conduct, is the immunity provided under the Communications Decency Act of 1996 (CDA), 42 U.S.C. § 230. In short, the CDA bars claims against interactive computer services based on the publication of third party content. Congress enacted the CDA for the stated purpose of promoting "the continued development of the Internet . . . unfettered by Federal and State regulation."[4] The act recognizes that is impossible to scrutinize the millions of postings made by users over e-mail or on Internet message boards. The act further recognizes that holding interactive computer services liable for posting defamatory or otherwise harmful user-generated content would severely diminish the online posting of third party content of all kinds.

Michael D. Marin (mmarin@velaw.com) is a partner and Christopher V. Popov (cpopov@velaw.com) is an associate in the Austin office of Vinson & Elkins, LLP. They represented MySpace, Inc. and its parent company, News Corp., in Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843 (W.D. Tex. 2007).*

To ensure that websites and other interactive computer services would not be crippled by such lawsuits, the CDA provides interactive computer services with broad immunity.[5] In pertinent part, 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."[6] Importantly, the CDA further provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[7]

In light of these provisions, courts have broadly applied CDA immunity to all claims in which

(1) the defendant is "a provider or user of an interactive computer service,"
(2) "the cause of action treats the defendant as a publisher or speaker of information," and
(3) "the information at issue" is provided by a third party information content provider.[8]

The first and third prongs are easily satisfied in the social networking context. Social networking sites are providers of interactive computer services, and user-generated profiles found on social networking sites obviously constitute information provided by third party information content providers. In cases where a third party merely posts defamatory content on his profile, the second prong of the CDA analysis is easily satisfied as well; and the website clearly cannot be held liable as the publisher or speaker of that content.

The claim in a prototypical sexual predator case, in contrast, is less about speech (the actual words published online) and more about conduct, i.e., what happens when the parties meet offline. Indeed, the words themselves may be completely innocuous. Importantly, however, the *Doe* case held that this distinction between a sexual predator case and a typical defamation case is irrelevant for purposes of CDA immunity. This holding is proper under the CDA's plain language and necessary to effectuate its legislative purpose. But to fully appreciate why CDA immunity should apply in this circumstance, it is important to consider the similarities and differences between sexual predator cases and the more typical CDA case that merely involves some form of otherwise actionable speech.

Actionable Speech

The CDA has been most frequently applied to bar defamation-based claims. In the typical case, a plaintiff who believes that he or she has been defamed online by a third person sues the website that allowed the third person to publish the defamatory statement. Because the plaintiff's claim against the website in that case is based solely on its role as the publisher of the third party content, courts have held with virtual unanimity that such claims are barred under the CDA.[9]

A website's immunity from claims based on actionable speech is not diminished by allegations that it was on notice of the content at issue. In *Zeran v. America Online, Inc.*, for instance, the victim of a vicious prank sued AOL for its failure to remove a false advertisement for T-shirts featuring tasteless slogans relating to the 1995 bombing of the Oklahoma City federal building. The ad instructed interested buyers to call the plaintiff to place an order.[10] After receiving death threats from people who were enraged by the ad, Zeran learned of the prank and immediately demanded that AOL remove the ad from its bulletin board and post a retraction. Zeran argued that even if AOL were immune from liability for the initial posting, it was negligent for failing to remove the ad after Zeran gave notice of its falsity. The Fourth Circuit, however, affirmed the district court's dismissal of Zeran's claims, explaining that the CDA necessarily protects interactive computer services from liability even after they are notified of an allegedly defamatory or threatening post because the insupportable legal burden imposed by potential tort liability would undermine the CDA's goal of promoting speech on the Internet through interactive computer services.[11]

Under *Zeran* and its progeny, websites and other interactive computer services cannot be held liable for publishing defamatory or otherwise actionable speech generated by a third party.

Actionable Speech and Resulting Physical Injuries

Although the CDA is directed at claims that seek to hold an interactive computer service liable as the "publisher or speaker" of third party content, the immunity provided under § 230(c) is not limited to defamation- or speech-based torts. Courts have routinely applied CDA immunity to bar negligence and other claims based on physical harm that a plaintiff suffered as a result of defamatory or otherwise harmful content, and they have explicitly rejected arguments that CDA immunity is limited to claims for defamation.[12]

Indeed, applying CDA immunity to torts flowing from actionable speech is necessary to effectuate the act's purpose. Many, if not all, online defamation cases can be pleaded to include a claim for negligence or some other more general tort.

A classic example of such a case is *Carafano v. Metrosplash.com, Inc.*,[13] in which an unidentified third party posted a false online personal ad on Matchmaker.com portraying an actress named Christine Carafano to be a sexually promiscuous woman in search of random sexual partners. Shortly after the ad was posted, Carafano began receiving sexually explicit phone calls, letters, and hand-delivered notes at her home. The messages were so threatening that Carafano was forced into hiding for months. After the ordeal, Carafano sued Matchmaker.com. Although the essence of her lawsuit was defamation, Carafano asserted various causes of action including negligence, and she sought damages not just for the harm to her reputation but also for the emotional damage she suffered as a result of threats she received.

The Ninth Circuit affirmed the dismissal of all the claims, including negligence, holding that under § 230(c) of the CDA, "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity."[14] In so holding, the Ninth Circuit recognized that imposing tort liability of any kind on a website for its failure to ensure that all third party postings are "safe" or otherwise problem free would threaten the viability of websites and other interactive computer services and thereby reduce the channels of communication available on the Internet.

Physical Injuries Flowing from Facially Innocuous Speech

The prototypical online sexual predator case is at least superficially distinguish-

able from the prior two categories in that the suit might not involve a speech-based tort whatsoever. In the *Doe* case, for instance, the plaintiffs asserted no claim for defamation and explicitly argued that their claims were not based upon any particular posting on MySpace.com but rather on the fact that MySpace knowingly maintained a forum in which sexual predators could communicate with and seduce minors. As such, the plaintiffs argued that the CDA did not bar their claims against MySpace.

The court, however, concluded that this attempt to plead around the immunity provided by the CDA was disingenuous. Specifically, the court noted that no matter how artfully the plaintiffs attempted to plead their lawsuit, the underlying basis of their claims was that MySpace was negligent for allowing the minor and the man who assaulted her to exchange phone numbers and other personal information on MySpace. The court observed that the sole causal connection between MySpace and the plaintiffs' injuries was MySpace's publication of the communications between the minor and her attacker. For that reason, the court found, MySpace was entitled to immunity under the CDA regardless of the particular causes of action or theories of liability that the plaintiffs actually asserted.[15]

The *Doe* court's analysis is sound both as a matter of statutory interpretation and as a matter of public policy. Although defamation and other claims based on independently harmful speech are the most common claims barred by immunity geared toward the publication of third party content, nothing in the CDA limits the scope of its immunity to defamation or other speech-based torts. Rather, the CDA states in unmistakably clear terms that interactive computer services are immune from all claims stemming from their publication of such information: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[16] Thus, any claim that seeks to hold an interactive computer service liable based solely on its causal connection as the publisher of third party content is barred under the CDA.

Furthermore, this application of the CDA to harm flowing from facially innocuous publications is just. As explained above, Congress provided for broad CDA immunity because it is the "policy of the United States" to promote the further development of the Internet. Congress realized that imposing liability on interactive computer services for the publication of third party content would have a profound chilling effect on Internet speech. Due to the practical impossibility of screening the staggering volume of third party content posted online daily, websites faced with liability for user-generated speech would have no choice but to greatly restrict the volume of third party content they publish.

Courts applying these principles have concluded that the same practical limitations apply where liability is premised on the website's failure to respond when given notice of objectionable user-generated speech on its site. These arguments were only more compelling when applied in the context of the *Doe* case, where the communications appeared harmless on their face. If interactive computer services cannot reasonably be expected to screen patently objectionable content, including content that has been identified as objectionable, logic compels that it would be even more unreasonable to expect interactive computer services to screen facially innocuous content. If social networking sites were suddenly required to ensure that the millions of third party postings published on their sites daily were not only true but also well intentioned, social networking would no longer be viable as a business model.

No Duty Principles

In addition to the statutory immunity of the CDA, negligence claims seeking to hold social networking sites liable for the conduct of its users may be barred in many instances by well-established principles of common law. To state a claim for negligence or gross negligence, a plaintiff typically must establish the existence of a legal duty, a breach of that duty, and damages proximately caused by the breach. As the *Doe* court established, there is no legal basis for the proposition that a social networking website has a duty to protect its users from the criminal or tortious actions of other users. The general rule in Texas and elsewhere is that "a person has no legal duty to protect another from the criminal acts of a third person or to control the conduct of another."[17]

The general rule, of course, has exceptions. Certain special relationships may impose a duty upon one party to control the actions of another, including employer-employee and parent-child relationships. And many jurisdictions impose a duty on owners to protect their guests from foreseeable third party criminal acts occurring on their premises. None of these exceptions applies in the case of online social networking. The website's relationship with its users is not the type of special relationship that gives rise to a duty to control their actions. With respect to MySpace, each user is merely one of over 150 million people who have posted a profile on the website. MySpace, like most of its competitors, charges no fee, so users are not even customers.

Notwithstanding this attenuated relationship between the website and its users, the plaintiffs in the *Doe* case argued that MySpace has a duty to protect its users from sexual predators. Their argument was based on the novel theory that MySpace.com is a "cyber premises" on which it is foreseeable that predators will prey upon unsuspecting children. The court rightfully rejected the argument, noting that there is no legal basis for cyber-premises liability and that imposing liability under these circumstances would mean the end of social networking: "To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks and close this avenue of communication."

Although *Doe* is the only case that addresses the issue with respect to social networking websites, it was not the first to reject the notion that interactive computer services have a duty to prevent injuries to their users. In *Doe v. GTE Corp.*, the Seventh Circuit affirmed the district court's dismissal of claims against a web hosting service for hosting clandestine videos of collegiate athletes who were unknowingly videotaped nude in a locker room.[18] Judge Easterbrook, writing for the court, rejected the notion that an Internet service provider has a duty to prevent injuries to third parties, comparing Internet service providers to other communication intermediaries, such as the postal service or a phone company,

which routinely enable third parties to commit crimes or perpetrate torts:

> Landlord, phone company, delivery service, and web host all could learn, at some cost, what [the user] was doing with the services and who was potentially injured as a result; but state law does not require these providers to learn, or to act as Good Samaritans if they do. The common law rarely requires people to protect strangers, or for that matter acquaintances or employees.[19]

Judge Easterbrook's observations are as astute as they are far-reaching. Just as phone companies and couriers have no duty to prevent third parties from using their services to perpetrate criminal and tortious activity, social networking sites should not be saddled with a legal duty to prevent third parties from using their services to commit crimes.

First Amendment Defense

In addition to claiming generally that MySpace had a duty to protect its users from one another, the plaintiffs in *Doe* argued that MySpace had a legal duty to verify the age and identity of its users; i.e., the plaintiffs argued that without effective age verification, MySpace's efforts to protect minors who use the site are meaningless. The argument echoes the primary battle cry of politicians seeking to put pressure on social networking sites to prevent sexual predators from contacting minors online. Although the *Doe* court rightly rejected this theory of liability as inconsistent with common law principles and the immunity provisions of the CDA, mandatory age verification is also prohibited by the First Amendment.

Against Age Verification

For years, Congress has unsuccessfully attempted to impose age verification requirements on websites that display pornographic images and videos. Its first attempt was embodied in § 223 of the CDA, 47 U.S.C. § 223, which criminalized the "knowing" transmission to any recipient under eighteen years of age any "obscene or indecent" message and any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Porn site operators could avoid criminal liability under § 223 by instituting age verification through certain designated forms of identification, such as a credit card or an adult identification number.[20]

Not long after the section was enacted, however, the Supreme Court issued its opinion in *Reno v. ACLU*, which held that the mandatory age verification scheme violated the First Amendment because it was not narrowly tailored to serve a compelling interest and because there were less restrictive alternative means of preventing minors from viewing adult content.[21] This conclusion turned largely on the trial court's findings that (1) there is no available technology that would permit a noncommercial website to verify the age or identity of its users, and (2) localized filtering and content-blocking software is a less restrictive and more effective means of keeping minors off of adult websites. Ultimately, the Court concluded that mandatory age verification would have a chilling effect on constitutionally protected Internet speech because (1) some adults may not have the necessary identifying credentials (e.g., credit cards), and (2) even those who have the necessary identifying credentials would be unwilling to provide them out of fear of identity theft or other misuse of the personal information.[22]

Congress's second attempt to shield minors from online pornography was embodied in the Child Online Protection Act (COPA), 47 U.S.C. § 231, which, like the CDA, imposed criminal and civil penalties on websites that made online pornography available to minors. Although COPA was designed in part to address the faults that the Supreme Court found with the CDA, it contained an affirmative age verification defense that was virtually identical to the CDA provision struck down by the *Reno* Court.

Immediately after COPA became law, a consortium of plaintiffs challenged the COPA statute in a case now called *ACLU v. Gonzales*.[23] Based largely on the Supreme Court's holding in *Reno,* the district court preliminarily enjoined the government from enforcing the age verification scheme. In 2002, the Supreme Court affirmed that preliminary injunction and remanded the case for trial with instructions to the district court to update the factual record to reflect current technological developments, account for any changes in the legal landscape, and determine whether there are more effective and less restrictive means of preventing minors from viewing pornography than an across-the-board age verification requirement.[24] On March 22, 2007, the district court issued a lengthy opinion that examined the relevant technologies and again concluded that localized filtering and content-blocking software is a less restrictive and more effective means of keeping minors off adult websites than age verification.[25]

Less Restrictive Means

The *Reno* and *Gonzales* opinions establish that however attractive it may seem to require adult websites to institute age verification, the technology for them to do so does not exist. Age verification ultimately amounts to identity verification, and the online verification process simply verifies the age of the person associated with whatever form of identification is used; there is no way to ensure that the online user is actually the person associated with that form of identification. The problem is compounded when dealing with minors, for whom there is little accessible data in the first place.[26] Accordingly, blocking software (i.e., software that restricts access to certain websites or categories of websites on a given computer) is a more effective means of shielding minors from adult content online.

The *Reno* and *Gonzales* opinions also establish that blocking software is a less restrictive means of regulating child access to adult content because it applies at the point of consumption instead of the distribution level. The opinions note that requiring all users, including adults, to present identification before viewing adult content is likely to reduce the number of adults who would otherwise view this constitutionally protected form of expression.[27] Some adults will not have the required form of identification, and some who do will not be willing to provide it out of fear of identity theft or out of a preference to visit the sites anonymously. Blocking software, on the other hand, can be installed on a given computer that is likely to be used by minors without impairing the access of adults to certain sites; and, as such,

blocking software is a more effective and less restrictive form of regulation. Thus, mandating age verification violates the First Amendment.

These arguments apply with even greater force to mainstream social networking. Although much of the speech exchanged over social networking sites might be considered trivial, there is no doubt that, on average, these sites consist of higher value speech than pornography sites. In addition to serving as a primary means of online communication for many, social networking sites have become avenues to learn more about political candidates, social causes, music, and art.[28] To the extent that the public square has ever existed in American culture, it is fair to say that it exists on MySpace, Facebook, and their competitors. Imposing liability standards that would chill access to social networking would offend First Amendment principles at their core.

Although *Reno* and *Gonzales* struck age verification requirements in federal criminal statutes, the analysis from these cases applies with full force to attempts to impose civil tort liability for failure to institute age verification. It is well established that "the application of state rules of law in state courts in a manner alleged to restrict First Amendment freedoms constitutes 'state action' under the Fourteenth Amendment."[29]

Third Party Standing

Furthermore, social networking websites should have valid third party standing to invoke the First Amendment rights of their users to invalidate an age verification liability scheme directed at the websites themselves. First, it is well established that a third party may invoke the rights of an individual if the individual is unlikely to have an opportunity to uphold her rights directly. This principle is demonstrated in *Eisenstadt v. Baird*, where the Supreme Court sustained a doctor's challenge to an anticontraceptive law based on the rights of an unmarried individual denied access to contraceptives. The Court allowed the doctor to raise the defense because the law did not subject patients to prosecution and so "denied them a forum in which to assert their own rights." Second, third parties may invoke the rights of another where there is a close relationship between the third party and the individual whose rights the third party seeks to invoke. In *Craig v. Boren*, for instance, the Supreme Court held that a bartender was permitted to challenge a state drinking age law that discriminated against men on the basis of gender because the bartender suffered economic injury through the loss of customers.

Both of these principles of third party standing should apply to social networking sites. Given that the anticipated claim—tort liability for failure to institute age verification measures—would apply to the social networking site operator, and not its users, the site operator should have the right under the first example to assert its users' rights. And social networking companies should be able to invoke their users' rights under the second example because they are closely connected to their users' constitutionally protected activity. That is, like the bartender in *Craig,* social networking companies face a restriction on their own operations through state laws aimed at their users' activities.

State Enforcement

Enterprising plaintiffs' attorneys are not the only ones demanding that social networking companies be held liable for their users' conduct. Perhaps no issue garners greater bipartisan political support than child safety, a point that is evidenced by the fact that a coalition of attorneys general from forty-four states is demanding that social networking sites be required to institute age verification.[30]

The Connecticut legislature, for instance, is currently debating legislation that would require social networking sites to implement age and identity verification for all users accessing the sites from computers in Connecticut.[31] The Connecticut bill, which is championed by Connecticut Attorney General Richard Blumenthal, would prohibit owners or operators of social networking websites from allowing a minor to create or maintain online profiles without (1) first obtaining written consent from the minor's parent and (2) giving the parent access to the profile page at all times.[32] The bill would also require social networking sites to implement procedures to verify the accuracy of age and other personal information collected from users upon registration, although the bill offers no explanation of how such information would be verified. Companies failing to comply with the bill's age verification requirement would be subject to injunctions and statutory penalties under Connecticut's unfair trade practices act. What is more, Attorney General Blumenthal has publicly stated that ten to twenty other attorneys general are thinking of introducing similar legislation in their respective states.[33]

If enacted, however, the Connecticut bill and those like it are unlikely to survive legal challenge. First, the CDA's immunity provisions bar liability for all claims based on third party content, including those based on state statutes. The CDA's expansive language grants broad immunity limited only by specific statutory exceptions that exclude four categories of claims from its reach: (1) claims involving a "federal criminal statute," (2) "any law pertaining to intellectual property," (3) "any State law that is consistent with [the] section," and (4) claims under the "Electronic Communications Privacy Act."[34] Furthermore, as noted previously, § 230(e)(3) states that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[35] Courts have applied these provisions broadly to bar claims based on both state and federal statutes. As one court applying the CDA to bar claims based on a federal civil rights statute explained, "Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied. . . ."[36] Accordingly, the Connecticut bill, even if enacted, will be barred by the CDA.

The Connecticut bill would also be vulnerable to a First Amendment challenge much like the one successfully launched by the ACLU against the age verification provisions of the CDA and COPA statutes. As explained above, the Supreme Court has held that requiring adult websites to verify the age of their users violates intermediate scrutiny under the First Amendment because there are more effective and less restrictive means of protecting minors from adult content. Those arguments apply with greater force to social networking websites, which provide a higher value medium for speech than do porn sites.

Aside from the legal challenges facing mandatory age verification, commentators are beginning to question whether

age verification is even a desirable solution to this complicated social problem.[37] Indeed even if online age verification were technologically feasible, it is unlikely to ever be foolproof. Instituting it on a broad scale may give parents and minors a false sense of security, or, worse, the burden of administering the age verification system could force mainstream social networking sites offshore, where meaningful regulation would become virtually impossible.[38]

Conclusion

There is no denying that society has an obligation to protect its children from sexual predators, wherever they operate. The problems related to online sexual predators, however, are complicated. Although it may seem attractive to place the burden to stop these heinous crimes on social networking sites that inadvertently enable them, imposing such a liability scheme would chill Internet speech and could ultimately have the unintended consequence of forcing mainstream websites overseas.

Notwithstanding these realities, however, social networking websites and lawyers who represent them should be prepared to face private lawsuits and legislation seeking to hold them liable for what their users say and do. As outlined in this article, well-established statutory, common law, and constitutional principles should shield websites from such liability and hopefully encourage lawmakers to focus on more productive law enforcement and education based solutions to the problem of online sexual predators.

Endnotes

1. Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007).

2. *See* Doe II v. MySpace, Inc., No. SC092421 (L.A. Super. Ct. filed Jan 17, 2007); Doe III v. MySpace, Inc., No. SC092423 (L.A. Super. Ct. filed Jan 17, 2007); Doe IV v. MySpace, Inc., No. SC092424 (L.A. Super. Ct. filed Jan 17, 2007); Doe V v. MySpace, Inc., No. SC092422 (L.A. Super. Ct. filed Jan 17, 2007).

3. John O'Brien, *Blumenthal Wants More MySpace Regulations*, LEGALNEWSLINE.COM, Mar. 12, 2007, www.legalnewsline.com/news/contentview.asp?c?191808; Jennifer Medina, *States Ponder Laws to Keep Web Predators from Children*, N.Y. TIMES, May 6, 2007, at 29.

4. 42 U.S.C. § 230(b)(1).

5. *See* Dimeo v. Max, 433 F. Supp. 2d 523, 528 (E.D. Pa. 2006) ("The provision 'precludes courts from entertaining claims that would place a computer service provider in a publisher's role,' and therefore bars 'lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content.'") (quoting Green v. Am. Online, Inc., 318 F.3d 465, 471 (3d Cir. 2003); Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997)).

6. 42 U.S.C. § 230(c)(1).

7. 42 U.S.C. § 230(e)(3).

8. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 712–16 (Ct. App. 2002).; Michelangelo Delfino v. Agilent Techs., 145 Cal. App. 4th 790, 804–05 (Ct. App. 2006).

9. *See, e.g.,* Batzel v. Smith, 333 F.3d 1018, 1034 (9th Cir. 2003); Ben Ezra, Weinstein, & Co., Inc. v. AOL, Inc., 206 F.3d 980, 986 (10th Cir. 2000); Blumenthal v. Drudge, 992 F.Supp. 44, 53 (D.D.C. 1998).

10. Zeran v. AOL, Inc., 129 F.3d 327, 334 (4th Cir. 1997).

11. *Id.* at 330, 333.

12. *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006) (noting that "courts have extended the reach of the CDA to immunize ISPs from liability in several settings besides defamation suits").

13. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).

14. *Id.*

15. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007) ("Plaintiffs argue this suit is based on MySpace's negligent failure to take reasonable safety measures to keep young children off of its site and not based on MySpace's editorial acts. The Court, however, finds this artful pleading to be disingenuous.").

16. 42 U.S.C. § 230(e)(3).

17. Walker v. Harris, 924 S.W.2d 375, 377 (Tex. 1996).

18. Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

19. *Id.* at 661.

20. *See* 47 U.S.C. § 223(e)(5)(B).

21. Reno v. ACLU, 521 U.S. 844 (1997).

22. *Id.* at 855–57.

23. ACLU v. Gonzales, No. 98–5591, 2007 WL 861120 (E.D. Pa. Mar. 22, 2007).

24. Ashcroft v. ACLU, 542 U.S. 656 (2004).

25. *Gonzales,* 2007 WL 861120, at *34–40.

26. *See* Lisa Lerer, *Why MySpace Doesn't Card,* FORBES.COM, Jan. 25, 2007, www.forbes.com/security /2007/01/25/myspace-security-identity-tech-security-cx_ll_0124myspaceage.html.

27. *See Gonzales,* 2007 WL 861120, at *36; *Reno,* 521 U.S. at 856–57 & n.23.

28. *See, e.g.,* Jenny Lee, *MySpace Generation Getting to Know Presidential Hopefuls Online,* QUADCITIES ONLINE, Apr. 30, 2007, http://qconline.com/archives/qco/display.php?id ? 336280; Chris DeWolfe, *The MySpace Generation: How a Project of Feed Burritos to the Hungry in L.A. Spread All the Way to Damascus,* FORBES.COM, www.forbes.com/free_forbes/2007/0507/072.html.

29. Cohen v. Cowles Media Co., 501 U.S. 663, 668 (1991).

30. John O'Brien, *Blumenthal Wants More MySpace Regulations,* LEGALNEWSLINE.COM, Mar. 12, 2007, www.legalnewsline.com/news/contentview.asp?c?191808.

31. H.B. 6981, 2007 Leg., Reg. Sess. (Conn. 2007).

32. *Id.*

33. O'Brien, *supra* note 3 (noting that Attorney General Blumenthal "told the Associated Press that 10–20 other attorneys general are thinking of introducing similar legislation in their respective states").

34. 42 U.S.C. § 230(e)(1)–(4).

35. *Id.* § 230(e)(3).

36. Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 539 (E.D. Va. 2003) (quoting TRW, Inc. v. Andrews, 534 U.S. 19, 28 (2001)).

37. *See* Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,* PROGRESS ON POINT 3 (Mar. 2007), www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf.

38. *Id.*

Is the Federal Government Making VoIP Safer?

JONATHAN E. MEER

As Voice over Internet Protocol (VoIP) has increased in popularity and become a mainstream communications technology with more than eight million subscribers,[1] concerns have emerged about its security. VoIP technology has created security concerns in the past but recently such threats have extended beyond VoIP users to all telephone users. Incidents of spoofing (the use of fake caller ID information to defraud), denial of service, spamming over Internet telephony, and phreaking (breaking into the telephone network illegally) are becoming more widespread with VoIP. The federal government has begun to take action.[2] For example, on June 13, 2007, the House of Representatives unanimously passed a bill that would make caller ID spoofing a violation, punishable by $10,000 per each occurrence up to $1 million.[3] But does this latest legislative attempt to secure VoIP make the technology safer for phone calls? This article reviews the security threats that have arisen with VoIP and the federal responses to them.

Theft of Service

One early security issue that emerged from the widespread use of VoIP was phreaking, i.e., the theft of phone calls. Phreaking, a term that originated from the use of various audio frequencies to manipulate a phone system, has become widespread with the growing use of VoIP. The most notorious case of phreaking took place in 2006 and led to the arrest of Edwin Pena, who hacked into the computer networks of unsuspecting VoIP service providers to reroute his customers' calls. Pena sold more than ten million minutes of service at deeply discounted rates, netting more than $1 million from the scheme.[4] Stealth Communications reported that in 2007, thieves steal 200 million minutes a month, worth $26 million, by selling them to smaller telecoms that either sell printed phone cards or operate call centers.[5]

Although phreaking is not limited to VoIP, the latest rash of this crime has been through phone services on the Internet. Phreakers are stealing minutes and reselling them on the black market, but societal demands for faster phone lines has curbed this crime somewhat with the expansion of the traditional telephone network to T1 lines, which are commonly leased to Internet service providers.[6] However, updating the networks still has not stopped the external threat of phreakers using illicit phreaker programs to attack small telecoms, which many times lack the money for a secure gateway server that connect a carrier's telephone network to the Internet.[7]

Today, VoIP companies are placing the onus on consumers to uncover theft of service. Many VoIP providers include in their service contracts a provision that the consumer will be liable for all use of the service and "any and all stolen Service or fraudulent use of the Service" until the VoIP provider is notified.[8] Some companies have turned to private VoIP networks, instead of the public Internet, to protect themselves from phreakers.[9] Companies also use user verification and cryptographic capabilities to protect their VoIP clients.[10] Other growing protections include firewalls, encryption, and other software-based measures similar to those used for data security.[11]

Vishing

Although traditional concerns over VoIP safety come from the theft of service, new security concerns exist for all telephone users because of VoIP. A prevalent security issue with VoIP is voice fishing, also known as "vishing," which is the making of phone calls to solicit potential victims and gain access to their personal information. Fraudulent telephone calls soliciting personal information are not new. However, vishing has become even more of a problem because VoIP phone numbers and ID can be established without the same level of verification required on a traditional phone line.[12] For instance, some incidents of vishing involve criminals using a phone number with a similar area code, even the same prefix, as a local bank and tricking victims into offering their personal information.[13]

Some criminals have gone so far as to fool telephone identification services by taking on a completely different name and number through the use of legitimate software created to protect privacy and using it for illegal activities.[14] The *Washington Post* has collected a number of anecdotal reports about spoofing scams with misleading Caller ID and 1-800 numbers. These include calls threatening a bench warrant for failure to appear for jury duty and scams that warn of a violation of Bank of America's Acceptable Use Policy and then requests the account holder's PIN.[15] In Jefferson City, Missouri, more than 1,000 people received a phone call that appeared to be from a local bank, with the caller ID showing the bank's customer service line. The customers were told that their accounts would be deactivated unless they provided their personal information to the caller.[16] Although some customers did provide personal information, the bank was notified of the scam before the alleged criminals absconded with any funds.[17]

Government Regulation

The federal government has taken control of VoIP regulation. In 2004, the Federal Communications Commission (FCC) ruled that Vonage and its use of VoIP technology are exempt from state and local regulation.[18] On March 21, 2007, the U.S. Court of Appeals for the Eighth Circuit in *Minnesota Public Utility Commission v. FCC* upheld the 2004 FCC ruling, which bars states from regulating Internet-based phone services.[19] The court determined that because VoIP telephone calls can be made from nearly anywhere and are thus an interstate service, no single state can appropriately regulate VoIP services.[20] This ruling reaffirmed the federal government's responsibility to take action to make VoIP technology safe for the general public.

Congress has generally deferred the regulation of VoIP to the FCC although it has passed or considered some legislation that impacts VoIP. For example,

Jonathan E. Meer (lawclerk.lombardi@judiciary.state.nj.us) is the law clerk to the Honorable Sebastian P. Lombardi of the New Jersey Superior Court.

in 2004, both the House and the Senate considered bills that would disallow states to regulate VoIP or limit the FCC's authority to regulate VoIP, but neither bill was adopted.[21] In 2004, the FCC blocked the Minnesota Public Utilities Commission from applying its traditional telephone company regulations to Vonage service. This exempted the VoIP service provider from complying with the state's laws and regulations governing a "telephone company," such as those dealing with authority, tariffs, and 911 emergency services.[22]

The Telecommunications Act of 1996 mandated that VoIP be defined as either a telecommunications service similar to an incumbent or competitive telephone company, or as an information service exempt from state regulations.[23] The 2004 FCC order clarifies that VoIP providers are to be considered providers of information services, not telecommunications carriers as defined by the Telecommunications Act.[24] Still, Congress has proposed bills that do have the indirect effect of addressing VoIP service. H.R. 251, which would impose fines for spoofing, is currently before the Senate.

The FCC has taken steps to regulate VoIP, but many issues regarding privacy and security still remain. One early regulation of VoIP concerned 911 capabilities.[25] The FCC imposed Enhanced 911 (E911) obligations on providers of interconnected VoIP services, requiring the network to automatically provide a 911 caller's originating number and, in most cases, location information to emergency service personnel.[26]

In addition, VoIP providers must contribute to the Universal Service Fund that supports communications services programs such as E-Rate, which provides Internet access to public schools and libraries.[27] Further, the FCC requires VoIP providers to comply with the Communications Assistance for Law Enforcement Act (CALEA) of 1994. CALEA allows enforcement agencies to conduct electronic surveillance as similarly required for all traditional telephone providers.[28] This FCC requirement was reaffirmed in 2006, clarifying that May 14, 2007, was the CALEA compliance deadline for facilities-based broadband Internet access and interconnected VoIP services.[29] However, neither of these steps addressed regulations securing VoIP.

Future Regulation

With VoIP still largely unregulated, the next issue that the federal government will likely address in increasing the medium's security is Customer Proprietary Network Information (CPNI). CPNI is data specific to individual customers generated when customers make calls, including call detail records, call volumes, customer account information, billing information, technical information, service destination, and the service plans to which a customer subscribes.[30] Some industry insiders believe that with a little detective work, CPNI data can reveal customers' Internet service provider.[31]

The Telephone Records and Privacy Protection Act, which Congress passed last year, amended the federal criminal code to prohibit obtaining, or attempting to obtain, confidential phone record information from a telecommunications carrier for all phone customers, including VoIP subscribers.[32] In 2006, the Prevention of Fraudulent Access to Phone Records Act was proposed in Congress and was resubmitted in 2007.[33] This is one of the bills proposed to create new consumer data protection laws by placing stricter requirements on the collection of personal information. Privacy advocates and companies are at odds on the proposed national guidelines and their effect on states' regulation of privacy, but a bill such as the Prevention of Fradulent Access to Phone Records Act could provide a baseline of expected consumer protection.[34] Although the proposed act does not directly address VoIP, it seeks to address CPNI protection measures used by telecommunications carriers.[35] The act would permit a telecommunications provider to use aggregated data for its own usage, such as to improve service and solicit new business, but would require customer information to remain private.[36] The proposed measures include: (1) requiring telecommunications carriers to institute customer-specific identifiers to access CPNI; (2) encryption of CPNI or other safeguards to secure the data; and (3) deletion of CPNI after a reasonable period of time if storage is no longer necessary.[37] Representative John Dingell, chairman of the House Committee on Energy and Commerce, is optimistic that the Act will be brought to the House floor in 2007, and a similar bill is proposed in the Senate.[38] In summary, these proposed measures would require greater verification to access a person's proprietary information.

Conclusion

The recent proposals by Congress to regulate use of CPNI, impose the Records Privacy Act, and criminalize spoofing reflect the government's concern about the security issues present in VoIP usage. As our information society becomes more interconnected, these security issues must be addressed. As more people use VoIP for their telephone calls, the need for regulations and legislation protecting against the dissemination of private information and preventing fraud continues to increase.

Endnotes

1. Matt Richtell, *Skype's New Unlimited Calling Plan*, N.Y. TIMES, Dec. 13, 2006.
2. Nadeem Unuth, *Security Threats in VoIP*, at http://voip.about.com/od/security/a/SecuThreats.htm.
3. *Bill Targets ID Theft,* WAXAHACHIE (TX) DAILY LIGHT, June 13, 2007.
4. Preston Gralla, *The Inside Story of A Million-Dollar VoIP Scam*, Networking Computing, June 8, 2006, *at* www.networkcomputing.com/channels/networkinfrastructure/188702745; Sharon Gaudin, *Accused VoIP Fraudster Sought as Fugitive*, INFO. WK., Sept. 15, 2006.
5. Benjamin Sutherland, *Stealing the Minutes*, Newswk., Mar. 19, 2007.
6. *History of Phreaking*, at http://passivemode.net/phreaking; s*ee also Telecommunications Tutorial Guides*, *at* www.infosyssec.org/infosyssec/security/teletut1.htm.
7. Sutherland, *supra* note 5.
8. Axis VOIP Terms of Service, *at* www.axint.net/tos; Speakeasy VoIP Service Subscriber Agreement Highlights, *at* www.speakeasy.net/tos/voip.php.
9. *Id.*
10. Kevin Murphy, *Is VoIP a Security Risk?*, COMPUTER BUS. REV. ONLINE, Mar. 30, 2006.
11. Paul D. Kretkowski, *How Secure Are Your VoIP Calls?*, VOIP NEWS, Jan. 2, 2007.
12. *Just when you thought it was safe: Vishing makes a splash on the Web*, Emory Federal Credit Union Identity Theft Resolution Serv., *at* www.emoryfcu-identitytheft911.com/articles/article.ext?sp=707.
13. *Id.*
14. Mike Musgrove, *New Tricks Fool Caller ID*, WASH. POST, Oct. 30, 2004, at E01.
15. Brian Krebs, *'Vishing': Dialing for Dollars*, WASH. POST, June 26, 2006, *at*

http://blog.washingtonpost.com/securityfix/2006/06/vishing_dialing_for_dollars.html; Brian Krebs, *'Vishing': Dialing for Dollars*, WASH. POST, Mar. 8, 2007, http://blog.washingtonpost.com/securityfix/2007/03/vishing_dialing_for_dollars_pa_1.html.

16. Michelle Brooks, *Warning! Scam to Steal Personal Information Shows Bank on Caller ID*, JEFFERSON CITY NEWS TRIB., Mar. 1, 2007.

17. *Id.*

18. Carson Carlson and Ryan Naraine, *FCC: VOIP Is Not Subject to State Rules*, EWK., Nov. 9, 2004, *at* www.eweek.com/article2/0,1895,1748815,00.asp; Vonage Holdings Corp. v. Minn. Pub. Utils. Comm'n, 394 F.3d 568, 569 (8th Cir. 2004).

19. Minn. Pub. Utils. Comm'n v. FCC, 2007 U.S. App. LEXIS 6448 (8th Cir. 2007).

20. Patrick Condon, *Court Backs FCC over States in VoIP Case*, HOUS. CHRON., Mar. 21, 2007.

21. Roy Mark, *Congress Hangs Up on VoIP for 2004*, Internet News, Sept. 3, 2004, *at* www.internetnews.com/bus-news/article.php/3403911.

22. 19 FCC Rcd 22404 (FCC 2004).

23. *Id.*

24. *Id.*

25. Fed. Communications Comm'n, E911 Requirements for IP-Enabled Service Providers, May 19, 2005, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-116A1.pdf.

26. FCC Consumer Advisory: VoIP and 911 Service, *at* http://ftp.fcc.gov/cgb/consumerfacts/voip911.html.

27. Anne Broache, *FCC Approves New Internet Phone Taxes*, CNET NEWS, June 21, 2006, http://news.com.com/FCC+approves+new+Internet+phone+taxes/2100-7352_3-6086437.html.

28. Communications Assistance for Law Enforcement Act and Broadband Access and Services, FCC, Aug. 5, 2005, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf.

29. Press Release, Federal Communications Comm'n, FCC Adopts Order to Enable Law Enforcement to Access Certain Broadband and VoIP Providers, May 3, 2006, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-265221A1.pdf.

30. K.C. Halm, *Expanded Privacy Obligations for Telecom Carriers and VoIP Providers Under Consideration at the FCC*, *at* http://www.privsecblog.com/archives/federal-regulation-expanded-privacy-obligations-for-telecom-carriers-and-voip-providers-under-consideration-at-the-fcc.html.

31. *CPNI–The Gold Mine under LECs*, MEASURE X, May 12, 2006, *at* http://www.measure-x.com/newsletter/42.html.

32. Telephone Records and Privacy Protection Act, 18 U.S.C § 1039 (2006).

33. Prevention of Fraudulent Access to Phone Records Act, H.R. 4943, 109th Cong., 2d Sess. (2006); Prevention of Fraudulent Access to Phone Records Act, H.R. 936, 110th Cong., 1st Sess. (2007).

34. Matt Hines, *Debate Lingers over Federal Data-Handling Laws,* INFOWORLD DAILY NEWS, Apr. 3, 2007, *at* http://www.infoworld.com/article/07/04/03/HNfeddatasec_1.html.

35. *Hearings on Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act*, 110th Cong., 1st Sess. (Mar. 7, 2007) (statement of Marc Rotenberg, President, EPIC).

36. Prevention of Fraudulent Access to Phone Records Act, H.R. 936, § 203(h)(1)(B).

37. *Id.* § 201.

38. *Dingell Releases SEC Response on Hewlett-Packard Probe; Pledges Action on Pretexting Legislation*, STATES NEWS SERV., Apr. 13, 2007. Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. 1st Sess.

A Tale of Seditious Libel in the Twenty-First Century

CHARLES L. BABCOCK AND AMANDA L. BUSH

What follows is a work of fiction, but, hey, it could happen.

A Reporter's Notebook: How I Got into This Mess

BY TOM GILBERT,
INQUIRER STAFF WRITER

It was a dark and stormy night.

I've always wanted to use that as a lead, but until now, I've never had the chance. But it truly was a dark and stormy night when this whole mess began.

Most of you don't know me. I've been a journalist for twenty years, longer if you count journalism school at the University of Florida. I'm forty-two years old. Divorced. No kids. Smoker (but only after I jog). I drink (but moderately for a reporter). No girlfriends at the moment and no news sources that might turn into girlfriends. Does anybody really believe the Pelican Brief could happen to a reporter? At least not the Julia Roberts part.

I've been working at the *Washington Inquirer* for twelve years, most recently covering the Justice Department. I'm no Bob Woodward, but I've got pretty decent sources and have had some success (we posted the NSA story on our website five minutes before the *Post* and the *Times*). My dad got me this job. He knew somebody who knew somebody, and I got an interview and it stuck. You should know that my dad is a loser—the only thing he ever did for me was get me this job, which, by the way, is probably going to land me in jail. Anyway. . .

It was a dark and stormy night, and I was about to go home when a source calls me. Sorry, I can't reveal his identity, even though, as you have no doubt read, I was ordered to by a U.S. district judge. He (the source) sounds very distressed and asks if we can meet right away. I suggest Old Ebbitt Grill. He says, "No way. Too public." And then he tells me to meet him at the Little Fountain Café, which I learn is "a quiet, dimly lit, intimate dining room hiding in plain view" below the "frantic nightlife scene on Adams Morgan's main drag." Don't you love the Internet?

I ask him, "What's this about?"

"I don't want to talk on the phone, but you'll be interested."

"Can you give me a hint?"

"Not on the phone."

He hangs up. So I head for the subway and take the Red Line to the Woodley Park-Zoo exit and walk across the bridge into Adams Morgan. Did I mention it was raining? I arrive. Soaked. My source is at a table in the way back, and dimly lit does not begin to describe how dark it is in this place. I find him, and he's been drinking. Great.

"So, Rudy (not his real name), how are you doing?"

He looks up at me, and his eyes are bloodshot. Drinking a lot, I'm thinking. His hand shakes, just a little, as he offers it to me without standing. I figure you can tell a lot about people by how they shake hands. If I had kids, I would make them practice handshaking until they got it right. Firm. Confident. Look the other guy straight in the eye. This guy isn't any of that. Feeble. Soft. Averted eyes. I'm thinking that this guy is certainly in a position to know a lot. He's in a sensitive government position. I've been cultivating him for about three years. Not too hard, but I haven't been ignoring him either. He's provided me some stuff I've used in the past—stuff that checked out and was reliable. I suspect he was the source for some of the best stuff in Woodward's last book, but I would, of course, never ask.

"So, Rudy, what's up?"

"Why are you here?"

"Because you invited me just about twenty minutes ago, as I recall."

Charles L. Babcock (cbabcock@jw.com) is a partner and Amanda L. Bush (abush@jw.com) is an associate with Jackson Walker L.L.P. Mr. Babcock has represented the media for over twenty-five years and is a former journalist.

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DEFENDANTS' BRIEF

UNITED STATES OF AMERICA,
Plaintiff

v.

TOM GILBERT

and

WASHINGTON INQUIRER CO., INC.,
Defendants

I. INTRODUCTION

The indictment in this case should be dismissed for two primary reasons: first, the Espionage Act does not prohibit the conduct complained of by the government, and second, even if it did, the Espionage Act would be unconstitutional under the First Amendment as applied here because this prosecution is, in effect, an effort by the government to punish speech highly critical of it, also known as "seditious libel." And it is generally accepted that prosecutions of seditious libel violate the First Amendment.

Prosecutions under the Espionage Act against the media are unprecedented. Indeed, in the recent prosecution of two former lobbyists of the American Israel Public Affairs Committee (AIPAC) for conspiring to violate the Espionage Act, the government conceded:

> [W]e recognize that a prosecution under the espionage laws of an actual member of the press for publishing classified information leaked to it by a government source would raise legitimate and serious issues and would not be undertaken lightly, indeed, the fact that there has never been such a prosecution speaks for itself.[1]

In that case, pending in this court, two former lobbyists of the AIPAC were indicted for conspiring to violate the Espionage Act.[2] The indictment alleged that the defendants conspired with a Pentagon official to communicate information about national defense to people not authorized to receive it, including a reporter for the *Washington Post*.[3]

This is a case of first impression and has been brought, we believe, because the government is embarrassed about the disclosure of its illegal wiretapping program, not because of a concern for national security. It is, in essence, a prosecution for seditious libel and therefore unconstitutional under the First Amendment.

II. HISTORICAL UNDERPINNINGS OF THE SEDITION AND ESPIONAGE ACTS

The historical context surrounding the Sedition Act and Espionage Act and the Supreme Court's and Fourth Circuit's treatment of prosecutions thereunder provide the cornerstone for establishing that Tom Gilbert's and the *Inquirer*'s actions are protected by the First Amendment and may not be prosecuted.

A. *Early Origins of Seditious Libel*

Seditious libel, as we now understand it, first appeared in the Elizabethan era as the "notion of inciting by words or writings disaffection toward the state or constituted authority."[4] In 1606, the Star Chamber, the administrative tribunal established by the Tudors in the 1500s, deemed seditious libel "a crime because it tended to undermine respect for public authority."[5] The "Star Chamber was dissolved in 1641, but seditious libel, like blasphemy, [continued] as a common law offense." Over 100 years later, the existence of this offense would influence the development and interpretation of law in America.[6]

Seven years after the Bill of Rights was signed into law, the U.S. Congress passed the Sedition Act of 1798, essentially criminalizing the publication of "unfounded" criticism toward the U.S.

(Continued on page 15)

He sighs, "Yes."

So I figure we're going to play this Washington game where he pretends that he has information that will change the course of human history but doesn't want to reveal it because it would violate his code of honor or some such crap, and I'm supposed to pull it out of him any way I can. I wait and just look at him. A waitress comes. I order a Rusty Nail. "With Chivas please." My drink comes. We still haven't said anything. I haven't inquired about his kids because I don't know if he has kids. He hasn't asked about mine, which is fine, because I don't have any (that I know about).

We order dinner. It comes. We eat. Still nothing, and I'm wondering if I haven't just blown an entire evening over some nutty bureaucrat with a conscience that is not quite guilty enough. At least I'm on an expense account, although not on overtime. We're a Guild paper, and you have to have it approved ahead of time, which I have neglected to do (quite often).

"I've got some documents," he finally says.

"What sort of documents?"

"Documents that are very secret. Highly classified. Espionage Act secret."

"What does that mean, Espionage Act secret?"

"It means so secret that if they knew I had taken them out of the building, I would lose my job and probably be prosecuted."

There's nobody near us, but I look around anyway. "So why did you remove these highly classified Espionage Act secret documents that could get you fired and prosecuted?"

"To give them to you."

"And why would you do that?" (Sometimes you have to play hard to get.)

"Our government is, shall we say, doing something that is very wrong."

"So why don't you report it?"

He looks at me with that pitying look that says, "You just don't understand life inside the Beltway, do you?" Which is, of course, b.s. I understand it plenty well; I just haven't figured out this guy's angle. Inside the Beltway, everybody has an angle.

"Okay," I say. "Will you let me have the documents? Did you bring them with you?"

"If I give them to you, it might cause you some problems."

"What sort of problems?"

"I assume if you think these are genuine, and they are, that you will write something. If you write something, they will know that you have classified documents, and they will want to know where you got them. . . ."

"You know that's not a problem."

"And they may want to prosecute you and your paper for publishing this information."

"Why don't you let me worry about all that."

A thin smile from Rudy. He orders another drink. Me, too. If we're going to bring down the government, we might as well have that warm feeling in our tummies.

Well, to cut a long story a little short, he gives me the documents (about 100 or so). They're in an envelope. He passes the envelope to me under the table.

We finish dinner and say goodbye. He wants to leave first. "Wait ten min-

utes and then you can leave," he says. So I have another drink, although I switch to scotch and water. More than two Rusty Nails, and my judgment about women becomes impaired . . . although, to be honest, it's not real good when I'm sober.

I take the train to my one-bedroom apartment in North Bethesda, but I don't open the envelope until I get home. I start reading. Pure dynamite. Oh, my God! If these documents are legitimate, the government is doing some bad stuff: illegal wiretaps on opposing political leaders, including presidential candidates; wiretaps of the Senate majority leader ("because we don't think he's a Patriot," according to an e-mail); surveillance of government critics, including Ralph Nader. There's a memo about "How to Take over the Government in Times of National Emergency," authored by a former secretary of defense.

The real issue was not national security but the public's right to express discontent with government policy.

There are e-mails, memos, position papers, authorizations to the FBI. It goes all the way to the top of the Justice Department and pretty high up in the White House, although the president himself doesn't get tagged with any paper.

I call my editor, James T. Olson. We call him Jimmy—to his face, not just behind his back. He's okay with that, thinks it's funny. He never calls me Superman.

"Jimmy, it's Tom and, uh, I may have the beginnings of a pretty big story that is perhaps best not discussed over the phone," I say.

"So then why did you call me at 11:30 at night?"

"Uh, just to alert you and maybe set up a meeting tomorrow. I'm a little paranoid about this thing, and maybe we should meet in a park or something."

"Tom, it's the middle of winter and raining like hell outside. Why not at the office tomorrow?"

"Tomorrow is fine, but not the office. I'll explain, okay?"

Jimmy is used to me. He's indulged me before, so he says fine, and we arrange to meet at a Howard Johnson's (I didn't think there were any of these left) the next morning before work. I forget to ask for overtime authorization. Shit.

I find out later, and this is unbelievable, that the FBI listened to this conversation between me and Jimmy. Amazing.

Anyway, not to bore you with the details, but, as you've probably heard, we check out the documents, and they are legit. Way legit. We run a series of stories accusing the government of secret wiretapping, and all hell breaks loose, as you would imagine. The administration tries to get a prior restraint. No dice (see *United States v. New York Times*). All the cable guys want me to go on their shows, and I am thinking that this is a great thing for my, so far, modest career. But Jimmy and the other editors think this will be a bad thing because there are rumors we are under investigation. Can you imagine that? We expose this major violation of the law, and we're under investigation?

At first I thought it was just a competitive thing—you know, my paper wants the story for itself—but it didn't take long to see they were right. The Department of Justice announces that a special prosecutor has been appointed to look into "the matter," and it turns out that "the matter" is me and Rudy.

Well, for starters, I'm never going to give up a source unless he tells me face-to-face that it's okay, and my read on Rudy is that he is trying to dive as deep as he possibly can on this, although there is a report that the Justice Department is giving people polygraphs to see if they talked to me. Anyway, the really bad thing is that the SP (Special Prosecutor) indicts me for publishing state secrets, saying that I stole the documents. The SP claims that because I won't reveal my source, I must not have a source, which means I didn't get the documents from anyone but somehow broke in and stole them.

Ridiculous. As my friend Max Frankel (okay, I met him once) wrote, "practically everything that our government does, plans, thinks, hears and contemplates in the realm of foreign policy is stamped and treated as secret—and then unraveled by that same government, by the Congress and by the press in one continuing round of professional and social contacts and cooperative exchanges of information."

Unquestionably true, but it hasn't, as you know, stopped the SP. The *Inquirer* and I were indicted in the U.S. District Court for the Eastern District of Virginia, the same place where they try terrorists. We were charged with violations of the Espionage Act. There were 100 counts, one for each document I allegedly "stole and used for our series: *Secret Government Wiretapping Program Exposed: Every Step You Take, Someone's Watching You*.

The paper hired a separate lawyer for me, a wonderful guy from Denver who specializes in this sort of thing, although he candidly told me up front that there was no precedent for this case. Great. So what was our argument? As he outlined it to me, it made sense. I may get some of the legalese wrong, but here goes: We fought every step of the way distinguishing our case from criminal prosecutions under the Espionage Act and using an argument called "First Amendment Due Process"[1] to rebut what we considered a prosecution of seditious libel. At some point, we moved to dismiss the indictment. Our brief is in the sidebar.

Well, it didn't work. The jury found us guilty. The judge gave our argument careful consideration, but, in the end, I think it was just too novel for her. So we'll see what the Fourth Circuit and the Supreme Court say about this whole shenanigan affair. We did get one break. I was only sentenced to 100 hours of community service and fined $1,000. The newspaper was fined $5,000. The judge said from the bench that she didn't care what the sentencing guidelines said, that we had done a public service even if we technically had violated the law. So that was nice.

It also has been great to see the support from fellow journalists. Just about every news organization has filed amicus briefs in our favor except the one jerk at a big New York paper who said this case would make bad precedent and shouldn't be appealed. Let him see how it feels when he has a prosecutor cross-examining his happy ass. Sorry. I'm really not bitter about this whole thing. The Pulitzer prize keeps me warm at night.

It's been a long time since the sun was out, but I can see some rays shining through the clouds. I think we're going

to win this appeal, but it will take several years and the Supreme Court is going to have to do it. My lawyer is optimistic, too. He told me that the legal theory he used was developed with a couple of lawyer friends at their cottage in Canada over some scotch. His friend's favorite drink is a Rusty Nail, too. How perfect is that? Like just about all of the leaking that goes on in Washington, as Max says, "that's how it's done, barroom style: an official playing bureaucratic tennis . . . a reporter preying on the knowingness of his source."

Well here's to the First Amendment. And Rusty Nails. . . .[2]

Endnotes

1. *See* Charles L. Babcock, *Allegedly Criminal Newsgathering and First Amendment Due Process*, 2 LDRC BULL. 63 (2002).

2. The quotations from Max Frankel first appeared in his article entitled "The Washington Back Channel" in the *New York Times* (March 25, 2007).

Defendants' Brief

(Continued from page 13)

government.[7] Interestingly, "both true and false criticism of the government was considered libel."[8] In fact, "legal thought of the pre-revolutionary era proclaimed that 'the greater the truth, the greater the libel.'"[9] The Sedition Act did not last long, expiring in 1801 after the election of Thomas Jefferson to the presidency.[10] "Though the Sedition Act was not an enduring piece of legislation, the very existence of the Act stands as a reminder of the power of dissenting voices in the press and the urge of those in power to control them."[11]

Although the constitutionality of the Sedition Act itself was never tested in court, the Supreme Court subsequently recognized that First Amendment protections extend to "seditious libel."[12] In *New York Times v. Sullivan*, the Supreme Court surveyed the previous controversy surrounding the enactment and enforcement of the Sedition Act and concluded that the debate

> first crystallized a national awareness of the central meaning of the First Amendment. . . . Although the Sedition Act was never tested in this Court, the attack upon its validity has carried the day in the court of history. . . . [That history] reflect[s] a broad consensus that the Act, because of the restraint it imposed upon criticism of government and public officials, was inconsistent with the First Amendment.[13]

The Court went on to quote James Madison in saying that in a republican government, "the censorial power is in the people over the Government, and not in the Government over the people."[14] It then concluded that "[t]he right of free public discussion of the stewardship of public officials was thus, in Madison's view, a fundamental principle of the American form of government."[15]

B. *The Espionage Act of 1917—Seditious Libel Part II*

Seditious libel next emerged in the form of the Espionage Act of 1917 just prior to the United States' entry into World War I.[16] As the likelihood of American participation in the war increased, the Department of Justice became concerned that the nation's existing laws would be inadequate to "regulate the conduct of the individual during war time."[17] Congress debated the Espionage Act bill at length, and much of the debate concerned the history and meaning of the First Amendment.[18] For instance, a provision of the bill that would have allowed the president to censor the press dominated congressional discussion but was eventually eliminated in conference. The Espionage Act passed without it, making it a crime to convey information relating to the national defense with the intent to harm the U.S. government or to promote the success of its enemies.[19]

The first challenge to the Espionage Act came in 1919 in *Schenck v. United States*.[20] In that case, the defendants, including a prominent socialist leader, were indicted and convicted for urging resistance to the draft.[21] A unanimous Supreme Court upheld the conviction, and Justice Oliver Wendell Holmes, in writing the opinion, did not steer very far from the older, British notion that free speech and press meant little more than limiting prior restraints.[22] His test for constitutionality would last more than fifty years: "The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent."[23]

Eight months after *Schenck*, the Supreme Court confronted *Abrams v. United States*,[24] a case that involved a prosecution under the Espionage Act of 1918. In that case, five Russian immigrants were convicted for publishing and distributing pamphlets that criticized the Wilson administration and protested U.S. policy against the emerging Bolshevik regime.[25] Seven members of the Supreme Court applied Justice Holmes's "clear and present danger" test to sustain the convictions, holding that the prohibited words created a clear and present danger of obstructing the war effort.[26] Justice Holmes, joined by Justice Brandeis, dissented, recognizing that the real issue was not one of national security but the public's right to express discontent with government policy.[27]

Justice Holmes's dissent in *Abrams* is widely considered the starting point for this country's move away from the British notion of seditious libel and toward a modern, American view that free and uninhibited speech, no matter how critical of the government, should be the rule.[28] Justice Holmes observed thus:

> [T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market. . . . I think that we should be vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country. I wholly disagree with the argument of the Government that the First Amendment left the common law as to seditious libel in force. History seems to me against that notion.[29]

In the shadow of World War I, *Schenck* and *Adams* defined the boundaries of prosecutions under the Espionage Act. Faced with cases stemming from the "Red Scare," courts stretched the bound-

aries of permissible prosecutions using an approach that has since been revisited.

C. *The Espionage Act Today*

After the Great War ended, the Court did not revisit Espionage Act prosecutions until the country was faced with another global challenge: World War II. By then, the language defining the scope of a violation read, for the most part, as it does today. "Over the years, numerous commentators have criticized [the Espionage Act] as" vague, overbroad, "excessively complex, confusing, and . . . impenetrable."[30] "Yet, despite repeated calls for reform" of the statutes, they have remained unchanged since 1950 and have "weathered several constitutional challenges on both vagueness and First Amendment grounds."[31] Nevertheless, the facts underlying these challenges and their outcomes are in stark contrast to our case involving a reporter and a newspaper and therefore highlight the reasons that a prosecution under the Espionage Act in this instance would violate the First Amendment.

1. "Constitutional Vagueness" Challenges and the Development of a Scienter Requirement

On its face, the Espionage Act, 18 U.S.C. § 793, purports to prohibit the gathering, retention, or communication of information "relating to the national defense."[32] Specifically, section 793(a) prohibits the gathering of information from places[33] connected to national defense if done "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. . . ."[34] Section 793(b) prohibits the copying, taking, making, or obtaining of any "sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense" or any attempt to do so "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. . . ."[35]

Section 793(d) prohibits anyone lawfully having possession of a "document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note relating to the national defense" from "willfully" communicating or transmitting it to anyone not entitled to receive it.[36] Similarly, section 793(e) prohibits anyone having unauthorized possession of a "document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note relating to the national defense" from "willfully" communicating or transmitting it to anyone not entitled to receive it or retaining it and failing to deliver it to an officer or employee of the United States entitled to receive it.[37]

In 1941, the Supreme Court first considered a constitutional vagueness challenge to the phrase *information relating to the national defense* as used in sections 793(a) and (b) of the Espionage Act.[38] In *Gorin v. United States*, one defendant, a citizen of the Soviet Union, had obtained for substantial pay from his co-defendant, a U.S. naval intelligence officer, the contents of over fifty reports and photographs relating to Japanese activities in the United States, which the two defendants conspired to transmit to the Soviet Union.[39] The Supreme Court rejected the defendants' argument that the phrase *information relating to the national defense* in sections 793(a) and (b) was limited to the places listed in section 793(a), holding instead that the term *national defense* was "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[40] The Court explained that "[w]hether a document or report is covered by sections [later codified as 793(a) and (b)] depends on their relation to the national defense, as so defined, not upon their connection with places specified in section [793(a)]."[41] Importantly, the Court in *Gorin* also read into the statute a scienter requirement.[42] As the Court explained,

> [t]he obvious delimiting words in the statute are those requiring "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation." This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established.[43]

Decades later, the Fourth Circuit in *United States v. Truong Dinh Hung*[44] went further, holding that the phrase *related to the national defense* encompasses more than military matters and includes, for instance, the U.S. diplomatic cables and other classified papers relating to the 1977 Paris peace negotiations with the North Vietnamese, American POWs in Indochina, and the names of U.S. sources for intelligence about the Vietnamese government.[45]

Although the court acknowledged the scienter requirement of section 793(a), calling it "critically important because the Supreme Court relied upon it . . . to rebut a claim that the espionage statutes were unconstitutionally overbroad," the Fourth Circuit did not extend the same logic to section 793(e).[46] In upholding the defendants' convictions under section 793(e), the court said that the section does not contain the same strong scienter language of section 793(a) but rather only "requires that the accused 'willfully' transmit the information."[47] As for any ambiguity relating to the term *unauthorized possession* of national defense information, the court said it was cured in this case because the trial court adequately instructed the jury that "a person would have authorized possession if he had an appropriate security clearance and if he gained access to the document because it was necessary to the performance of his official duties."[48]

In 1988, the Fourth Circuit in *United States v. Morison* further limited the possibility of a constitutional vagueness challenge to the Espionage Act.[49] It also for the first time faced the potential conflict between the Espionage Act and the First Amendment.[50] In *Morison*, the defendant, a part-time civilian analyst at the Naval Intelligence Support Center and part-time editor of a publication, stole three classified photos of a Soviet nuclear-powered aircraft carrier after construction and provided them to his publication, *Jane's Defence Weekly*, and the *Washington Post*.[51] The court of appeals rejected the defendant's argument that because he did not transmit the information to a foreign government but instead leaked it to the press, his actions did not fall under the Espionage Act.[52] The Fourth Circuit held that the phrase *those not entitled to receive it* was not limited to "spies or to 'an agent of a foreign government,' either as to the trans-

mitter or the transmittee of the information."[53] The two statutes "declare no exemption in favor of one who leaks to the press. It covers 'anyone.' It is difficult to conceive of any language more definite and clear."[54] The court observed that "courts have recognized the legitimacy of looking to the classification system for fleshing out" this phrase.[55] Given the defendant's naval intelligence training, the court indicated that he was certainly familiar with the government's classification system and had, in fact, agreed in writing to abide by it.[56]

The Fourth Circuit court also held that the phrase *related to the national defense* included "all matters that directly or may reasonably be connected with the defense of the United States against any of its enemies . . . [including] the military and naval establishments and the related activities of national preparedness."[57] Acknowledging the Supreme Court's analysis in *Gorin* that the phrase requires the information to be closely held by the government, the court in *Morison* affirmed the district court's jury instruction that "the government must prove that the documents or the photographs are closely held in that they have not been made public and are not available to the general public."[58] The court further acknowledged that sections 793(d) and (e) prescribe that prohibited activity be "willful," which the court defined as an act "done voluntarily and intentionally and with the specific intent to do something that the law forbids. That is to say, with a bad purpose either to disobey or to disregard the law."[59]

Finally, with respect to the defendant's First Amendment defenses to the government's prosecution of him under the Espionage Act, each of the three judges wrote separately. Judge Russell, who wrote the majority opinion, concluded that there were no "First Amendment rights to be implicated here" because the legislative history was "silent on any Congressional intent in enacting sections 793(d) and (e) to exempt from its application the transmittal of secret military information by a defendant to the press or a representative of the press."[60]

Judge Russell relied on *Branzburg v. Hayes*, quoting the following passage from Justice White's opinion:

> It would be frivolous to assert . . . that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.[61]

A government employee, Judge Russell said, was not entitled to invoke the First Amendment to immunize his conduct merely because he leaked the information to the press.[62]

Judge Wilkinson, with whom Judge Phillips concurred, disagreed, stating, "Morison as a source would raise newsgathering rights on behalf of press organizations that are not being, and probably could not be, prosecuted under the espionage statute."[63]

More recently, in *United States v. Squillacote*, the Fourth Circuit made it clear that information that is closely held by the government, even if it has been "leaked," will continue to be information "relating to the national defense," as that phrase is used in the Espionage Act. [64] The court explained thus: "[A] document containing official government information relating to the national defense will not be considered available to the public (and therefore no longer national defense information) until the official information in that document is lawfully available."[65] Thus, "mere leaks of classified information are insufficient to prevent prosecution for the transmission of a classified document that is the official source of the leaked information."[66] Which brings us to today. . .

2. The AIPAC Case: Seditious Libel in the Twenty-first Century?

Last year, Steven Rosen and Keith Weissman, two former AIPAC lobbyists who were indicted on charges of conspiring to violate the Espionage Act statutes, moved to dismiss the charges against them, arguing that sections 793(d) and (e), as applied to them, are unconstitutionally vague and violate their First Amendment rights of free speech and to petition the government.[67] On August 9, 2006, Judge T. S. Ellis III denied the motion, holding that the Espionage Act was constitutional as applied to them, particularly in light of its scienter requirements.

Judge Ellis first rejected the defendants' argument that the phrase *information relating to the national defense* was insufficiently clear as applied to them because the information was transmitted orally.[68] The phrase, he said, has "consistently been construed broadly to include information dealing with military matters and more generally with matters relating to U.S. foreign policy and intelligence capabilities."[69] Rather than limiting information to tangible information, the court recognized that the scope of the phrase *information relating to the national defense* is limited only in two ways: (1) the information must be closely held by the government, and (2) the disclosure must be potentially damaging to the United States or useful to an enemy of the United States.[70] With respect to the defendants' argument that the phrase *entitled to receive* is vague, the court cited *Morison* in noting that the government's uniform classification system for national security information clearly restricts access of classified information to those with a corresponding security clearance.[71]

The court also rejected the defendants' contention that it was difficult to know whether the information they received was classified because they received it orally.[72] Although acknowledging the potential merit of such an argument from a factual standpoint, the court ultimately found it unpersuasive as a reason for declaring the statute unconstitutionally vague.[73] Instead, the court relied on the statute's scienter requirements, explaining that the government must prove the defendants willfully committed the prohibited conduct, which "eliminates any genuine risk of holding a person criminally responsible for conduct which he could not reasonably understand to be proscribed."[74] According to the court, "the government must prove beyond a reasonable doubt that the defendants knew the information . . . was closely held by the United States," "that disclosure of [the] information [would] potentially harm the United States," "that the persons to whom the defendants communicated the information were not entitled under the classification regulations to receive [it]," and "that the defendants communicated the information . . . with 'a bad purpose either to disobey or to disregard law.'"[75] It follows, the court said, that

> if the defendants, or either of them, were truly unaware that the informa-

> tion they are alleged to have received and disclosed was classified, or if they were truly ignorant of the classification scheme governing who is entitled to receive the information, they cannot be held to have violated the statute.[76]

Finally, with respect to the defendants' First Amendment challenge, the court acknowledged the "inherent tension between the government transparency so essential to a democratic society and the government's equally compelling need to protect from disclosure information that which could be used by those who wish this nation harm."[77] The court rejected the government's "proposed categorical rule that the espionage statutes cannot implicate the First Amendment" and said that *Morison* could not be taken to stand for that proposition.[78] Recognizing that authority on the issue is sparse, the court nevertheless opined that "the government can punish those outside of the government for the unauthorized receipt and deliberate retransmission of information relating to the national defense."[79]

III. CRIMINAL PROSECUTIONS OF THE PRESS UNDER THE ESPIONAGE ACT

Throughout the history of the United States, a member of the news media has never been criminally prosecuted under the Espionage Act for gathering, publishing, or retaining classified information, although numerous opportunities have presented themselves.

A. Chicago Tribune *Article: "Navy Had Word of Jap Plan to Strike at Sea"*

The first instance in which a prosecution of the press under the Espionage Act was considered involved a *Chicago Tribune* article entitled "Navy Had Word of Jap Plan to Strike at Sea," published on June 7, 1942, immediately following the American victory in the Battle of Midway in World War II.[80] The article was written by a correspondent who had seen intelligence reports left in an officer's cabin that disclosed that the strength and disposition of the Japanese fleet had been well known in American naval circles days before the attack.[81] Although the article said nothing about the United States' code-breaking activities, it cited "reliable sources in naval intelligence" and contained a detailed breakdown of the Japanese force and its movements, leading readers to conclude that the United States had broken Japanese codes and was reading the enemy's encrypted communications.[82] The Justice Department went so far as to appoint an outside prosecutor and convene a grand jury to consider whether to indict the *Tribune* and its owner, editor, and publisher, Robert McCormick, for violating the Espionage Act of 1917.[83] Ultimately, no charges were brought, in part because military officials were unwilling to share additional classified information about intelligence gathering.[84]

B. *The Pentagon Papers Case:* New York Times Co. v. United States

The closest the Supreme Court has ever come to considering a government prosecution of the press for publishing confidential information concerning national security secrets was in *New York Times Co. v. United States*.[85] In 1967, Secretary of State Robert McNamara ordered a full-scale evaluation of the United States' involvement in the Vietnam War, which was documented in a forty-seven volume report.[86] Daniel Ellsberg, a former Defense Department economist who was disillusioned with the war, copied portions of the report and sent them to the newspapers.[87] On June 13, 1971, the *New York Times* began publishing excerpts of what became known as the "Pentagon Papers."[88] The Nixon administration immediately sought to restrain further publication, and within a month, the Supreme Court handed down a per curiam decision.[89] Six justices held that the government had not met its "heavy burden of showing justification" for a prior restraint on the press and that the *Times* therefore was free to continue to publish the Pentagon Papers.[90] Although Justice Stewart, with whom Justice White joined, was convinced the executive branch was correct that some of the documents should not be published in the national interest, Stewart commented that he could not "say that disclosure of any of them will surely result in the direct, immediate, and irreparable damage to our Nation or its people."[91]

Although the Court did not specifically decide "whether the First Amendment immunizes the press from criminal prosecution for publishing national defense information," five members of the Court—Justices White, Stewart, Blackmun, and Marshall and Chief Justice Burger—seemed to suggest that the statutes could impose criminal liability on newspapers for retaining or publishing national security secrets. Justice White, joined by Justice Stewart, stated,

> [F]rom the face of subsection (e) and from the context of the Act of which it was a part, it seems undeniable that a newspaper, as well as others unconnected with the Government, are vulnerable to prosecution under § 793(e) if they communicate or withhold the materials covered by that section.[92]

Justice Marshall commented that it was plausible that subsection 793(e) applied to press publications.[93] Chief Justice Burger and Justice Blackmun, in dissent, respectively registered "general agreement" and "substantial accord" with Justice White's views on the issue.[94]

Only Justices Black and Douglas disagreed. Justice Black stated that "only a free and unrestrained press can effectively expose deception in government."[95] Justice Douglas similarly observed that "open debate and discussion of public issues are vital to our national health."[96] Justice Douglas further concluded that section 793(e) does not apply to the press because the statute prohibits unlawful "communication," not "publication" of protected national defense information.[97]

However, because *New York Times* involved a prior restraint, a type of speech that bears a particularly "heavy presumption against its Constitutional validity," the issue of whether section 793(e) can be used to prosecute the press for gathering, publishing, or retaining confidential national security information remains an open question. Indeed, "in the thirty-five years since the Pentagon Papers case, the Supreme Court has not *once* upheld a content-based criminal prosecution of truthful speech relating to the activities of government that did not involve some special circumstances, such as public employment."[98]

Prompted by the Court's per curiam decision in *New York Times*, Harold Edgar and Benno Schmidt Jr. in 1973 analyzed with painstaking detail the legislative history of the Espionage Act and the potential consequences of prosecuting the press under it.[99] Edgar and Schmidt opined that sections 793(d) and (e) were sweepingly broad and were not intended to be applied to the "publica-

tion of defense information that is motivated by the routine desires to initiate public debate or sell newspapers."[100] They also argued that the term *willfully* in both sections 793(d) and (e) must be construed to exclude conduct undertaken by the press for purposes of stimulating public debate; otherwise, the statutes would be vague and unconstitutional under the First Amendment.[101]

The scholars relied on two key historical points in coming to the conclusion that sections 793(d) and (e) do not apply to the press:

(1) In considering the Espionage Act of 1917 and the predecessor statutes to sections 793(d) and (e), Congress rejected a provision that would have allowed the President to prohibit newspapers from publishing information concerning the national defense;[102] and

(2) When the Espionage Act was amended in 1950 (creating the sections now known as 793(d) and (e)), both the Legislative Reference Service and the Attorney General opined that section 793 would not in their view apply to conduct ordinarily engaged in by newspapers.[103] The same legislative history was previously cited by Justice Black in *New York Times* for his conclusion that section 793(e) does not apply to the press.[104]

C. Bartnicki v. Vopper

In a case not concerning a prosecution under the Espionage Act, the Supreme Court recently held in *Bartnicki v. Vopper*[105] that where a journalist receives information "from a source who has obtained it unlawfully," the journalist may not be punished for receipt or publication of the information "absent a need of the highest order."[106] In that case, "a radio commentator[] received in the mail from an anonymous source a tape recording of an unlawfully intercepted telephone conversation, which [he] played on the air" during his radio show.[107] The Court rejected the government's argument that it should be able to punish journalists to deter those who unlawfully intercept conversations, stating that "[i]t would be quite remarkable to hold" that a law-abiding journalist can be punished merely for receiving and publishing information merely "to deter conduct by a non-law abiding third party."[108] Although Vopper admittedly received "stolen" property, the Court held that he was nevertheless protected by the First Amendment because Vopper played no role in the illegal interception, he had obtained the information lawfully, and the information received involved a matter of public concern.[109] Thus, the Court observed, "a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.[110]

IV. APPLICATION TO THIS CASE

"To date, there has been no case in which a working journalist in passive receipt of classified information has been prosecuted under the [Espionage Act]" for gathering, retaining, or publishing the information.[111] Moreover, the little existing precedent in Espionage Act cases differs significantly from our case. In *Gorin*, *Morison*, *Truong Dinh Hung*, and *Squillacote*, the defendants had either given direct assistance to a foreign government or actively misappropriated classified information. Here, on the other hand, the defendant reporter Gilbert passively received the classified information, which was unsolicited and voluntarily given to him for his use in a news report. Likewise, Gilbert had no intention of harming the U.S. government or assisting a foreign government. Further, with the exception of *Gorin*, the defendants in previous Espionage Act cases were government employees who had access to classified information by virtue of their employment and transmitted that information in violation of an agreement with the government. Here, of course, Gilbert and the *Inquirer* are members of the news media who received information, unsolicited, from a government employee. They neither sought out nor misappropriated the classified information.

Further, in analyzing the statutory language of section 793 and Supreme Court and Fourth Circuit precedent, it is evident that Gilbert and the *Inquirer*'s actions fall outside the scope of the Espionage Act.

A. *Sections 793(a) and (b)*

Sections 793(a) and (b) of the Espionage Act concern obtaining and copying information related to the national defense and do not mention communicating such information to others, much less publishing that information. As such, these two sections on their face do not apply to the actions of Gilbert or the *Inquirer*.

Moreover, even if sections 793(a) and (b) applied to press publications in general, they do not apply to Gilbert and the *Inquirer* here because the information is not "relating to the national defense," as that phrase has been defined by the U.S. Supreme Court and the Fourth Circuit. The information given to Gilbert concerned the fact that the government was secretly wiretapping opposing political leaders, including 2008 presidential election front-runners, members of Congress, and the press who were critical of the government. In contrast, in *Gorin*, the Supreme Court defined *relating to the national defense* as "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[112] In *Truong Dinh Hung*, the Fourth Circuit expanded the phrase to include more than military matters, such as U.S. diplomatic cables and classified documents pertaining to the 1977 Paris peace negotiations and names of sources of intelligence.[113] But neither court has gone so far as to include within that definition information that is unflattering of the government, such as a policy to illegally wiretap political opponents.

Setting aside issues relating to the nature of the material, Gilbert and the *Inquirer* nevertheless fall outside the scope of the Espionage Act given the strict scienter requirements imposed by *Gorin.* Under *Gorin*, proof of bad faith, i.e., "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation," is required to sustain a conviction under section 793(a) or (b).[114] Gilbert and the *Inquirer* obtained the information to inform the public on a matter of public concern, not to injure the United States or advantage a foreign nation. Accordingly, they cannot be liable under sections 793(a) and (b).

B. *Sections 793(d) and (e)*

The two sections of the Espionage Act that create the most difficulty in a case involving a criminal prosecution of a member of the news media are sections 793(d) and (e). Section 793(d), however, cannot and does not apply to Gilbert and the *Inquirer* because the statute prohibits anyone lawfully having possession of a document, writing, photograph, etc., "relating to the national

defense" from "willfully" communicating or transmitting it to anyone not entitled to receive it.[115] Because the classified documents were leaked to Gilbert and the *Inquirer*, they did not have "lawful" possession of the documents, as that term is defined in the statute.

Section 793(e), on the other hand, addresses the situation presented here and provides, in pertinent part, that

> (e) whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.[116]

Gilbert and the *Inquirer* had unauthorized possession of the documents; therefore, an analysis under this section is appropriate. Nevertheless, in considering the scope of the scienter requirements, Gilbert and the *Inquirer* are shielded from prosecution under this statute as well.

First, as mentioned above in the discussion pertaining to sections 793(a) and (b), the information given to Gilbert cannot be characterized as relating to the national defense. As Judge Wilkinson stated in *Morison*, "The espionage statute has no applicability to the multitude of leaks that pose no conceivable threat to national security but threaten only to embarrass one or another high government official."[117]

In addition to requiring proof that Gilbert and the *Inquirer* committed the prohibited acts willfully, the statute imposes an additional scienter requirement that the information was communicated with "reason to believe it could be used to the injury of the United States or to the advantage of any foreign nation."[118] As the court in *Rosen* stated,

> requiring the government to prove that "the possessor has reason to believe [the information relating to the national defense] could be used to the injury of the United States or to the advantage of any foreign nation" is not duplicative of the requirement that the government prove the defendant willfully disclosed information that is potentially damaging to the United States because the latter concerns only the quality of the information, whereas the former related to the intended (or recklessly disregarded) effect of the disclosure.[119]

Gilbert and the *Inquirer* obtained the information to engage the public in a matter of public concern, not to injure the United States or advantage a foreign nation. Thus, section 793(e) does not apply to Gilbert or the *Inquirer* in this instance.

Finally, section 793(e) does not apply to the defendants because the phrase *not entitled to receive it* does not prohibit the transfer of classified information from one citizen to another but only from a government employee to a citizen. In *Morison*, the Fourth Circuit determined that the phrase *entitled to receive* is regulated by the government's uniform classification system for national security information,[120] which classifies information into three categories—Top Secret, Secret, and Classified—depending on the degree of harm to the United States that would result from the information's disclosure.[121] The 1951 executive order that created the classification system did not regulate the transfer of information from citizen to citizen but merely requested government employees to observe the standards and join the federal government to prevent disclosure.[122] Thus, *Morison*'s interpretation of *entitled to receive* does not apply to Gilbert and the *Inquirer* in this case.

In addition, the information leaked to Gilbert and the *Inquirer* pertaining to the government's secret wiretapping of its political opponents should not have been classified and therefore does not fall within the scope of any of the Espionage Act statutes. The danger in wrongful classification of documents is obvious. As Justice Stewart observed in the Pentagon Papers case, "[w]hen everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection and self-promotion."[123]

As Gilbert's and the *Inquirer*'s actions do not fall within the scope of the Espionage Act, their prosecution can be characterized as one of seditious libel, which is unconstitutional under the First Amendment. It is axiomatic that political speech and newsgathering are protected by the First Amendment.[124] Moreover, as the Supreme Court observed in *Bartnicki*, the dissemination of truthful information about matters of public concern is protected from liability under the First Amendment as long as the secondary transmitter of the information was not involved in the initial illegality.[125] Although arising under Title III, the Supreme Court's analysis in *Bartnicki* applies equally here. As the Court stated in *Bartnicki*, "it would be quite remarkable to hold" that a law-abiding journalist can be punished merely for receiving and publishing information "to deter conduct by a non-law-abiding third party."[126] The source's conduct in unlawfully obtaining and disclosing classified information to Gilbert and the *Inquirer* does not remove their First Amendment protection for speech about a matter of public concern.[127]

Endnotes

1. Government's Consolidated Responses to Defendants' Pretrial Motions at 16, United States v. Rosen, No. 1:05CR225 (E.D. Va. Aug 9, 2006).
2. United States v. Rosen, 445 F. Supp. 2d 602, 607 (E.D. Va. 2006).
3. *Id.* at 607–10.
4. *See* James H. Landman, *Trying Beliefs: The Law of Cultural Orthodoxy and Dissent*, INSIGHTS ON L. & SOC'Y 2.2 (Winter 2002).
5. *Id.* (discussing De Libellis Famosis, (1606) 77 Eng. Rep. 250).
6. *Id.*
7. Sean Michael McGuire, *Media Influence and the Modern American Democracy: Why the First Amendment Compels Regulation of Media Ownership*, 4 CARDOZO PUB. L. POL'Y & ETHICS J. 689, 691–92 (2006).
8. CHARLES N. DAVIS, SEDITIOUS LIBEL (Nat'l Newspaper Ass'n ed., 2006), www.nna.org/AboutNNA/Current%20Press%20Releases/Seditious%20Libel.htm.
9. *Id.*
10. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 276 (1964).

11. McGuire, *supra* note 7, at 691–92.
12. Am. Booksellers Ass'n v. Hudnut, 771 F.2d 323, 329–30 (7th Cir. 1985), *aff'd*, 475 U.S. 1001 (1986).
13. *Sullivan*, 376 U.S. at 273–76.
14. *Id.* at 275.
15. *Id.*
16. Davis, *supra* note 8.
17. DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS 249 (1997).
18. *Id.* at 250.
19. *Id.* at 250–51 (citing H.R. 291, 65th Cong., 1st Sess. § 2(c) (1917)).
20. 249 U.S. 47 (1919).
21. *Id.* at 48–49.
22. *Id.* at 51–52.
23. *Id.* at 52.
24. 250 U.S. 616 (1919).
25. *Id.* at 617–18.
26. *Id.* at 619, 623.
27. *Id.*
28. James L. Swanson, *Judicial Elections and the First Amendment: Freeing Political Speech*, *in* CATO SUPREME COURT REVIEW 85, 94 (James L. Swanson ed., 2001–02).
29. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).
30. United States v. Rosen, 445 F. Supp. 2d 602, 613 & n.7 (E.D. Va. 2006) (citing N.Y. Times Co. v. United States, 403 U.S. 713, 754 (1971)); *see also* United States v. Morison, 844 F.2d 1057, 1086 (4th Cir. 1988); Harold Edgar & Benno C. Schmidt, Jr., *Curtiss-Wright Comes Home: Executive Power and National Security Secrecy*, 21 HARV. L. REV. 349, 393 & n.159 (1986); Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 998 (1973).
31. Rosen, 445 F. Supp. 2d at 613.
32. 18 U.S.C. § 793 (2006).
33. Such places, include, for example, "any vessel, aircraft, work of defense, navy yard, naval station, submarine base, coaling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, or other place connected with the national defense. . . ." 18 U.S.C. § 793(a).
34. 18 U.S.C. § 793(a).
35. 18 U.S.C. § 793(b).
36. 18 U.S.C. § 793(d).
37. 18 U.S.C. § 793(e).
38. 312 U.S. 19, 23 (1941).
39. *Id.* at 22–23.
40. *Id.* at 28.
41. *Id.*
42. *Id.* at 27–28.
43. *Id.*
44. 629 F.2d 908 (4th Cir. 1980).
45. *Id.* at 917–18.
46. *Id.* at 918.
47. *Id.* at 919.
48. *Id.* at 919 n.10.
49. United States v. Morison, 844 F.2d 1057, 1068–70 (4th Cir. 1988).
50. *Id.*
51. *Id.* at 1060–62.
52. *Id.* at 1063.
53. *Id.*
54. *Id.*
55. *Id.* at 1074.
56. *Id.*
57. *Id.* at 1071.
58. *Id.* at 1071–72.
59. *Id.* at 1071.
60. *Id.* at 1067.
61. *Id.* at 1068 (quoting Branzburg v. Hayes, 408 U.S. 665, 691 (1972)).
62. *Id.* at 1070.
63. *Id.* at 1081 (Wilkinson, J., concurring).
64. 221 F.3d 542, 578 (4th Cir. 2000).
65. *Id.*
66. *Id.*
67. United States v. Rosen, 445 F. Supp. 2d 602, 607 (E.D. Va. 2006).
68. *Id.* at 618–20.
69. *Id.* at 620.
70. *Id.*
71. *Id.* at 622–23.
72. *Id.* at 623–25.
73. *Id.* at 624–25.
74. *Id.* at 625.
75. *Id.* (quoting United States v. Morison, 844 F.2d 1057, 1071 (4th Cir. 1988)).
76. *Id.*
77. *Id.* at 630.
78. *Id.* at 630–31.
79. *Id.* at 637.
80. Douglas McCollam, *The End of Ambiguity*, COLUM. J. REV., July/Aug. 2006.
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. N.Y. Times Co. v. United States, 403 U.S. 713, 718 (1971).
86. Geoffrey R. Stone, *Government Secrecy v. Freedom of the Press*, MLRC BULL. NO. 1, at 14 (2007).
87. *Id.*
88. *Id.*
89. *N.Y. Times Co.*, 403 U.S. at 714.
90. *Id.*
91. *Id.* at 730.
92. *Id.* at 740.
93. *Id.* at 745 (Marshall, J., concurring).
94. *Id.* at 752, 759.
95. *Id.* at 717.
96. *Id.* at 724.
97. *Id.* at 721 (Douglas, J., concurring).
98. Stone, *supra* note 86, at 19.
99. Edgar & Schmidt, *Espionage Statutes*, *supra* note 30.
100. *Id.* at 1033.
101. *Id.* at 1038–46, 1057–58.
102. *Id.* at 946–65.
103. *Id.* at 1025–26, 1030–31.
104. N.Y. Times Co. v. United States, 403 U.S. 713, 721 (1971).
105. 532 U.S. 514 (2001).
106. *Id.* at 527–28.
107. Stone, *supra* note 86; *see also Bartnicki*, 532 U.S. at 519–20.
108. *Bartnicki*, 532 U.S. at 529–30.
109. *Id.* at 525.
110. *Id.* at 535.
111. McCollam, *supra* note 80.
112. Gorin v. United States, 312 U.S. 19, 28 (1941).
113. United States v. Truong Dinh Hung, 629 F.2d 908, 917–18 (4th Cir. 1980).
114. *Gorin*, 312 U.S. at 27–28.
115. 18 U.S.C. § 793(d) (2006).
116. 18 U.S.C. § 793(d).
117. United States v. Morison, 844 F.2d 1057, 1085 (4th Cir. 1988) (Wikinson, J., concurring).
118. 18 U.S.C. § 793(d), (e).
119. United States v. Rosen, 445 F. Supp. 2d 602, 626 (E.D. Va. 2006).
120. *Morison*, 844 F.2d at 1073–74.
121. The designation "Top Secret" applies to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the country's national security. The designation "Secret" applies to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the country's national security. The designation "Confidential" applies to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the country's national security. Exec. Order No. 13,292, 68 Fed. Reg. 15,326 (Mar. 25, 2003).
122. Edgar & Schmidt, *supra* note 30.
123. N.Y. Times Co. v. United States, 403 U.S. 713, 729 (1971).
124. *See, e.g.*, Vieth v. Jubelirer, 541 U.S. 267, 324 (2004).
125. Bartnicki v. Vopper, 532 U.S. 514, 529–35 (2001).
126. *Id.* at 529–30.
127. *Id.* at 535.

The Newspaper-Broadcast Cross-Ownership Rule: The Case for Regulatory Relief

KATHLEEN A. KIRBY AND MATTHEW L. GIBSON

In 1975, Bruce Springsteen released his third album, *Born to Run.* Bill Clinton married Hillary Rodham, and Bill Gates used the term *Microsoft* for the first time in a letter to Paul Allen.[1] Newspaper readership was at its peak, and television viewers uniformly tuned in for evening news delivered by one of three network anchors: Walter Cronkite, John Chancellor, and Harry Reasoner.[2] AM Top 40 radio dominated, and FM had not yet reached the mainstream.[3] Cable systems were just sprouting,[4] and Sony marketed its innovative Betamax recorder for the exorbitant sum of $2,295.[5] Given America's presumably unavoidable reliance on newspapers and broadcast outlets as sources of news and information, the Federal Communications Commission (FCC or Commission) in 1975 promulgated rules prohibiting a daily newspaper publisher from owning broadcast stations in the same community, ostensibly to prevent any single corporate entity from becoming too powerful a voice within a community.

Thirty years later, the Boss released his twentieth album but had to contend with digital piracy. Bill Clinton, impeached but popular, took a backseat as Senator Hillary Rodham Clinton announced over the Internet her own presidential intentions; and multibillionaire Bill Gates split his time between hawking Microsoft products and philanthropic pursuits. Today, American consumers have virtually limitless choices in news and informational content on every subject imaginable, delivered in an ever-expanding variety of forms to suit every taste and schedule.

The challenges facing companies that professionally gather and publish local, national, and international news and information have become acute. The newspaper industry is wrestling with declining circulation and rising competition for advertising, and prominent publishing companies are on the auction block. With similar challenges facing broadcasters, Disney remarked in comments to the Commission that "[g]iven the increase in, and attractiveness of, new media outlets, the Commission may soon find itself considering ways to incent, rather than restrict, ownership of over-the-air broadcast stations."[6]

At the same time, in response to a congressional mandate, the FCC reviewed certain of its media ownership rules and attempted to relax some of them. After much legal wrangling and in the context of a dramatically different media sector, the U.S. Court of Appeals for the Third Circuit, although finding that the "blanket ban on newspaper/broadcast cross-ownership [is] no longer in the public interest,"[7] remanded the proposed rule changes to the FCC for further justification. Remarkably, in a world where traditional media companies are constantly revamping their business models in the face of new technologies and where the diversity of outlets vying for consumers' attention can be overwhelming, common ownership of daily newspapers and broadcast stations serving the same market still is prohibited, except in certain limited circumstances.[8]

The newspaper-broadcast cross-ownership ban has existed without any modification for more than thirty years. Today, the traditional media industries are in tumult. Help, however, may not be imminently forthcoming. Today's Commission appears caught in the vortex created by the Third Circuit's remand of the agency's attempt to reform its ownership rules, the claims of competing interest groups, and a shift in the political winds. Many therefore predict that the FCC will be slow to implement any further ownership deregulation.

For the past three years, there has been no active legal dispute as to whether the complete prohibition of newspaper-broadcast cross-ownership should exist. Although both the agency and the Third Circuit agree that a global ban on newspaper-broadcast cross-ownership disserves the public interest and should not be preserved,[9] the blanket ban persists—not as a public benefit but as an artifact of the Commission's failed attempt to unite its cross-ownership and local ownership policies into a single grand integrated theory of media ownership. The significance of such a ban is that as technological advances accelerate, the existing cross-ownership rule robs traditional media outlets of the option to compete, perhaps even to survive, during what can only be fairly characterized as a seismic shift in the media landscape.

Thirty Years of Regulation

Given the tenure of the newspaper-broadcast cross-ownership ban (also known as the Newspaper Rule), commentators, courts, and FCC commissioners have summarized the rule hundreds, if not thousands, of times. Nonetheless, for those new to the discussion, a brief overview of the Newspaper Rule's history follows.

In 1975, the Commission adopted regulations that prohibited a daily newspaper publisher from obtaining broadcast licenses in its paper's community.[10] When it implemented the Newspaper Rule, the Commission believed that common ownership of daily newspapers and broadcast stations would not enhance the diversity of viewpoints available to the public; instead, the Commission feared that common ownership would preclude new voices from obtaining the decreasing number of available broadcast licenses.[11]

Even in its decision adopting the ban, the Commission acknowledged the potential detriments of the prohibition and

---

Kathleen A. Kirby is a partner at Wiley Rein LLP. In 1975, when The Captain & Tennille in heavy rotation drove her from 77WABC to fledgling FM radio, she was introduced to the Boss and spent part of her first $15 paycheck on Born to Run*. Since that first experiment with FM radio, she has continued to embrace new information and entertainment technologies.*

Matthew L. Gibson is an associate at Wiley Rein. In 1975, he was not yet born. Today, he gets his news and information from online aggregators, newspapers, and the radio.

the uncertain foundation on which it was enacted. In particular, the agency recognized the pioneering spirit of cross-owners and specifically concluded that newspaper-affiliated stations tended to be superior licensees, particularly in terms of locally oriented service.[12] To justify the restriction when it was adopted three decades ago, the FCC relied on what the agency itself acknowledged to be a "mere hoped for gain in diversity."[13]

Given its speculative origins, it is not at all surprising that the efficacy of the cross-ownership ban has long been in question at the Commission. As early as 1996, in approving the merger of ABC and the Walt Disney Company,[14] the agency stated its intention to "commence an appropriate proceeding to obtain a fully informed record in this area and to complete that proceeding expeditiously."[15] Then-Chairman Reed Hundt, appointed by President Clinton, issued a separate statement emphasizing his concern that "there is reason to believe that . . . the newspaper-broadcast cross-ownership rule, is right now impairing the future prospects of an important national source of education and information: the newspaper industry."[16] The FCC subsequently reneged on the promise to conduct a broad review, however, initiating an inquiry only with respect to the much narrower issue of amending the existing waiver policy for newspaper-radio cross-ownership.[17]

First Biennial Review

Without completing that proceeding, the FCC released in March 1998 a notice of inquiry to commence the first biennial review proceeding pursuant to Section 202(h) of the Telecommunications Act of 1996.[18] That inquiry represented the Commission's first effort to carry out the congressional mandate to determine periodically whether any of its broadcast ownership restrictions "remain necessary in the public interest as the result of competition" and to repeal or modify any rules that do not meet this stringent test.[19] In addition to seeking comment on all of its media ownership rules, the agency noted that it "anticipate[d] taking action in the [newspaper-radio waiver proceedings] during 1998."[20] The Commission, however, took no action until June 2000, when, after Congress intervened to set a specific deadline, the agency finally issued its 1998 Biennial Review Report.[21] Recognizing that "there may be circumstances in which the rule may not be necessary to achieve its public interest [objectives]," the FCC committed to "initiate a rulemaking proceeding to consider tailoring the rule accordingly."[22]

Well over a year later, the Commission finally sought comment on a broad list of questions ranging from retention of the rule in its existing form to complete repeal.[23] Extensive comments were filed by a wide array of industry participants, public interest organizations, and individual consumers.[24] Although the 2001 cross-ownership proceeding was ripe for decision, the FCC determined instead to roll it into its 2002 Omnibus Rulemaking, which included consideration of several other media ownership rules and was designated as the Commission's 2002 Biennial Review.[25]

This omnibus proceeding was conducted in response to a series of decisions by the D.C. Circuit repudiating the reasoning underlying the FCC's decisions to retain certain of its broadcast ownership restrictions in past biennial review orders. In both *Fox Television Stations v. FCC* and *Sinclair Broadcast Group v. FCC*, the court strongly reprimanded the agency for failing to buttress with solid factual evidence or logical reasoning its decisions to retain national and local limits on television station ownership.[26]

In response, the FCC tried to make its 2002 Omnibus Rulemaking the most "comprehensive" review of media ownership ever undertaken by the agency.[27] As the Third Circuit observed in its review of the agency's decision in the proceeding, "interested parties filed thousands of pages of comments, consisting of legal, social, and economic analyses, empirical and anecdotal evidence, and industry and consumer data to respond to the issues identified in the Commission's Notice."[28] In conjunction with this proceeding, the FCC also established a Media Ownership Working Group (MOWG), which commissioned a number of independent studies, including several that focused specifically on issues related to newspaper-broadcast cross-ownership.[29] After extensive analysis of the mammoth record in the proceeding, the Commission released the text in June 2003.

Tiered Approach

Based on its review of the existing record, the Commission determined that it could no longer justify the complete ban on common ownership of daily newspapers and broadcast stations in the same market.[30] Although it found that a complete cross-ownership prohibition did not promote the public interest, the Commission chose to retain some limitations on media cross-ownership.[31] In its 2003 Report and Order, the Commission opted for a tiered approach in which (1) an outright ban would remain in markets containing fewer than four full-power television stations, (2) some cross-ownership would be permitted in markets with four to eight full-power television stations, and (3) cross-ownership would be freely permitted in markets with more than eight full-power television stations.[32] Few, if any, parties were completely satisfied with the Commission's new approach to the Newspaper Rule or the other ownership rules under review. The resulting appeals were consolidated in the Third Circuit under *Prometheus Radio Project v. FCC.*

Although the Commission and the Third Circuit quibble over whether Section 202(h) is a "one-way [deregulatory] ratchet," they seemed in accord that "regulation[s] deemed useful when promulgated must remain so" or be repealed or modified.[33] The appeals court agreed that the newspaper-broadcast cross-ownership ban no longer served the public interest and should therefore be eliminated. But because the court disagreed with the Commission's justification for its tiered approach,[34] the total ban, which both bodies viewed as harmful to the public interest, remains in effect today. *Prometheus* thus ignited another round of rule making. Now that additional comments have been filed in the remand proceeding, which has been combined with a revised congressional mandate to review the media ownership rules quadrennially,[35] the industry awaits a Commission decision.

The Saga Continues?

The Third Circuit put the Commission in an awkward position in its remand of the revisions to the Newspaper Rule. Although it agreed that the Commission was under a statutory mandate to "repeal or modify" a ban that no longer served the public interest, the Third Circuit allowed the Newspaper Rule to persist.

On remand, comments and studies from all points along the regulatory/ dereg-

ulatory spectrum have only fueled the cross-ownership debate. Despite the ownership proceedings' cumbersome record, the task before the Commission is, as a legal matter, imperative and straightforward: it must consider the record before it, account for the many changes that have taken place in the media marketplace since 2003 (as well as those that can be anticipated before its next review of the ownership rules in 2010), and move quickly to square its regulatory regime with the realities of an astonishingly diverse and demanding media marketplace.

Republican FCC Chairman Kevin Martin is seeking to avoid the intense criticism that his predecessor, Michael Powell, faced after Powell's Commission, by a partisan three-to-two vote, approved liberalizing the media ownership rules in 2003. However, Martin's cautious approach, combined with the shift in control of Congress, seems to have doused any prospect of swift agency action to conform cross-ownership regulation to technological reality. In response to criticism that the FCC's review of the media ownership rules was done largely behind closed doors in a secretive manner, the Commission is in the process of staging six so-called media ownership road shows designed to solicit additional public comment on the need for regulation.[36] In addition, the FCC has committed to concluding a long-standing proceeding on broadcast localism before turning to the media ownership dilemma.[37]

Despite the comprehensive record already in existence, the agency has commissioned ten new studies: How People Get News and Information; Ownership Structure and Robustness of Media; Effect of Ownership Structure and Robustness on the Quantity and Quality of TV Programming; News Operations; Station Ownership and Programming in Radio; News Coverage of Cross-Owned Newspapers and Television Stations; Minority Ownership (two separate studies); Vertical Integration; and Radio Industry Review: Trends in Ownership, Format, and Finance. Each of the studies will be completed and released for public comment before the Commission takes further action with regard to media ownership regulation.[38]

Although there has been some suggestion that consideration of the ban should be separated from the FCC's review of other media ownership rules (e.g., limits on local radio and television ownership), that does not appear likely. As newspapers and broadcasters remain indefinitely *Prometheus* bound, opportunities to attain the synergies owners claim are associated with combined print, radio, television, and online news (e.g., cross-promotion, shared newsgathering resources, and packaged multimedia advertising deals) seem to have evaporated. On both sides of the debate, it has become increasingly clear that the debate must now be framed by developments in new media.

Trailing Behind Technology

Innovation is annoyingly ignorant of pleading cycles, and, as many parties have noted, the media landscape has changed dramatically even over the five years since the Commission began its assessment of the cross-ownership ban in its 2002 Biennial Review. Although the current political environment seems to favor increased regulation, the Commission has ample cause to make cross-ownership restrictions the exception rather than the rule. Indeed, it would be folly not to do so.

In 2003, based on the wide-ranging record before it, the Commission concluded thus: "(1) the [newspaper-broadcast cross-ownership] rule cannot be sustained on competitive grounds, (2) the rule is not necessary to promote localism (and in fact may harm localism), and (3) most media markets are diverse, obviating a blanket prophylactic ban on newspaper-broadcast combinations."[39] The Third Circuit resoundingly upheld these critical judgments concerning newspaper-broadcast cross-ownership.

Local Markets Are Well-Served

At this point, therefore, it would appear that the Commission need only speak to the court's limited concerns regarding perceived flaws in the agency's viewpoint diversity analysis. The FCC could simplify its task by eschewing any metric and focusing on whether consumers in individual media markets have a sufficient number of news and informational outlets available to them so as to ensure that they will be well informed and exposed to a variety of viewpoints. In this digital era, particularly given the evolution of the Internet into a fundamental and widely used source of world, national, and local news, information, and opinion, there is no question that audience members in local markets of all sizes are well served by a vast range of traditional and alternative media outlets.

The most recent round of FCC comments, which belabor questions of localism and competition already resolved by the Third Circuit; the tenor of media ownership hearings held around the country; statements from congressional leaders; and the Commission's own reluctance to act suggest an unwillingness to accept the extent to which today's media landscape differs from that of 1975. To some, though, it seems obvious that the abundant sources of information, entertainment, and viewpoints available to today's consumers have rendered any discussion of whether structural ownership regulations are necessary to preserve diversity in today's media marketplace almost nonsensical. The realities of the twenty-first century marketplace and the experiences of same-market newspaper-broadcast combinations, as well as the obvious need for regulatory parity, overwhelmingly support repeal of the newspaper-broadcast cross-ownership ban.

A Reality Check

If American media companies are to thrive, the Commission and the courts cannot continue to react as though it is 1999. In the three years since the Third Circuit's *Prometheus* decision, innovation has once again transformed Americans' appetite for information such that the 2002 Biennial Review and *Prometheus* now seem quaint. The past three years have seen the development of new classes of media outlets, new theories of information sharing, and new methods of information gathering. Since *Prometheus,* Americans have experienced so many technological revolutions that the term is beginning to lose its meaning.[40] Each passing revolution merely adds to the Commission's burden of justifying continued regulation of newspaper-broadcast cross-ownership. In responding to the Third Circuit's remand, the Commission must give sufficient weight to the development of several new types of media outlets as truly independent sources of local information as well as to the vicious competition spurred by the low-to-nonexistent barriers to entry for online media.

"A generation ago, only science fiction writers dreamed of satellite-delivered

television, cable was little more than a means of delivering broadcast signals to remote locations, and the seeds of the Internet were just being planted in a Department of Defense project."[41] By 2003, consumers "could select 'from hundreds of channels of video programming . . . in every market in the country and, via the Internet, [could] access virtually any information, anywhere, on any topic.'"[42] Remarkably, in remanding the Commission's numerical ownership limits, the Third Circuit noted that it could not rely on the Commission's finding that Internet sources "mitigate the threat that local station consolidations pose to viewpoint diversity."[43] The experiences of the past three years and the emergence of new media, particularly online media, refute the Third Circuit's position.

Media of Choice?

The Internet has made a remarkable contribution to the marketplace of ideas, and the expansion and fragmentation of the media marketplace has naturally changed the way in which consumers seek and receive their news. Although it is true that newspapers and broadcast stations remain important sources of local news and information,[44] nontraditional media draw an audience that rivals that of mainstream media sources.[45] In addition to traditional media's high-traffic online offerings, micropolitan websites, blogs, and online citizen journalism have proliferated. Newspapers and broadcast stations are no longer the predominant sources of news and information they were in 1975.[46] For many, they are not considered the media of choice.[47]

Technology has also changed the traditional media's role as an information gatekeeper. Now, any motivated Internet user can receive information in quantities and varieties previously known only to publishers and broadcasters that subscribed to costly wire services. By aggregating disparate news sources and providing customized filters to sift through the growing heaps of information, both mainstream search engines (Yahoo! and Google) and emerging services (boglines.com) provide Internet users with a personalized virtual Teletype machine.

Blogs

The term *weblog* was coined on December 17, 1997, by Jorn Barger, who created the term "to describe the process of 'logging the web' as he surfed."[48] The transmutation of *weblog* to *blog* (both in its noun and verb forms) is attributed to Peter Merholz and dates to April or May of 1999.[49] In 2004, the Third Circuit used neither the term *blog* nor *weblog* in its *Prometheus* decision, and Judge Scirica's dissent included only one instance of the term *weblog*.[50] If use of the term *blog* is any measure of its relative importance over time, it is worthwhile to note that twenty-three commentators representing both pro-regulatory and deregulatory interests used *blog* 332 times in their opening comments to the 2006 Quadrennial Review.

The increasing local significance of blogs is supported by the discussions in the comments to the 2006 Quadrennial Review. Indeed, surveys conducted by the Pew Internet & American Life Project (Pew Internet Project) reveal that the number of blog readers is increasing at an explosive rate. In September 2005, the Pew Internet Project surveyed the Internet usage habits of American adults. Of the self-reporting Internet users, 27 percent indicated that they had read another person's blog. Four months later, 39 percent of Internet users stated that they had read one or more blogs.[51]

Pro-regulatory advocates have mounted several attacks on blogs' inclusion in diversity analyses. First, they argue that blogs are "not primarily a journalistic undertaking" and are "just not local news and information."[52] Although such a belief may have been accurate at one time, blogs increasingly provide unique reporting on events of local and national concern, and the comments submitted in the 2006 Quadrennial Review proceeding demonstrate as much. For example, the bloggers at Firedoglake.com reported extensively on the recent trial of Vice President Cheney's former chief of staff, I. Lewis "Scooter" Libby. Firedoglake.com's coverage was widely reported in both new and traditional media.[53]

Blogs can provide original journalistic content on local affairs, too. Take, for example a March 23, 2007, posting on dcist.com, a blog devoted to local affairs in the District of Columbia. In the posting, a blogger discussed recent floor speech in the House of Representatives about the ongoing debate concerning the District of Columbia's congressional representation (or lack thereof). The blogger was intrigued by a floor statement made by a member of Congress, who argued against granting District of Columbia residents a congressional vote because each of the 535 members of Congress already has a vested interest in local affairs in the District of Columbia. Taking him at his word, the blogger provided readers with the congressman's official contact information. Judging from the comments to the post, readers of dcist.com appear to be reaching out to members of Congress on "constituency" issues such as garbage collection and unrepaired potholes.[54]

Emerging local media outlets are not limited to text, however. For example, the photo website Flickr.com, launched in 2004, allows users to contribute, classify, and search an enormous database of photographs. A search for the tag *news* yields more than 30,000 images.[55] Although many of the photographs tagged with *news* are images related to the news industry itself (for example, news vans, television broadcasts, etc.), many photographs capture newsworthy events, such as local fires, vigils, protests, and concerts. Internet users are beginning to make similar use of YouTube.com for video content. YouTube.com, launched in 2005, allows users to search based on text or to browse predefined categories, which include a grouping for "News & Politics."[56]

This expansion in online media is fueled, in part, by the low-to-nonexistent cost of creating a revenue-generating online media outlet. Anyone with Internet access and content can contribute to viewpoint diversity. Many sites, such as Blogger.com, provide free hosting to would-be bloggers. Moreover, bloggers have become increasingly attractive to online advertisers, and the free nature of hosting services does not deprive bloggers of a revenue stream from online advertising. Blogger.com, for example, permits users to recognize advertising revenue through services such as Google.com's AdSense platform.

Over the past several years, the media market has become increasingly decentralized and diverse, and online media have emerged as independent sources of viewpoint diversity and as competing suppliers of advertising space. This decentralization of local

media outlets has not escaped the notice of traditional media. Indeed, *Time*'s selection of You as its "Person of the Year" for 2006 surprised nearly everyone. Despite the ongoing conflict in Iraq, the trial and execution of a deposed Iraqi dictator, and the power-shifting midterm congressional elections, *Time*'s editors saw 2006 primarily as "a story about community and collaboration on a scale never seen before."[57] People-powered media have arrived and are changing the way that Americans consume information.

Learning from Experience

Given the cacophony of voices characterizing the modern media era, the Commission's diversity analysis appears relatively simple and straightforward. The reality, though, is that the Commission's analysis has been endlessly complicated by political influences. To combat the hue and cry over the evils of so-called Big Media, deregulatory proponents have continued to speak to the wealth of data demonstrating media cross-ownership's real-world benefits: newspaper-broadcast combinations across a broad spectrum of markets provide exceptional local content and community-oriented service.

When it banned newspaper-broadcast cross-ownership in 1975, the Commission chose not to break up then-existing combinations. The FCC elected to require divestitures only in a narrow range of circumstances because a "mere hoped for gain in diversity,"[58] which it previously described as an "abstract goal,"[59] could not justify sweeping divestiture requirements. These grandfathered combinations, along with newspaper-broadcast combinations that exist pursuant to waivers or under a policy that permits a broadcast station owner to acquire a newspaper in the same market and operate it until the end of the station's license-renewal term,[60] have demonstrated important advantages of cross-ownership.

As the newspaper and broadcast industries have evolved, local newspaper-owned television stations have had the unique opportunity to experiment and find synergies between the two businesses. On the whole, existing combinations show that local cross-ownership is a stabilizing economic force that allows for efficient use of assets to provide diverse local programming. Given the ability of news industries to share newsgathering resources with sister outlets and the journalistic and community-oriented traditions that daily newspapers bring to the table, it makes perfect sense that cross-ownership would generate these benefits. Researchers have long concluded that the operational efficiencies made possible by cross-ownership enable outlets to compete more effectively and to focus on their core local service objectives.[61]

That '70s Show

In its 1975 Report and Order, the Commission praised newspapers' "pioneering spirit" in the early days of radio; then it instituted a ban on all future newspaper-broadcast cross-ownership. At that time, the Commission focused on competition, viewpoint diversity, and ownership diversity but did not give sufficient weight to existing evidence that cross-ownership promotes localism.[62] Since then, the Commission has adopted localism as a third public interest goal; thus, it is interesting to note that what was true in 1973 remains so today: newspaper-broadcast combinations promote this public interest goal.[63]

In its 1975 Report and Order, the Commission made a passing reference to seven studies that, in today's terms, analyze issues of localism. With one outlier, the studies largely disprove the argument that cross-ownership harms localism.[64] More importantly, the Commission's Staff Study of 1973 Television Station Annual Programming Reports, which was the first study to use 1973 annual programming reports, showed a statistically significant increase in the amount of local programming broadcast by newspaper-owned television stations.[65] Specifically, the Commission staff found that after controlling for variables such as market size, network affiliation, and group ownership, the average "co-located newspaper-owned" television broadcaster produced 12 percent more local programming than did other television broadcasters in 1973.[66]

More and Better Local Planning

The same conclusion, that cross-owned outlets offer more and better local programming, has been reached time and time again.[67] The Third Circuit agreed with the Commission's assessment that "the newspaper/broadcast cross-ownership ban undermined localism."[68] Nevertheless, virtually every commentator in the 2006 Quadrennial Review devoted significant energy to explain how newspaper-broadcast cross-ownership promotes or inhibits the Commission's goal of localism. Inasmuch as the Commission uses local news programming as a localism yardstick, the existing combinations' experience strongly supports the deregulatory position.[69]

In Fredericksburg, Virginia, the combined resources of the *Free Lance-Star* and its three radio stations create efficiencies permitting reporters more easily to cover stories in distant communities. This combination also permits important local breaking news to be disseminated quickly and accurately.[70] The quality of local coverage has not suffered because of the newspaper and radio stations' integrated operations. Both the stations and the *Free Lance-Star* have received dozens of awards for the quality of their journalism.[71] Similarly, as the result of the efficiencies created by the joint ownership of the *News-Gazette*, WDWS (AM), and WHMS-FM in Champaign, Illinois, WDWS (AM) replaced a syndicated news show with a locally produced three-hour daily talk show.[72] Anecdotal evidence suggests that WHMS-FM is the only music station in its market that employs a full-time news staff.[73] As a result, WHMS-FM broadcasts forty hours of local news programming each week.[74]

Studies and More Studies

Media General has provided for the Commission a detailed assessment of the locally oriented value each of its six newspaper-broadcast combinations adds to its respective market.[75] In a comprehensive study of each combination, Professor Adam Clayton Powell III of the University of Southern California concluded that all six communities received more and better local news and public affairs programming than they would absent the convergence benefits of the combinations.[76] Areas in which benefits can be seen include breaking news, expanded news content, investigative and enterprise pieces, greater understanding of the community,[77] and production of specials and investigative reports that could not have been done on a stand-alone basis.[78] The tangible results are evident in everything from the outlets' joint investigation of the

hurricane-preparedness plans of Tampa-area governments,[79] to an in-depth series on the experiences of parents who have lost children to cancer, to coordination on town hall meetings held for local candidates.[80] Such extensive community-oriented efforts simply would be out of reach for most stand-alone outlets.

Belo Corporation has stated that the existence of its Dallas combination has served as a "direct catalyst" for an overall increase in the quantity and quality of local news available in the market.[81] In particular, Belo explained that the sharing of resources not only has enhanced the news coverage of its co-owned TV station and daily newspaper but also has helped make possible the launch of several additional local and regional outlets, including a regional cable news channel, a Spanish-language daily newspaper, and a free daily specifically targeted to younger readers.[82]

Similarly, in Phoenix, a Gannett-owned combination brings heightened local content to the market. Gannett's KPNX-TV has the highest-rated local newscast,[83] while the *Arizona Republic* has taken advantage of the efficiencies inherent in cross-ownership to increase its in-depth and investigative reporting.[84]

Cox Enterprises also claims localism benefits from its newspaper-broadcast combinations in Atlanta and Dayton.[85] In both of these cross-ownership markets, the broadcast stations have the resources to offer exceptional locally oriented programming. For example, the Atlanta station airs the only weekly half-hour public affairs program in the market, and the Dayton station produces a similar weekly half-hour public affairs program.

Tribune Company currently holds newspaper-broadcast combinations in several markets, including Chicago, New York, Los Angeles, Hartford, and South Florida, some of which are grandfathered and some of which Tribune holds under temporary waivers or pursuant to the FCC's Footnote 25 policy.[86]

The Tribune combination in Chicago, which is grandfathered, is the nation's third-largest market and provides, perhaps, the best case study. According to Tribune's comments filed with the FCC, the newspaper-broadcast combination has allowed each entity to streamline operations and provide more extensive informational coverage by taking advantage of both local efficiencies and companywide resources. The radio station and its sister outlets jointly plan for coverage of special events, such as local and national elections. Likewise, the *Chicago Tribune* works with WGN-TV to co-sponsor public opinion polls before major local, state, and national elections. WGN-TV's chief meteorologist and his staff of professional weather forecasters provide a "weather page" for each daily edition of the *Chicago Tribune.* Moreover, all three media outlets contribute to www.chicagotribune.com, enabling that website to offer far more content than otherwise would be possible.

At Tribune and elsewhere, the websites offered do far more than "merely republish" the content developed by their sister newspaper, radio, or television station.[87] Because of the immense capacity and unique attributes of the Internet, newspaper publishers and broadcasters via the Web greatly differentiate, supplement, and constantly update the information they disseminate to their audiences. These websites host chat rooms about top stories and forums on issues such as elections, public safety, immigration, schools, and even the neighborhood weather. Multiple blogs contain reporting, commentary, and observations on everything from local politics and sports to pop culture. Opinion pages offer venues for readers to state their views.

Economic Survival

Incredibly, certain commentators contend that there is no evidence that the seismic shift in the media landscape has had any competitive impact on newspaper publishers or broadcasters.[88] The record unambiguously demonstrates, however, that traditional broadcasters and newspaper publishers are facing formidable challenges in today's highly fragmented media marketplace.[89] In particular, the flexibility of new and alternative media to react quickly as the paradigm has shifted from "one size fits all" to individualized media "on-demand" is well documented.[90]

As new technology has multiplied the number of media outlets, the traditional print and broadcast media face increased competition for audiences and revenues. The average newspaper's circulation has declined by at least 1 percent per year since 1975, and, over the past several years, the rate of decline has increased noticeably. The value of publicly traded newspaper companies decreased by 20 percent in 2005 and by another 14 percent in 2006.[91] The forced sale of Knight Ridder and Tribune Company's recent public struggle to reach an agreement with a buyer only underscore the diminishing economic power of newspaper publishers.[92] Even the *New York Times* has not been immune to these trends. Its share price has fallen by nearly 40 percent in recent years.[93] The combination of decreased circulation and advertising revenues has forced publishers to cut costs, even to the extent of reducing newsroom staff. It is expected that from 2000 to 2007, newspapers, in aggregate, will employ 7 percent fewer reporters.[94]

Audience Erosion

Television broadcasters are facing a similar problem: audience erosion began with the increased number of offerings by multichannel video providers and has accelerated with the advent of streaming Internet video. For example, in the large markets of New York, Los Angeles, and Chicago, virtually every television broadcast station's share of the total local television viewing audience decreased from 2001 to 2006.[95]

With declining audiences and advertising revenues, newspaper publishers and broadcasters must change their business models in order to remain profitable and to survive in the information age. As the Third Circuit noted in *Prometheus*, newspaper-broadcast cross-ownership can create economic efficiencies without sacrificing journalistic integrity.[96] The record on remand supports the court's observations. For example, Fredericksburg, Virginia's local paper, the *Free Lance-Star,* owns four local radio stations. Through colocation and the merger of some of the five properties' operational, human resources, and administrative staffs, the *Free Lance-Star* recognizes an annual savings of $500,000 while increasing local programming on the radio stations.[97] The publisher of the *News-Gazette* in Champaign, Illinois, has recognized similar economies of scale from cross-ownership. The integration of the *News Gazette*, WDWS (AM), and WHMS-FM results in an annual savings of $100,000 and increased investment

in the stations' news operations.[98]

Media General's experience in Tampa offers yet another example of how cross-ownership of local newspaper and television properties can "reverse the [economic] downturn and profitably provide communities with more and better local news."[99] Before Media General consolidated its news-gathering operations, circulation of the *Tampa Tribune* was declining in key demographics. With the efficiencies created by cross-ownership and operation with WFLA-TV, Media General saw a "level[ing] off [of] circulation declines."[100] But Media General was not the only one to see benefits from the economic buttressing of the *Tampa Tribune.* The cross-ownership efficiencies have allowed WFLA-TV to add an additional thirty minutes of local programming each day. Obviously, economic efficiencies are not anathema to the public interest. [101]

Although it is true that common ownership of a local daily newspaper and a local broadcast station does not maximize diversity of ownership, common ownership is sometimes necessary to maintain the status quo, especially given the state of the industry.[102] One owner of two outlets will always be a better servant of the public interest than two outlets silenced.

Taming *Red Lion*

Finally, it is, of course, worth noting that the *Prometheus* court rejected a constitutional challenge to the Newspaper Rule, finding that the Commission violated neither publishers' nor broadcasters' First Amendment rights through the reformation of the Newspaper Rule.[103] The Third Circuit's constitutional ruling rests primarily on the belief that precedent constrained the court from finding a First Amendment violation in the revised Newspaper Rule. The court's interpretation of precedent, however, confuses its inability to overturn binding precedent with its ability to distinguish a case on the facts. From this perspective, post-*Prometheus* broadcast technologies undermine the Third Circuit's findings.

Shortly after the start of the 1968 inquiry into media ownership, the Supreme Court granted the Commission a regulatory boon in *Red Lion Broadcasting v. FCC.*[104] In upholding the fairness doctrine against a First Amendment challenge, the Court held that the "scarcity of radio frequencies" in the "unique" media of broadcast services was sufficient to allow some governmental regulation of speech. After all, it was "the right of the viewers and listeners, not the right of the broadcasters, which [was] paramount."[105] Significantly, the *Red Lion* Court framed its analysis in terms of the scarcity inherent in the (then) "present state of commercially acceptable technology."[106]

The 1975 Report and Order provided the Supreme Court with an opportunity to revisit the scarcity doctrine in *FCC v. National Citizens Committee for Broadcasting.*[107] Once again, the Court rejected a First Amendment challenge to the Commission's regulations, finding that "[i]n light of this physical scarcity, Government . . . regulation of broadcast frequencies [is] essential."[108] The Newspaper Rule stood because of the Court's deferential review.

At its heart, though, the scarcity doctrine of *Red Lion* and its progeny depends on finding some measure of scarcity in the broadcast media, and courts invoking *Red Lion* often cite the Commission's pronouncements on the crowding of radio and television spectra.[109] But such determinations are factual, not legal, in nature, and they address the continuing applicability of the scarcity doctrine, not its continued validity as a legal theory. Viewing *Red Lion* in this light could enable a court to account for technological advances without upsetting its status as legal precedent.[110] Such an approach is attractive because it would preserve the scarcity doctrine for future courts without shackling the industry to outdated facts.

The broadcast media are far different today than they were in June 2004. In March 2007, the Commission announced the long-awaited approval of rules governing HD Radio. The in-channel on-band (IBOC) technology that drives HD Radio allows FM broadcasters to slice their allotted spectrum into multiple audio and data streams. Even though IBOC has not changed the amount of bandwidth available for broadcasters, it has trebled the number of FM outlets available in a given market through a more efficient use of available spectra. Broadcasters, in turn, are permitted to lease excess capacity to third parties, thereby increasing the diversity of voices and viewpoints within a given market.

A similar transformation is occurring in the television industry. Analog television broadcasts are scheduled to cease on February 17, 2009, and every broadcast station will have the capacity to deliver combinations of high-definition programming or multiple streams of programming on its allotted channels. Already, some broadcasters are taking advantage of this newfound capacity to offer different streams of programming. For example, a local public television station in Washington, D.C., WETA-TV, currently broadcasts five unique digital streams on Channel 26.

New and emerging technologies do not merely allow for a more efficient slicing of the spectral pie. Technology can expand the pie as well. For example, noted an article in *Nature* magazine, researchers at the University of Utah recently announced that they have created a filter that may enable the currently unusable terahertz region of the spectrum to be used for wireless communications.[111] When terahertz communications technology emerges, certain types of wireless communications services could be shifted from congested regions of the spectrum, allowing for the expansion of broadcast bands.

The Third Circuit did not address HD Radio multicasting or terahertz technologies in *Prometheus.* But how could it have? The Commission did not authorize HD Radio multicasting until March 8, 2005, nearly a year after the Third Circuit decided *Prometheus,* and *Nature* published the terahertz article in March 2007. *Prometheus* therefore stands as an example of how an otherwise valid legal construct can be undermined by the use of old facts.

Conclusion

Simply put, newspaper-broadcast cross-ownership regulation is an anachronism. Today's media bear little resemblance to those of 1975; and to the extent that diversity has increased since 1975, the Commission's "hoped for gain in diversity" has been realized because of advancing technologies, not because of the Newspaper Rule. With the benefit of hindsight, it has become apparent that the speculative fears voiced by the Commission in 1975 were misplaced. Had the commissioners known of the

looming information age, perhaps they would have been less inclined to focus on the potential for commonly owned newspaper and broadcast outlets to diminish diversity of viewpoints and would have accorded more weight to existing studies that made clear even then how such combinations benefited localism.

Although the Commission has remained mired in a regulatory morass, the technological developments impacting the media industry have been far from stuck. The Commission is statutorily obligated to make sure that its ownership rules reflect the situation "as it is, not as it was."[112] The belief that these structural ownership rules are necessary to preserve a diversity of voices ignores the overwhelming evidence that the marketplace of ideas has never been more robust, and the need for regulatory relief never more immediate.

The means through which to ensure a vibrant media marketplace—one where consumers continue to have access to the valuable services and quality journalism provided by newspapers and free, over-the-air broadcast stations—is to level the playing field through regulatory relief. Over-the-air television broadcasters and daily newspapers are facing unprecedented competitive and financial challenges. Without relaxation of the local ownership restrictions, it will be increasingly difficult for broadcasters and newspapers to fund the local news operations that have long been their hallmark and that so clearly serve the public interest.

Endnotes

1. *See 1975*, WIKIPEDIA, http://en.wikipedia.org/wiki/1975 (last visited Apr. 5, 2007).

2. *See* www.poynter.org/content/content_view.asp?id = 99440 (last visited Apr. 5, 2007).

3. *See Top 40*, WIKIPEDIA, http://en.wikipedia.org/wiki/Top_40_(radio_format) (last visited Apr. 5, 2007).

4. *See* www.museum.tv/archives/etv/U/htmlU/unitedstatesc/unitedstatesc.htm (last visited Apr. 5, 2007).

5. *See* www.cedmagic.com/history/betamax-lv-1901.html (last visited Apr. 5, 2007).

6. John Eggerton, *Who Cares About Ownership Rules?,* BROADCASTING & CABLE 3 (Mar. 12, 2007).

7. Prometheus Radio Project v. FCC, 373 F.3d 372, 398 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005).

8. Despite the prohibition, numerous same-market newspaper-broadcast combinations exist today. When it adopted the rule in 1975, the Commission grandfathered combinations in many markets (as long as the ownership of the combination remained the same). In other instances, the FCC has granted permanent or temporary waivers of the newspaper-broadcast cross-ownership rule. Finally, certain newspaper-broadcast combinations exist under a policy that permits a broadcast station owner to acquire a newspaper in the same market and operate it until the end of the station's license renewal term, or for one year, whichever period is longer. 1975 Multiple Ownership Report, 50 FCC 2d at 1076 n.25 [hereinafter Footnote 25 policy].

9. *Id.;* 2002 Biennial Regulatory Review—Review of the Commission's Broadcast Ownership Rules & Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, Report & Order & Notice of Proposed Rulemaking, 18 FCC Rcd 13,620, 13,747, ¶ 327 (2003) [hereinafter 2003 Report and Order].

10. Amendment of Sections 73.34, 73.240 & 73.636 of the Commission's Rules Relating to Multiple Ownership of Standard, FM, & Television Broadcast Stations, Second Report & Order, 50 FCC 2d 1046, 1075, ¶ 102 (1975) [hereinafter 1975 Multiple Ownership Report].

11. *Id.* at 1075, ¶ 101.

12. *Id.* at 1046, 1074, 1078–81.

13. *Id.* at 1078, ¶ 109.

14. The FCC's rules required that absent a waiver, the grandfathered newspaper-broadcast combinations held by ABC in Fort Worth and Detroit be split upon the merger with Disney. Disney requested a permanent waiver of the newspaper-broadcast rule, but the FCC found that the newspaper-radio combinations had not been justified under existing criteria for such waivers and that this restricted, adjudicatory proceeding was not the appropriate forum in which to amend its waiver policies. Accordingly, the FCC granted Disney temporary twelve-month waivers of the newspaper-broadcast rule in Detroit and Fort Worth. Application of Capital Cities/ABC, Inc., Memorandum Op. & Order, 11 FCC Rcd 5841, 5888 (1996).

15. *Id.*

16. *Id.* at 5906 (separate statement of Chairman Hundt). *See also id.* at 5915–16 (separate statement of Commissioner Barrett) ("The fact that this rule is over twenty (20) years old provides an even more compelling justification for the Commission's initiation of a rulemaking proceeding to determine the future applicability of this rule.").

17. *See* Newspaper/Radio Cross-Ownership Waiver Policy Notice of Inquiry, 11 FCC Rcd 13,003.

18. 1998 Biennial Regulatory Review, Notice of Inquiry, 13 FCC Rcd 11,276 (1998).

19. Telecommunications Act of 1996, Pub. L. No. 104-104, § 202(h), 110 Stat. 56, 111–12 (1996).

20. 1998 Biennial Review, 13 FCC Rcd at 11,280, ¶ 10.

21. 1998 Biennial Regulatory Review, Biennial Review Report, 15 FCC Rcd 11,058 (2000), *vacated on other grounds by* Fox Television Stations, Inc. v. FCC, 280 F.3d 1027, 1048, *reh'g granted in part*, 293 F.3d 537 (D.C. Cir. 2002).

22. *Id.* at 11,102, ¶ 83.

23. Cross-Ownership of Broadcast Stations & Newspapers, Order & Notice of Proposed Rulemaking, 16 FCC Rcd 17,283 (2001). In the interim, the FCC had concluded, in the space of just seven months, its 2000 Biennial Regulatory Review. The Commission's 2000 Biennial Regulatory Review, Report, 16 FCC Rcd 1207 (2001), however, was devoted largely to a recitation of the conclusions reached in the 1998 Biennial Review and a concurrent proceeding on television ownership matters and did not alter the conclusions reached in those proceedings. *See id.* at 1217, 1225–26.

24. 2003 Report and Order, *supra* note 9, at 14,013 (app. A) (listing commentators in response to 2001 Newspaper/Broadcast Cross-Ownership NPRM).

25. 2002 Biennial Regulatory Review, Notice of Proposed Rulemaking, 17 FCC Rcd 18,503 (2002).

26. *Fox Television Stations*, 280 F.3d at 1048 (remanding the FCC's national television station ownership rule and vacating its television-cable cross-ownership restriction); Sinclair Broad. Group, Inc. v. FCC, 284 F.3d 148, 159 (D.C. Cir. 2002) (remanding the local television ownership rule to the Commission for further consideration).

27. News Release, Fed. Communications Comm'n, FCC Sets Limits on Media Concentration; Unprecedented Public Record Results in Enforceable and Balanced Broadcast Ownership Rules, MB Docket Nos. 02-277, 01-235, 01-317, 00-244, 2003 FCC LEXIS 3121, at *1 (2003) (FCC decision "represents the most comprehensive review of media ownership regulation in the agency's history").

28. Prometheus Radio Project v. FCC, 373 F.3d 372, 386 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005).

29. *See, e.g.,* Thomas C. Spavins, Loretta

Denison, Scott Roberts, & Jane Frenette, *The Measurement of Local Television News and Public Affairs Programs*, MB Docket No. 02-277 (Sept. 2002), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-226838A12.pdf (last visited Apr. 5, 2007) [hereinafter MOWG Spavins Study]; David Pritchard, *Viewpoint Diversity in Cross-Owned Newspapers and Television Stations: A Study of News Coverage of the 2000 Presidential Election Campaign*, MB Docket No. 02-277 (Sept. 2002), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-226838A7.pdf.

30. 2003 Report and Order, *supra* note 9, at 13,747, ¶ 327.

31. *Id.* at 13,748, ¶ 330.

32. 47 C.F.R. § 73.3555(c).

33. *Prometheus*, 373 F.3d at 394.

34. *Id.* at 399–400. The court's criticism focused on flaws in the Diversity Index (DI) used by the agency as support for the Cross-Media Limits (CMLs). The DI, which was loosely based on the Herfindahl-Hirschmann Index (HHI) used by the Department of Justice and Federal Trade Commission to measure competition, attempted to assess the diversity of viewpoints offered by local news and informational outlets. The FCC applied the DI to a range of sample markets in order to assess current levels of diversity and determine what types of combinations would pose an unacceptable diversity risk. The court stated that the FCC had not identified any consideration other than the DI as having influenced the formulation of the CMLs. Although the court noted that it did not object "in principle" to the FCC's use of the DI "as a starting point" for assessing local diversity, it found that the DI employed "several irrational assumptions and inconsistencies." Specifically, in the court's opinion, the FCC gave too much weight to the Internet as a media outlet, irrationally assigned outlets of the same media type equal market shares, and inconsistently derived the CMLs from the DI results.

35. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 202(h), 110 Stat. 56, 111–12 (1996); Consolidated Appropriations Act, 2004, Pub. L. No. 108-199, § 629, 118 Stat. 3, 99–100 (2004) (amending Sections 202(c) and 202(h) of the Telecommunications Act of 1996).

36. *See* www.fcc.gov/ownership/hearings.html.

37. John Eggerton, *Martin Promises Localism Study Before Ownership Moves,* BROADCASTING & CABLE, Jan. 8, 2007.

38. *See* www.fcc.gov/ownership/studies.html.

39. 2003 Report and Order, *supra* note 9, at 13,748, ¶ 330.

40. For example, a search for the phrase *technological revolution* in the Google news archive yielded 2,420 stories published between the release of *Prometheus* (June 24, 2004) and December 31, 2006. http://news.google.com/archivesearch?q=%22technological+revolution%22&num=20&as_ldate=06/24/2004&as_hdate=12/31/2006&lr=lang_en&sa=N&lnav=m (last visited Apr. 5, 2007).

41. 2003 Report and Order, *supra* note 9, at 13,623, ¶ 3.

42. *Id.*

43. Prometheus Radio Project v. FCC, 373 F.3d 372, 415 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005).

44. *See generally* Howard Kurtz, *Tightened Belts Could Put Press in a Pinch,* WASH. POST, Oct. 23, 2006, at C1.

45. See Pew Internet & Am. Life Project, *Online News: For Many Broadband Users, the Internet Is a Primary News Source* (Mar. 22, 2006), *available at* www.pewinternet.org/pdfs/PIP_News.and.Broadband.pdf.

46. 2003 Report and Order, *supra* note 9, at 13,665–67.

47. *See* Pew Internet & Am. Life Project, TEENS AND TECHNOLOGY 1, 4 (July 27, 2005), *available at* www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf; *see also* Pew Internet & Am. Life Project, *Generations Online 3* (Dec. 2005), *available at* www.pewinternet.org/pdfs/PIP_Generations_Memo.pdf.

48. *Jorn Barger*, WIKIPEDIA, http://en.wikipedia.org/wiki/Jorn_Barger (last visited Apr. 5, 2007).

49. *See Blog*, WIKIPEDIA, http://en.wikipedia.org/wiki/Blog (last visited Apr. 5, 2007).

50. Prometheus Radio Project v. FCC, 373 F.3d 372, 469 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005) (Scirica, J., dissenting in part, concurring in part).

51. www.pewinternet.org/trends/Usage OverTime.xls (last visited Apr. 5, 2007).

52. Reply Comments of AFL-CIO, MB Docket Nos. 06-121, et al. 14 (Jan. 16, 2007).

53. Andy Sullivan, *Bloggers Gain Access to "Scooter" Libby Trial*, REUTERS, Jan. 12, 2007, http://in.today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2007-01-12T090216Z_01_NOOTR_RTRJONC_0_India-283211-2.xml&archived=False; Liz Halloran, *Media Takes: A Dogged Blogger at the Libby Trial,* U.S. NEWS & WORLD REP., Feb. 13, 2007, *available at* www.usnews.com/usnews/news/articles/070213/13libby.htm; Joe Garofoli, *Analysts Say Information Now Could Be Harder to Get,* S.F. CHRON., Mar. 7, 2007, at A10.

54. *Meet Your New Representative, D.C.* (updated), DCIST, www.dcist.com/archives/2007/03/23/meet_your_new_r.php (last visited Apr. 5, 2007).

55. *See* http://flickr.com/search/?q=news&m=tags (last visited Apr. 5, 2007).

56. *See* http://youtube.com/categories_portal?c=25&e=1 (last visited Apr. 5, 2007).

57. Lev Grossman, *Time Person of the Year: You,* TIME, Dec. 25, 2006, at 40.

58. 1975 Multiple Ownership Report, *supra* note 10, at 1078, ¶ 109.

59. *Id.* at 1078, ¶ 108.

60. This policy permits a broadcaster acquiring a local daily newspaper to own both properties until the station's next renewal, or for one year, whichever period is longer. *Id.* at 1076 n.25 (statement of Commissioner Robinson, concurring in part, dissenting in part).

61. *See, e.g.,* Comments of Media General, MB Docket Nos. 06-121, et al. 23–29 (Oct. 23, 2006) [hereinafter Media General Comments].

62. 1975 Multiple Ownership Report, *supra* note 10, at 1074, ¶ 99.

63. *See, e.g.* MOWG Spavins Study, *supra* note 29, at 1; Statement of Professor Jerry A. Hausman, Comments of Clear Channel Communications, Inc., MB Docket Nos. 06-121, et al., exhibit 2 (Oct. 23, 2006).

64. The Commission looks at two factors when judging localism: "the selection of programming responsive to local needs and interests, and local news quantity and quality." 2003 Report and Order, *supra* note 9, at 13,644, ¶ 78.

65. 1975 Multiple Ownership Report, *supra* note 10, at app. C.

66. *Id.*

67. Media General Comments, *supra* note 61, at 23–29.

68. Prometheus Radio Project v. FCC, 373 F.3d 372, 399 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005).

69. *See, e.g.*, 2003 Report and Order, *supra* note 9, at 13,644–45, ¶¶ 77–78.

70. Comments of Newspaper Ass'n of Am., MB Docket Nos. 06-121 et al. 67–68 (Oct. 23, 2006) [hereinafter NAA Comments].

71. *See, e.g.*, WFLS, www.wfls.com/news (last visited Apr. 1, 2007).

72. NAA Comments, *supra* note 70, at 68–69.

73. *Id.*

74. *Id.* at 69.

75. *See* Media General Comments, *supra* note 61, at 7–22; *see also id.* app. 4.

76. *See id.* app. 4A at 2–3. Professor Powell

is the director of the Integrated Media Systems Center, the National Science Foundation's Engineering Research Center for Multimedia Research at the University of Southern California Viterbi School of Engineering.

77. *See id.* at 9, app. 4A at 2; *see also id.* app. 4A, exhibits A–F.

78. *See id.* at 10.

79. *Id.*

80. *Id.*

81. Comments of Belo Corp., MB Docket Nos. 06-121, et al. 13 (Oct. 23, 2006) [hereinafter Belo Comments].

82. *Id.* at 13–15.

83. *See* Comments of Gannett Co., MB Docket Nos. 06-121 et al. 27 (Oct. 23, 2006) [hereinafter Gannett Comments].

84. *See id.* at 28.

85. Comments of Cox Enters., Inc., MB Docket Nos. 06-121 et al. 13–16 (Oct. 23, 2006) [hereinafter Cox Comments].

86. In March 2007, Tribune Company agreed to a sale to real estate magnate Sam Zell, who will pay $34 per share for some 126 million shares and take the multimedia company private. Because none of the FCC "rights" to hold these combinations conveys to a new owner, the sale undoubtedly will create a new front in the battle over cross-ownership and face significant hurdles before regulatory approval. For information on the Footnote 25 policy, see *supra* note 8.

87. *See, e.g.,* azcentral.com, ARIZONA'S HOME PAGE, www.azcentral.com/ (last visited Apr. 5, 2007); coloradoan.com, BRINGING FORT COLLINS HOME, www.coloradoan.com/apps/pbcs.dll/frontpage (last visited Apr. 5, 2007); HONOLULU ADVERTISER ONLINE, www.honoluluadvertiser.com/apps/pbcs.dll/frontpage (last visited Apr. 5, 2007); STATESMAN J. ONLINE, www.statesmanjournal.com/apps/pbcs.dll/frontpage (last visited Apr. 5, 2007); newsleader.com, SERVING THE CTR. SHENENDOAH VALLEY, www.newsleader.com/apps/pbcs.dll/frontpage (last visited Apr.5, 2007); SPRINGFIELD NEWS-LEADER ONLINE, www.news-leader.com/apps/pbcs.dll/frontpage (last visited Apr. 5, 2007). For additional links to Gannett newspaper websites offering unique local content, community forums, user commentary, and other hyper-local features, see Gannett Newspapers on the Web, www.gannett.com/web/newspapers.htm (last visited Apr. 5, 2007).

88. *See* Comments of the Communications Workers of Am., et al., MB Docket Nos. 06-121, et al. 38–46 (Oct. 23, 2006); Comments of Consumers Union, et al., MB Docket Nos. 06-121 et al. 17 (Oct. 23, 2006).

89. *See* Belo Comments, *supra* note 81, at 18; Block Communications, Inc., Comments, MB Docket Nos. 06-121, et al. 2–4, 7–8 (Oct. 23, 2006); Cascade Broadcasting Group, L.L.C., Comments, MB Docket Nos. 06-121, et al. 1–4 (Oct. 23, 2006); CBS Comments, MB Docket Nos. 06-121, et al. 11 (Oct. 23, 2006); Cox Comments, *supra* note 85, at 10–12; Fox Comments, MB Docket Nos. 06-121, et al. 12–13 (Oct. 23, 2006) [hereinafter Fox Comments]; Freedom of Expression Comments, MB Docket Nos. 06-121, et al. 10, 22 (Oct. 23, 2006); Gannett Comments, *supra* note 83, at 21–25; Media General Comments, *supra* note 61, at 45, 63; Granite Broadcasting Corp. Comments, MB Docket Nos. 06-121, et al. 3–6 (Oct. 23, 2006); Gray Comments, MB Docket Nos. 06-121, et al. 10–15 (Oct. 23, 2006) [hereinafter Gray Comments]; Hoak Media LLC Comments, MB Docket Nos. 06-121, et al. 4–6 (Oct. 23, 2006); KMVD Licensee Co., LLC, Comments, MB Docket Nos. 06-121, et al. 6 (Oct. 23, 2006); Morris Comments, MB Docket Nos. 06-121, et al. 10–11 (Oct. 23, 2006) [hereinafter Morris Comments]; NAB Comments, MB Docket Nos. 06-121, et al. 23–34, 94–98 (Oct. 23, 2006) [hereinafter NAB Comments]; NBC Comments, MB Docket Nos. 06-121, et al. 7–12 (Oct. 23, 2006); Nexstar Comments, MB Docket Nos. 06-121, et al. 6–10 (Oct. 23, 2006); Shamrock Comments, MB Docket Nos. 06-121, et al. 6–7 (Oct. 23, 2006); Smaller Market Television Stations Comments, MB Docket Nos. 06-121, et al. 6–10 (Oct. 23, 2006); Tribune Comments, MB Docket Nos. 06-121 et al. 33–42, 46–52, 55–61, 64–69, 72–77 (Oct. 23, 2006) [hereinafter Tribune Comments].

90. *See* Fox Comments, *supra* note 89, at 5–6; Gray Comments, *supra* note 89, at 8–9; Hearst-Argyle Comments at 7–8**;** Morris Comments, *supra* note 89, at 12; NAB Comments, *supra* note 89, at 49–54; Progress and Freedom Foundation Comments at 36–40.

91. Rick Edmonds, Project for Excellence in Journalism & Poynter Inst., *Newspapers, in* THE STATE OF THE NEWS MEDIA: AN ANNUAL REPORT ON AMERICAN JOURNALISM (2007), *available at* www.stateofthenewsmedia.com/2007/printable_newspapers_chapter.asp?media=1&cat= 1.

92. Michelle Greppi, *Zell Buys Tribune, Plans to Sell Cubs,* TVWEEK.COM, Apr. 2, 2007, www.tvweek.com/news.cms?newsId =11813.

93. *Compare* N.Y. Times Co., 2002 Annual Report F-51 (2003) (reporting fourth-quarter 2002 share price of $50.11), *with* N.Y. Times Co., 2005 Annual Report F-61 (2006) (reporting fourth-quarter 2005 share price of $30.17).

94. Edmonds, *supra* note 91.

95. Tribune Comments, *supra* note 89, at 36–56 (citing Nielsen Station Indexes). In the three cities, the only television broadcast stations to experience share growth were the Spanish-language stations located in New York and Los Angeles, but the growth was insufficient to account for the other stations' decreased audience.

96. Prometheus Radio Project v. FCC, 373 F.3d 372, 415 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005).

97. NAA Comments, *supra* note 70, at 67.

98. *Id.* at 68.

99. Media General Comments, *supra* note 61, at 46.

100. *Id.* at 47.

101. *Id.*

102. Indeed, recent statements by Commissioner McDowell seem to suggest that he feels the benefits of existing newspaper-broadcast combinations "favor the status quo," pending the Commission's next attempt to modify or repeal the Newspaper Rule. *See* Corey Boles, *Tribune Sale Barriers Could Be Resolved, FCC Official Says,* MARKETWATCH, Apr. 5, 2007, www.marketwatch.com/news/story/tribune-sale-barriers-could-resolved/story.aspx?guid=%7B601530EE-393F-4C8B-B831-D900172E95A2%7D.

103. *Prometheus*, 373 F.3d at 401–02.

104. 395 U.S. 367 (1969).

105. *Id.* at 390.

106. *Id.* at 388.

107. 436 U.S. 775 (1978).

108. *Id.* at 799.

109. *See, e.g.,* Ruggiero v. FCC, 278 F.3d 1323, 1325 (D.C. Cir 2002) ("very little spectrum remains available for new full-powered stations"), *rev'd en banc*, 317 F.3d 239 (D.C. Cir. 2003).

110. *See* FCC v. League of Women Voters of Cal., 468 U.S. 364, 376 n.11 (1984) (reserving its right to reconsider the continued validity of the scarcity doctrine in light of future factual findings by the Commission).

111. Duncan Graham-Rowe, *Terahertz Filter Could Harness Unused Spectrum,* NEWSCIENTIST.COM, Mar. 29, 2007, www.newscientist.com/article/dn11492-terahertz-filter-could-harness-unused-spectrum-.html.

112. Prometheus Radio Project v. FCC, 373 F.3d 372, 391 (3d Cir. 2004), *cert. denied*, 545 U.S. 1123 (2005); *see also* Gannett Comments, *supra* note 83, at 14–15.

Tough New FCC Rules on Customer Call Records

ROSALIND K. ALLEN

Living in the information age continues to broaden our perspective of how we view ourselves and our place in the world. Telecommunications and information technologies promote data centralization and fluidity, helping us achieve increasing levels of efficiency and productivity. But these dynamic technologies also make data more vulnerable, creating increased opportunities for unauthorized access, use, disclosure, and alteration, as well as accidental loss and deletion. Of particular concern is the apparent ease with which personally identifiable information is collected and shared, often without the subject's knowledge or permission. Federal and state governments have responded with a flurry of data protection and privacy laws. Enabling people to exercise greater control over collection and use of their personally identifiable information is now a well-established consumer priority.

Recent high-profile incidents have focused attention on whether our laws afford adequate and effective protection for personal call records. When private investigators hired by Hewlett-Packard (HP) officials were easily able to identify the source of information leaks by obtaining call records of targeted reporters, privacy of personal call records became a national issue. The HP investigators gained unauthorized access to the personal call records through a practice known as pretexting. Pretexting is the practice of gaining access to an individual's sensitive personal information under false pretenses. For example, the HP investigators impersonated the reporters when they contacted telecommunications companies to get the call records.

The online environment has given rise to an industry of data brokers selling records of phone calls with dates, times, durations, and locations. To draw further attention to the unauthorized marketing of personal information, a blogger randomly contacted an online data broker and purchased General Wesley Clark's mobile phone records for 100 calls made during a three-day period in November 2005.

The legislative response to these revelations was quick and decisive. Congress enacted and the president signed into law the Telephone Records and Privacy Protection Act (TRPPA) of 2006, which criminalizes the practice of fraudulently obtaining another person's phone records, either directly or through the purchase of such information. Approximately twenty-four states have enacted or are proposing to enact antipretexting laws. A number of telecommunications providers have filed suits against numerous entities for fraudulently obtaining phone records.[1] The Federal Trade Commission (FTC) has also prosecuted pretexting to obtain consumer phone records as a deceptive and unfair trade practice under Section 5 of the FTC Act.[2]

In the wake of all these crackdowns on the pretexters, the Federal Communications Commission (FCC or Commission) decided more needed to be done. Section 222 of the Communications Act imposes obligations on telecommunications carriers to protect and control the use of the proprietary information (otherwise known as customer proprietary network information, or CPNI) derived from customers. The FCC already had CPNI rules in place but recently took steps to bolster them. Prompted by the high visibility of the phone record pretexting problem, as well as by a petition filed by the Electronic Privacy Information Center (EPIC) seeking stronger security and authentication standards for accessing CPNI, the Commission initiated a rulemaking proceeding that proposes additional safeguards to protect CPNI from unauthorized access and disclosure.

The FCC issued its revised CPNI rules on April 2, 2007.[3] The new CPNI rules take effect within six months of approval by the Office of Management and Budget. Compliance will require significant changes in the ways telecom providers protect and disclose customer data, as well as how the providers interact with their marketing contractors and joint venture partners. The FCC also broadened the universe of providers subject to Section 222 to include interconnected providers of Voice over Internet Protocol,[4] which will no doubt trigger renewed complaints that legacy regulations are burdening this competitive new market sector. Strict enforcement of the new rules is expected. Because some of the new regulations are overly broad and vague and do not appear to be narrowly tailored solutions that meet identified governmental interests, the new CPNI regime is likely to be challenged.

Call Detail Records

The FCC's new rules are premised on the belief that inadequate protection of CPNI by carriers has directly contributed to pretexting. Accordingly, as a starting point in its analysis, the FCC recognizes a new subset of CPNI, i.e., call detail records (CDR), which comprise the most sensitive types of CPNI. Specifically, CDR

> includes any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.[5]

By way of example, the FCC notes that remaining minutes of monthly use for a wireless customer qualify as CPNI but do not fall within the sensitive CDR category.

Safeguarding Access

Providers are prohibited from disclosing CDR unless specific authentication requirements are followed. First, the provider must establish a password for each customer account by authenticating

Roz Allen (rosalind.allen@hklaw.com) is a partner, specializing in communications and privacy law, in the Washington, D.C., office of Holland & Knight LLP.

the customer without using "readily available biographical information," such as the last four digits of a customer's Social Security number, mother's maiden name, or date of birth. Accepted methods of authentication include

(1) calling the customer at the telephone number of record for the service purchased. This means that if the customer is purchasing wireless service, the provider must call the customer at the wireless phone number associated with that service, not a home or work number; or
(2) sending the customer a personal identification number (PIN) by voice mail or text message to the telephone number of record, or by mailing the PIN to the address of record for the account. This could be an e-mail address.

If the provider receives a phone call from an individual seeking CDR, the provider cannot disclose the CDR unless the caller shares the preestablished password or PIN with the provider. This requirement is unnecessary if the caller volunteers all of the CDR needed to address a customer service issue during the call. Nonetheless, the provider must limit the discussion of CDR only to that volunteered by the caller and must not disclose any additional CDR without first obtaining a password.

Providers must also require passwords for customers seeking to access CDR through an online customer account. Furthermore, customers have the option of accessing all their CPNI (including CDR) by visiting a provider's retail location and presenting a valid government-issued photo ID that matches the account information.

It is inevitable that customers will forget passwords; therefore, the provider must create a backup method of authentication for use under these circumstances. Although the FCC is not specific about the correct backup method, this secondary form of authentication also cannot involve readily available biographical information or account information. Use of a "shared secret question" (e.g., "What is your favorite color?") chosen by the provider or the customer is suggested as an acceptable form of backup authentication.

Business Customers

It is not uncommon to give business customers the leverage to make sure they get the full range of their telecommunications services needs met. For that reason, if a business customer is assigned a dedicated account representative by the provider and the negotiated service agreement specifically addresses protection of the business's CPNI, the authentication requirements need not be followed. The business customer may, of course, negotiate more stringent authentication procedures that integrate well into the business's enterprisewide information management procedures. This exemption is only limited to the new authentication rules and does not relieve the provider from compliance with all other CPNI requirements.

Notification of Account Changes

Providers must notify customers immediately of significant account changes, such as password changes, online account changes, mailing address changes, or changes to the backup authentication method. This requirement will likely prove to be of significant practical value as an early warning system to consumers because these types of changes are often associated with identity theft. Notification to the customer may be via a voice mail or text message to the telephone number of record, or written notification to the address of record.[6]

Breach Notification

For purposes of CPNI, a breach is viewed as any intentional and unauthorized act of access, use, or disclosure. Timely breach notification is widely viewed as the most important and effective response to a compromise of personally identifiable information because it enables the consumer to minimize resulting damage. Breach notification has also come to define the reasonable standard of care for entities storing personally identifiable information. Approximately thirty-five states have enacted some form of a data breach notification law, and Congress is considering a federal privacy law that would include data breach notification.[7] Making breach notification a legal requirement protects consumers and makes clear that if consumers are not notified of actual (or, under some state laws, potential) data breaches, then those consumers have been injured. Moreover, if an entity storing personally identifiable information promptly reports the breach to affected consumers, data breach laws provide a measure of protection from further allegations of consumer harm. The new FCC rules, however, appear to frame breach notification primarily as a law enforcement tool rather than a means of avoiding customer harm.

Providers are prohibited from disclosing CDR unless specific authentication requirements are followed.

Once a provider establishes that a security breach of CPNI has occurred, both the U.S. Secret Service and the FBI must be notified of the breach within seven business days using an online site developed by the FCC. The customer may be notified of the breach only after seven business days following notification to the federal law enforcement agencies, unless one of the law enforcement agencies decides that customer notification would impede or compromise an ongoing or potential criminal investigation or national security matter. In that event, law enforcement agencies may direct the provider not to notify the customer for an additional period of up to thirty days, subject to extension if the federal law enforcement agency believes it is reasonably necessary. If the provider believes that there is "an extraordinary and urgent need to notify" in order to avoid an immediate harm, then the provider may notify the customer but must also inform the federal law enforcement agencies that notification has occurred.[8] The same approach must be followed whether there is a single incident compromising CPNI or a group of such incidents.

Although two of the FCC commissioners disagreed with the provision that federal law enforcement should be given the discretion to prevent, without explanation, a customer from learning that sensitive, personally identifiable information has been compromised, the new rules do not appear to provide for the FCC or any other third party to independently verify the need to withhold

consumer notification. This aspect of the decision can be directly attributed to a recommendation submitted into the record by the Department of Justice, and it is far from clear whether the implications of notification delay were fully considered.

The FCC also expressly preempts state law requirements that are inconsistent with the new rules.

The FCC does not define the federal law enforcement interest that would justify failure to notify a customer that unauthorized entities are accessing sensitive personal information and potentially allowing continuation of a dangerous activity without the customer's knowledge. Unauthorized access to call records has been associated with stalking and other threatening behavior. Under those circumstances, it is likely the customer is aware of the problem and has contacted the police. If not, warning a customer of an immediate threat to his or her safety would appear to justify the provider's immediate and extraordinary need to notify.

The FCC also expressly preempts state law requirements that are inconsistent with the new rules. This aspect of the FCC's rulemaking order is likely to become a substantial source of confusion and potential litigation. For example, apart from state antipretexting laws, some types of CPNI breaches would also be reportable under state data breach laws. Would the FCC rules preempt state law provisions that require notification of state law enforcement authorities? If federal law enforcement decided to prohibit or delay breach disclosure, would the provider be deemed in violation of state data breach laws that establish deadlines for breach notification? Risk-management considerations will likely cause providers to devote further resources to monitoring state law and establishing reliable procedures for tracking the specifics of each breach. The most efficient and effective way to modify risk management considerations would likely involve adjustments to current procedures for ensuring the security and integrity of the entity's information inventory.

Joint Venture and Third-Party Contractors

The FCC generated controversy with its decision to require an opt-in from customers before providers can share CPNI with joint venture partners or independent contractors for marketing purposes. Current rules allow such sharing unless the customer opts out of CPNI sharing within thirty days of provider notification. The opt-out process can continue to be used for sharing CPNI with provider agents and affiliates to market telecommunications-related services.

Obtaining customer opt-in is extremely difficult, and unless this aspect of the decision is modified or stayed, many providers may decide to reformulate their arrangements with third-party marketing entities into agency agreements. There is reason to believe, however, that the constitutionality of this rule will be challenged.

In *US West, Inc. v. FCC*,[9] the Tenth Circuit held that an opt-in requirement for disclosure of CPNI to joint venture partners and independent contractors violated the First Amendment because the FCC failed to satisfy the *Central Hudson*[10] test for permissible restrictions on commercial speech. *Central Hudson* provides that if commercial speech concerns lawful activity and is not deceptive or misleading, the government may impose restrictions only if

(1) It has a "substantial" state interest in regulating the speech,
(2) The regulation directly and materially advances that interest, and
(3) The regulation is "not more extensive than necessary to serve that interest."[11]

The Tenth Circuit expressed skepticism about the first and second prongs but concluded that even assuming those were satisfied, the opt-in rule was not narrowly tailored and the FCC had failed to show why notification followed by an opportunity to opt out would not be equally effective.

In resurrecting the opt-in proposal in the new CPNI order, the FCC argued that the record of this most recent proceeding differs substantially from prior proceedings and now supports opt-in. That argument might be supportable if the FCC decided to adopt an opt-in rule for CDR only rather than for all CPNI. The record of this proceeding does show that unauthorized disclosure of CDR violates personal privacy and may also facilitate domestic violence or stalking and endanger law enforcement officers, victims of crimes, witnesses, or confidential informants. The governmental interest in preventing unauthorized disclosure of CDR is therefore substantial, and the recent passage of TRPPA further supports that argument.

The Commission's decision, however, to extend opt-in to CPNI that is not CDR is difficult to support. First, as the Commission admits, the record of this new proceeding does not show that sharing of CPNI for marketing purposes with joint venture partners and third-party contractors leads to misappropriation of personal call records. There are no known instances of CPNI being compromised through these types of marketing activities. In fact, the record has little to say about this aspect of CPNI because the stated focus of this proceeding is safeguarding CDR. It appears that the FCC decided to extend opt-in to all CPNI based on an assumption that once CPNI is transferred to joint venture partners and third-party contractors, the provider loses control over the information. Taken as a whole, the record no more supports applying opt-in to CPNI that is not CDR than it did ten years ago.

Whether an opt-in is more extensive than necessary remains somewhat debatable. There is support in the record for measures stronger than the current opt-out but more narrowly tailored than the opt-in, such as use of a password for transferring CPNI to third-party contractors and joint venture partners.

Annual Certification

The FCC emphasizes that all carriers must take "every reasonable precaution" to prevent unauthorized disclosure of CPNI. Carriers are affirmatively on notice that they have not taken sufficient steps to adequately protect CPNI if even a single pretexter obtains unauthorized access to a customer's CPNI. The FCC declined to adopt specific safeguards at this time but indicated that

carriers must do more than comply with the requirements set forth in the new rules. Furthermore, the FCC explicitly rejected adopting a regime equivalent to the Gramm-Leach-Bliley safeguards rule for protection of personal financial information, based on the misperception that this would either insulate the provider from liability or provide pretexters with instructions for circumventing the safeguards. Nonetheless, carriers will be faulted if they do not adopt whatever additional safeguards are "feasible" to detect and prevent pretexting. The further notice for proposed rulemaking accompanying this order does give the FCC an opportunity to comprehensively explore the track record of a safeguards approach in other areas of privacy enforcement.

Carriers are now required to file an annual CPNI certification every March, reporting information for the preceding year. New information for the certification must include

(1) a summary of all customer complaints concerning unauthorized use of CPNI;
(2) a report of each breach, including dates of discovery and notification;
(3) any enforcement measures undertaken against data brokers;
(4) pretexting techniques observed; and
(5) measures taken to protect CPNI.

The enforcement scheme is unusual. Providers are required to detect and report pretexting with the knowledge that the disclosure will always trigger enforcement action.

Conclusion

An analysis of the FCC's new rules for protecting consumer call records strongly suggests that the regulatory scheme will continue to evolve. Apart from the fact that the FCC initiated a further notice of proposed rulemaking that is likely to better define carrier compliance requirements, it is entirely possible that the new rules will be challenged. If federal legislative developments come to fruition, it is also conceivable that the FCC will be required to reexamine its approach to ensure that treatment of CPNI is consistent with overall federal protections accorded personally identifiable information. An important takeaway is that the federal and state focus on protecting personally identifiable information will only expand over time. Many companies have recognized this trend and are undertaking the task of developing an enterprisewide, holistic approach to all information collected, used, and stored during the ordinary course of business. With each new legal development in the area of consumer privacy, adopting clear processes for information handling must be given priority.

Endnotes

1. *See, e.g.,* Cingular Wireless LLC v. Data Find Solutions, Inc., No. 1:05-CV-3269-CC (N.D. Ga. filed Dec. 23, 2005); Sprint Nextel Corp. v. All Star Investigations, Inc., No. 06 01736 (Fla. Cir. Ct. filed Jan. 27, 2006); T-Mobile USA, Inc. v. C.F. Anderson, No. 06-2-04163 (King County Super. Ct. Feb. 2, 2006) (stipulated order and permanent injunction); Cellco P'ship Verizon Wireless v. Data Find Solutions, Inc., No. 06-CV-326 (SRC) (D.N.J. Jan. 31, 2006) (order).

2. *See, e.g.,* Fed. Trade Comm'n v. Info. Search, Inc., No. 1:06-CV-01099-AMD, FTC File No. 062 3102 (N.D. Md. settlement entered Feb. 22, 2007); s*ee also Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act: Hearing Before the H. Comm. on Energy and Commerce,* 109th, 1st Sess. (Mar. 9, 2007) (statement of Lydia Parnes, Director, Consumer Protection, Federal Trade Comm'n).

3. In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information (report and order and further notice of proposed rulemaking), FCC 07–22 (released Apr. 2, 2007). The FCC also adopted a further notice of proposed rulemaking that seeks comment on whether: (1) password requirements should be expanded further; (2) audit trails for CPNI should be established; (3) physical safeguards for transfers of CPNI are necessary; (4) time limits should be imposed on retention of CPNI; and (5) information stored on mobile devices should be subject to controls. Comments were due on July 9, 2007, and reply comments on August 7, 2007. This article will focus solely on the rules actually adopted.

4. An interconnected VoIP service (1) enables real-time, two-way voice communications, (2) requires a broadband connection from the user's location, (3) requires Internet protocol-compatible customer premises equipment, and (4) permits users generally to receive calls that originate on the public switched telephone network (PSTN) and to terminate calls to the PSTN. 47 C.F.R. § 9.3.

5. 47 C.F.R. § 64.2003(d).

6. Such provider notification must be limited to the fact that a change was made and cannot reveal the specifics of that change.

7. On May 3, 2007, several federal privacy laws, including data breach notification provisions, received committee approval in the U.S. Senate: Personal Data Privacy and Security Act of 2007, S. 495 (co-sponsored by Senators Patrick Leahy and Arlen Specter) and Notification of Risk to Personal Data Act of 2007, S. 238, S. 239 (sponsored by Senator Dianne Feinstein).

8. Presumably, if the provider finds out about the breach from the customer, the notification to law enforcement would also explain that the customer knows about the breach.

9. 182 F.3d 1224 (10th Cir. 1999).

10. 447 U.S. 557, 564–65 (1980).

11. *Id.*

Effective Techniques for Trying Media Cases: Choosing Your Jury Panel

Editor's Note:
This is the debut article in a new practical tips series that will offer insights and concrete suggestions from seasoned trial lawyers on each phase of the trial, from jury selection to closing arguments. In this first installment, we've called on five attorneys to share their own experiences and advice on selecting a jury in a media case.

Make It Relevant and Solicit Juror Comments

THOMAS S. LEATHERBURY

Two tips: make your case real and accessible and encourage the jurors to speak in voir dire.

First, pick something about your case that the potential jurors can relate to their own experience and talk about it in voir dire. In a very complex patent dispute about lighting controls, my partner likened the way our clients' lighting controls were networked with the way computers in an office are networked. He simplified the concept and made it more accessible to the members of the panel.

In the most recent libel case we tried, one of our themes was that the broadcast at issue told a story that the public had a right and a need to know. In that case, we asked the potential jurors if they ever learned something from the news about their local school district or their city government that they felt they had a right to know. We knew about several recent local controversies from subscribing to the local paper in the year leading up to the trial.

Second, get everyone who could be on the jury to say something in voir dire. Pick work, family, activities, or another subject that should not be controversial, and get the potential jurors talking individually as much as time permits. The specific traits you may be looking for will vary from case to case. In many cases, voir dire time is so severely truncated that you may have to be satisfied with your impressions of how outspoken or outgoing the jurors are, how they seem to react to you and your clients, and the small amount of information they share; but at least you will have heard them speak and seen them react in a one-on-one exchange.

Thomas S. Leatherbury (tleatherbury@velaw.com) is a partner in the Dallas office of Vinson & Elkins, LLP.

Make the Best of What You're Given

ROBERT C. BERNIUS

Jury selection is based on skill, judgment, experience, intuition, and luck. Good questioning won't get you an ideal jury but can get you a jury that will give you a fair chance of winning—or at least a jury that is not openly hostile to you. However, there is no litany of questions for a media case on which you can rely. Your questions can't be generic; they are part of your trial story, they establish the themes to which you will return in summation, and they allow you to gauge each juror's reactions to those themes. How do you do it? Here are a couple of basic suggestions.

First impressions count. If the jury thinks you are a decent person who knows what he's doing, they'll try to give you the benefit of the doubt. Introduce yourself and your client even though ten lawyers ahead of you have done so, but don't be folksy ("Hi, I'm Freddy Forbush, and this is my client, Corky Jones."). You're in a courtroom, not at a picnic. Even if your case isn't much and you are sorry you ever got into it, act with confidence. You're trying to sell something. If possible, get the jury to smile with you. You're not there to put on a song-and-dance act, but a little humor helps. Vary the wording of your questions; if you repeat the same ones over and over, you will get rote answers. Try to say something to each juror individually, and use her name when you do it. But don't ignore what is going on in the jury box while you try to memorize names; and if you can't use names naturally, forget it—jurors know when you are patronizing them.

You aren't apt to find many leading lights of the community in the box; the sad fact is that people who should be on juries aren't. You aren't going to get jurors to go along with you if they don't know what you are talking about, so don't use lawspeak; jurors may not understand it. Keep it simple, but don't talk down to people.

How do you tell if you and a juror are on the same wavelength? Things can change, of course, but if at the outset you don't like her looks, the chances are she doesn't like you either. Does she look at you when she's answering a question? Does she mumble or speak right up? Does she fidget around when she's talking? Does she giggle or cross her arms? Does she say "How's that again?" to perfectly simple questions? Does she look at your opponent as the Second Coming? Pay attention to all of it.

Guard your peremptories. If a juror says that a newspaper wrongly reported

his arrest on a morals charge, try to get him to excuse himself rather than use a peremptory. You can suggest to him that perhaps he might not feel comfortable in the case or that his past experience might affect his thinking no matter how hard he tries to put it out of his mind. If you keep at it, he'll probably get the point, but nail it down so the other side can't rehabilitate him. On the other hand, if you detect a hesitation in a juror's answer when she's asked if she could treat your client as she would any other defendant, resist the temptation to inquire; the answer could infect the rest of the panel. If you're running low on challenges and don't know whether to excuse juror X, look around to see what's left. They may not be any better; everything is relative.

Of course, in a lot of jurisdictions, the judge handles jury selection. If that is the case, don't lose hope. Although your written questions may not be asked and probably won't elicit meaningful responses, you can still rely on stereotypes (e.g., postal workers do little or no work, eat out of the public trough, and are not bothered by getting something for nothing; social workers are all for the little guy who's been ground down by the system, etc.). And, if it looks grim, recall the observation of Finley Peter Dunne's fictional character Mr. Dooley: "Whin th' case is all over, the jury'll pitch th' testimony out iv th' window, an' consider three questions: 'Did Lootgert look as though he'd kill his wife? Did his wife look as though she ought to be kilt? Isn't it time we wint to supper?'"

Robert C. Bernius (rbernius@nixonpeabody.com) is a partner in the Washington, D.C., office of Nixon Peabody LLP.

Weeding Out the Toxic Juror

RICHARD M. GOEHLER

Although many nonmedia cases attract little attention, the media become news whenever they go on trial. Moreover, more than most types of litigants, the media face bias the moment they walk into a courtroom. Nearly everyone these days holds a strong opinion—generally, a negative one—about the people who produce newspaper copy and television programming. Thus, successful trial strategies of media counsel must include strategies on how to weed out biased, and especially toxic, jurors in the jury selection process.

Voir dire is the first opportunity to discover and overcome bias against the media, especially significant bias held by the toxic juror. Direct questions such as "Are you biased against the media?" are generally ineffective in learning what prospective jurors actually think. A more successful strategy is to ask about their experiences with the media:

- Do you listen to talk radio?
- Do you ever listen to Rush Limbaugh, Howard Stern, or Don Imus? What do you think of these shows?
- Do you ever call into talk radio shows? What do you think of people who do?
- Do you read the local newspaper? How about national newspapers like the *New York Times* or *Washington Post*?
- Do you watch local television news? CNN or Fox News?

Prospective jurors tend to freely discuss their media habits in general. This process can provide an excellent way to learn their opinions about and potential biases toward the media.

Voir dire can provide other opportunities to root out and reduce biases against the media in the courtroom. When there is an audio or video recording of a broadcast at issue, the media defendant should consider seeking the court's approval to play the recording for the prospective jurors. This can be especially important to accomplish at least two goals. First, it begins desensitizing the prospective jurors to statements that are shocking in nature: emotional reactions to the statements will likely have subsided by the time the deliberations begin. Second, airing the recording provides an opportunity to strike a juror for cause if the juror becomes instantly offended and expresses an inability to overcome a negative emotional reaction to the statements.

Richard M. Goehler (rgoehler@fbtlaw.com) is a partner in the Cincinnati office of Frost Brown Todd LLC.

Top Ten Tips for Picking Juries

10. Make your case more accessible by comparing its facts to real-life experiences.
9. Get everyone who could be on a jury to say something.
8. Try to establish your personal credibility.
7. Weed out the toxic potential jurors, i.e., those who hate you, your client, your mother, their mothers, or themselves.
6. If an audio or video broadcast is at issue, consider asking the court's permission to play it for prospective jurors.
5. Ask indirect questions (e.g., "Do you listen to talk radio?") to uncover potential biases.
4. Remember that first impressions, yours and theirs, count.
3. Address prospective jurors by their names.
2. Avoid prospective jurors who don't have a spouse, children, or a dog or cat; read mystery novels; and are self-employed.
1. Don't panic.

Solicit Their Views on the Media

NANCY WELLS HAMILTON

In approaching voir dire in a media case, it is important to get a read on your panel to determine who is media savvy, who hates the media, and who is pro-First Amendment. Granted, their eyes will gloss over if you start inquiring about their views on the First Amendment, but you can use terminology that is more friendly to the layperson and more conducive to discussion, such as beliefs in free speech and free press.

One approach is to ask the panelists

(either through a prepared questionnaire or in voir dire) about their habits with respect to the types of media they use most frequently ("What type of media do you use most frequently, i.e., Internet, cable TV, radio, newspapers, magazines, books, movies, etc.?") and then elicit responses as to why. Their responses will give you insight into whether they are news savvy or more interested in entertainment, whether they are critical thinkers or couch potatoes, and even what their political bent is (Fox, CNN, or E!; *New York Times, Wall Street Journal, Village Voice,* or *New York Post*).

For example, the other day while flying to Los Angeles, I finished the *New York Times* and offered it to the man in the seat next to me. His response was, "No, I don't want it. I don't want to ruin my view of the world." He was serious. I didn't explore why but did notice that he read mystery books and said he didn't have a wife, children, or a dog and was self-employed. From this information alone, I know that I would not want him on my jury.

Another benefit to these questions is to ferret out the pro-speech First Amendment jurors and to condition the panel to themes that you expect to develop in your case. One of the techniques I use is to identify a pro-First Amendment juror, ask an open-ended free speech question, and get that juror to make a speech to the panel for me.

Nancy Wells Hamilton (nhamilton@jw.com) is a partner in the Houston office of Jackson Walker L.L.P.

Sift and Loop

CHARLES A. BROWN

In the jury selection process, keep it simple. Don't try to argue your case; simply try to establish a rapport (i.e., establish your personal credibility) and eliminate the extremists (i.e., those who hate you, your client, your mother, or themselves).

In the jury selection process, don't be afraid to "sift" and then "loop." The sifting process is when you make inquiries with perhaps three or more potential jurors, probably not doing anything but dealing with names and places of employment and without really trying to create rapport. You are just sifting. But when you connect with a juror with whom you have some chemistry or just a nice comfort level, then start your real selection process with this juror. Establish a fundamental point; for example, "Whether or not you like the message the media convey, it is important in our society that the message be heard." Then, when you get your nodding agreement, loop back to the previous jurors and ask if they agree with this juror, Mrs. Jacobs. Now you have the other jurors agreeing with one of their own, and you can easily build upon this notion you have established.

The other jurors will hear the words being spoken, but, more importantly, they will sense the rapport between you and Mrs. Jacobs. By sensing this chemistry, they will be more willing to connect with you when you loop back. The chemistry and rapport for which you are striving is similar to entering a party or social occasion. You generally sift before you connect. Once you connect, it is easier to build rapport with others because you have a nucleus from which to begin. The same is true with jury selection, except without the wine.

I have tried cases where I have sifted through eight to ten potential jurors before I could find even one with whom I felt I could connect. Don't panic. You will find someone; and then when you loop back, you will be surprised at how the short, cryptic answers become complete thoughts and sentences.

Don't overcomplicate the process. Don't try to establish an agenda. Don't worry about all of the issues of your case. Just sift and loop.

Charles A. Brown (charlesabrownesq@cableone.net) is an attorney in private practice in Lewiston, Idaho.

Privilege and Defamation

(Continued from page 1)

not be resolved without unavailable classified government intelligence central to the plaintiff's allegations.

Trulock arose out of the government's investigation of Dr. Wen Ho Lee, a Taiwanese American scientist who was employed at Los Alamos National Laboratory, a government laboratory charged with ensuring the safety and reliability of the nation's nuclear stockpile. Dr. Lee was accused of mishandling sensitive documents concerning the United States' nuclear weapons.[8] Notra Trulock, then employed by the Department of Energy, was one of the government investigators responsible for initiating the investigation of Dr. Lee.

Lee and his lawyers charged in the press and in court documents that Trulock improperly focused on Dr. Lee because of his ethnicity. Trulock sued for defamation. During discovery, the government sought a protective order against the disclosure of classified documents, asserting that the reason for its initial investigation of Lee, including predicate information provided by Trulock, was protected from disclosure by the state secrets privilege.[9] After a magistrate granted the government's motion and entered a protective order, the government intervened as a defendant and moved for summary judgment on the ground that the case could not be litigated without the privileged information.[10] The district court agreed and dismissed the case. Trulock appealed.

As the court of appeals observed, the state secrets privilege is properly invoked to prevent the disclosure of evidence that raises national security concerns, that is, where "'there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged.'" Dismissal of a civil lawsuit pursuant to the state secrets privilege is required where (1) the privileged information is "critical to the resolution of core factual questions in the case"; (2) "the plaintiff's ability to prove his case necessarily depends on or threatens the disclosure of privileged information"; or (3) the absence of such information "deprives [the defendant] of a valid defense."[11]

The Fourth Circuit concluded that Trulock's motivation for his conduct in connection with the investigation of Dr. Lee "is itself a state secret."[12] It therefore dismissed the case, reasoning that "basic questions about truth, falsity, and

malice cannot be answered without the privileged information."[13]

Almost twenty years earlier, in *Fitzgerald v. Penthouse International Ltd.*, the Fourth Circuit affirmed the dismissal of a defamation case because the invocation of the state secrets privilege had prevented critical evidence from being available at trial.[14] In that case, the plaintiff alleged that a magazine article had falsely implied that he sold "top secret marine mammal weapons system" technology to foreign countries.[15] The plaintiff planned to call expert witnesses to testify as to falsity, but the Navy objected that an adjudication of the defamation claim would likely lead to public disclosure of classified information that "could reasonably be expected to cause grave damage to the national security."[16] After reviewing a classified affidavit filed by the Secretary of the Navy and acknowledging the severity of the remedy of dismissal, the Fourth Circuit nevertheless concluded that the district court had properly dismissed the case. "Due to the nature of the question presented in this action and the proof required by the parties to establish or refute the claim," the court explained, "the very subject of this litigation is itself a state secret."[17] Dismissal was necessary because "truth or falsity of a defamatory statement is the very heart of a libel action."[18]

Under the *Fitzgerald* rule, dismissal is appropriate when the merits of the controversy at issue are "inextricably intertwined with privileged matters."[19] Where the classified information can effectively be obtained elsewhere or is not highly material, dismissal may not be the appropriate remedy.[20] But when access to material bearing on core factual materials is denied, dismissal is warranted.[21]

Although the authors are aware of one court that has expressed a reluctance to expand this doctrine to encompass privileged information that may not literally qualify as a state secret, a close reading of *Fitzgerald* makes clear that the court concluded the unavailable information "was not itself the subject of the litigation."[22]

These cases provide a framework, perhaps more relevant in today's world of increasing secrecy, for arguing that information sought but ultimately withheld deals a fatal blow to a defamation action because an exploration of the truth is of the utmost importance in such an action.

Attorney-Client and Doctor-Patient Privilege

The principle of dismissal for refusal to produce evidence applies with equal force when either the attorney-client privilege or the doctor-patient privilege is invoked. If a plaintiff files a complaint that raises claims implicating the attorney-client privilege, for example, "at some point in the litigation, the plaintiff will have to make a decision as to whether to waive the attorney-client privilege or to abandon the claims."[23] Likewise, when a patient puts in issue his medical or psychiatric condition, the patient cannot then assert that information relating to that condition is beyond the reach of discovery.[24]

When the plaintiff cannot waive the privilege because the privilege is not his to waive, he must suffer the consequence of dismissal. This concept was applied in *Eckhaus v. Alfa-Laval, Inc.*,[25] a defamation action brought by an attorney against his client. In that case, the attorney, who had served for a brief period as the defendant's general counsel, asserted that he was defamed by his employer during a performance evaluation at which several officers of the company were present.[26] The company filed a summary judgment motion, arguing that continued prosecution of the case would require the attorney to reveal client confidences in violation of the state ethical rule relating to disclosure of client secrets. The attorney, on the other hand, asserted that an exception to the rule applied, namely, that such confidences could be revealed in response to a claim that the attorney had engaged in wrongful conduct. The court, however, concluded that the exception was inapposite because it applied only in cases where the client initiated the lawsuit against the attorney and made a formal accusation of misconduct. "Informal charges made during a performance review of an in-house attorney specifically contemplated by his employment contract do not amount to 'an accusation of wrongful conduct' under these authorities."[27] Accordingly, the court held that the attorney could not maintain his action because its prosecution would require him to disclose confidential communications with the client/defendant in violation of the rules of professional responsibility.[28]

Self-Incrimination

The argument for dismissal similarly applies when a plaintiff, or a third party who would otherwise provide evidence material to the case, invokes the privilege against self-incrimination. As one court put it,

> The scales of justice would hardly remain equal in these respects, if a party can assert a claim against another and then be able to block all discovery attempts against him by asserting a Fifth Amendment privilege to any interrogation whatsoever upon his claim. If any prejudice is to come from such a situation, it must, as a matter of basic fairness in the purposes and concepts on which the right of litigation rests, be to the party asserting the claim and not to the one who has been subjected to its assertion. It is the former who has made the election to create an imbalance in the pans of the scales.[29]

Rarely are the circumstances so stark. Practitioners should note that in the context of the privilege against self-incrimination, a privilege that arises from a constitutional right, courts are reluctant to impose the heavy penalty of dismissal, at least at first. Thus, the inquiry focuses on whether the case should be dismissed outright or stayed for some period of time to allow the criminal issues to resolve.

When access to material bearing on core factual materials is denied, dismissal is warranted.

To determine the appropriate outcome, some courts will apply a balancing test, focusing on the defendant's need for disclosure; the availability of possible alternatives, such as a stay; and the resulting prejudice to the parties.[30]

Other courts have suggested that a plaintiff's invocation of the privilege against self-incrimination should result in dismissal only as a last resort. In *Wehling v. Columbia Broadcasting System*,[31] for example, the Fifth Circuit directed the district court to enter a protective order staying further discovery in the case until the applicable statute of limitations for any criminal activity to which the plaintiff might be subject had

run. The court's order resulted in a three-year stay.[32]

In that case, Carl Wehling, the owner of several parochial and trade schools, sued CBS, asserting that he had been libeled by a network news report stating that he had defrauded the government and his students.[33] During discovery, Wehling refused to answer certain questions in his deposition and then asserted his Fifth Amendment privilege against self-incrimination after being ordered to comply. Wehling refused to comply with the order compelling his testimony and sought a three-year stay of the litigation, but the district court granted CBS's motion to dismiss with prejudice.

The more prudent approach may be to seek a stay, at least as the first step toward dismissal.

On appeal, the Fifth Circuit reversed. Although the court of appeals emphasized that a "civil plaintiff has no absolute right to both his silence and his lawsuit," it stated that "[n]either, however, does the civil defendant have an absolute right to have the action dismissed anytime a plaintiff invokes his constitutional privilege."[34] The court of appeals recognized that what the plaintiff sought—a "three-year hiatus in the lawsuit"—was "undesirable," but it determined that "such inconvenience seems preferable at this point to requiring plaintiff to choose between his silence and his lawsuit."[35] However, the Fifth Circuit left open the window to dismissal, holding that upon the expiration of the stay, the case could be dismissed if the district court determined both that CBS had been deprived of crucial information as a result of the delay in discovery imposed by the stay and that, as a result, its ability to prove the truth of its report had been compromised.[36]

A related, but more difficult, argument to make is that a third party's assertion of the Fifth Amendment privilege, which precludes the disclosure of critical information, warrants dismissal or the entry of a stay. On the one hand, the principle that the defendant is deprived of evidence necessary for a fair defense operates in this scenario. On the other hand, some courts have expressed reluctance to impose this drastic sanction on a plaintiff who does not and cannot control the assertion of the privilege.[37] However, when the plaintiff is a corporate entity and the person who asserts the privilege is a director or officer, or former director or officer, the equities may resolve in the defendant's favor. Of course, if the court finds that the information precluded from disclosure by the assertion of the Fifth Amendment privilege is not crucial to the outcome of the case, no stay—and certainly no dismissal—will be granted.[38]

Although a request for dismissal is likely to be the first choice of every defendant, the more prudent approach under some circumstances may be to seek a stay, at least temporarily as the first step toward dismissal. In any event, at some point after a stay is entered, the issue of dismissal must finally be confronted. Although dismissal of an action is not a remedy to be taken lightly, it can certainly be argued that dismissal is the only viable alternative when the discovery sought by the defendants is critical to a central issue in the litigation and an indefinite delay of the lawsuit could prejudice the defendants.[39]

How Should a Defendant Ensure Fairness?

No matter what the case, the process toward dismissal must be a slow and methodical one. The groundwork for framing that issue must begin early with discovery requests, including deposition questions, aimed very precisely at eliciting the privileged information.

In *Glunk v. KYW-3 TV*,[40] for example, the plaintiff, a doctor who had been sued by the estate of a deceased patient for causing the patient's death, brought a defamation action against a television station that reported on the malpractice lawsuit. However, when his deposition was taken, the doctor refused to testify about his treatment of the deceased patient, an issue that went directly to the heart of his defamation claim, claiming that such testimony was barred by restrictions imposed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[41] and the doctor-patient privilege. He also refused to respond to questions related to his hospital privileges and the outcome of his peer review experiences, claiming that the peer review proceedings were privileged under the Pennsylvania Peer Review Protection Act.[42] The defendants moved to compel answers to these questions.

With respect to the doctor's claims that he could not disclose information subject to HIPAA or the doctor-patient privilege, the court ruled from the bench that the plaintiff would be compelled to reconvene his deposition and that it would rule on each of the doctor's privilege claims on a question-by-question basis. With regard to the doctor's refusal to respond to questions concerning his peer review experiences, the court agreed with the defendants that the plaintiff must produce this information, which was highly material to his defamation action.[43] Shortly thereafter, the doctor withdrew his claim.

Conclusion

Defendants certainly should not hesitate at an early stage to raise the suggestion that dismissal is warranted in the particular context of a defamation action, given the recognition by many courts that there exists a constitutional imperative to avoid "long and expensive litigation productive of nothing."[44] Although dismissal is a severe penalty, there is significant authority to support the proposition that it is warranted when—as is the case in defamation actions where truth is clearly at issue—the defendant's inability to obtain privileged information seriously impedes its ability to litigate core issues in the case.

Endnotes

1. In *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 776–77 (1986), the U.S. Supreme Court held that a defamation plaintiff cannot recover damages against a media defendant for speech of public concern unless the plaintiff proves in the first instance that the speech is false.

2. For examples of rules authorizing a court to dismiss a case as a sanction for a party's failure to make discovery or to obey an order of the court respecting discovery, see FED. R. CIV. P. 37 (b)(2)(C) (allowing for dismissal of a case when a party commits discovery violations, such as failing to obey an order to provide or permit discovery); CAL. CIV. PROC. CODE § 2023.030(d)(3) (authorizing court to dismiss an action for misuse of the discovery process); N.Y. C.P.L.R. § 3126(3) (McKinney 1970 & supp. 1989)

(permitting court to dismiss the action, or any part thereof, for refusing to obey an order for disclosure of information that court determined ought to have been disclosed); FLA. R. CIV. P. 1.380(b)(2(C) (providing that if a party fails to obey an order to provide or permit discovery, then the trial court may issue an order dismissing the action or rendering a default judgment against the disobedient party); MD. RULE 2–433(a)(3) (authorizing court to dismiss an action, or any part thereof, or enter a judgment by default for failure to comply with discovery); TEX. R. CIV. P. 215(b)(5) (authorizing court, after notice and hearing, to dismiss an action, with or without prejudice, for failure to comply with discovery requests).

3. *See, e.g.,* Caesar v. Mountanos, 542 F.2d 1064, 1068 (9th Cir. 1976) ("Every person who brings a lawsuit under our system of jurisprudence must bear disclosure of those facts upon which his claim is based."); Upper Deck Co. v. Breakey Int'l, BV, 390 F. Supp. 2d 355, 362 (S.D.N.Y. 2005) (dismissing plaintiff's claim for lost royalties where plaintiff refused to divulge supporting information in discovery; court refused to consider same information when plaintiff proffered it in opposition to summary judgment); *In re* SCT Sec. Litig., No. 84–6004, 1988 WL 13263, *1 (E.D. Pa. Feb. 18, 1988) (unpublished disposition) (stating that third-party plaintiff "'has no absolute right to both his silence and his lawsuit'" and dismissing third-party complaint for plaintiff's refusal to disclose information relevant to his claims) (citation omitted); Wolford v. Cerrone, 584 N.Y.S.2d 498, 499 (N.Y. App. Div. 1992) (affirming dismissal of personal injury action where plaintiff failed to attend independent medical examination); Nardella v. Dattilo, 35 Pa. D. & C.4th 257, 261 (Pa. Ct. Com. Pl. 1996) ("[I]t would be fundamentally unfair to allow a litigant to make allegations about, and claim damages on the basis of, a mental or emotional condition and at the same time prevent a litigation adversary from testing those allegations or examining the asserted causal nexus."); Loftus v. Consol. Rail Corp., 12 Pa. D. & C.4th 357, 359, 361–62 (Pa. Ct. Com. Pl. 1991) (agreeing with defendant that it "'defies the principle[s] of justice and equity if plaintiff is permitted to submit a claim for alleged emotional and mental injury and yet forbid the party against whom the claims are made from discovery of the nature and extent of those allegations'" and ordering plaintiff either to make the requested disclosure or suffer dismissal of claims relating to emotional or physical injury).

4. 475 U.S. 767 (1986).

5. Fitzgerald v. Penthouse Int'l, Ltd., 776 F.2d 1236, 1243 n.11 (4th Cir. 1985).

6. Although the state secrets privilege was officially recognized by the U.S. Supreme Court in *United States v. Reynolds*, 345 U.S. 1 (1953), the legal foundation for the privilege was established in the nineteenth century in *Totten v. United States*, 92 U.S. 105, 107 (1875). There, the Supreme Court stated thus:

> [P]ublic policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated. . . . Much greater reason exists for the application of the principle to cases of contract for secret services with the government, as the existence of a contract of that kind is itself a fact not to be disclosed. *Id.* When the privilege is successfully invoked, the privileged information cannot be considered in the course of the legal proceedings, and the task of the court in such a case is to determine how the assertion of the privilege affects the continued prosecution of the case. *See* Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 547–48 (2d Cir. 1991) (dismissal proper if state secrets privilege "so hampers the defendant" that trier of fact is likely to reach an erroneous result); Kasza v. Browner, 133 F.3d 1159, 1170 (9th Cir. 1998) (dismissal proper if "the very subject matter of [plaintiff's] action is a state secret"); *In re* United States, 872 F.2d 472, 476 (D.C. Cir. 1989) (dismissal proper "[i]f the [privileged] information is essential to establishing plaintiff's prima facie case").

7. 66 F. App'x 472 (4th Cir. June 3, 2003) (unpublished disposition).

8. *Id.* at 473. Lee was initially accused of stealing nuclear secrets and selling them to the People's Republic of China. The government later charged Lee with mishandling restricted data, a charge to which Lee ultimately pled guilty. *Id.* at 474.

9. *Id.* at 474–75.

10. The privilege belongs to the government. *Reynolds*, 345 U.S. at 7 (stating that the state secrets privilege "can neither be claimed or waived by a private party"). Thus, in cases where the government is not a party, a motion for dismissal usually is preceded by some form of government intervention. *E.g., Fitzgerald*, 776 F.2d at 1237 (government intervened and moved to dismiss action on state secrets grounds).

11. *Trulock*, 66 F. App'x at 475–76 (citation omitted).

12. *Id.* at 477.

13. *Id.* at 476.

14. 776 F.2d at 1243–44.

15. *Id.* at 1242.

16. *Id.*

17. *Id.* at 1243.

18. *Id.* at 1243 n.11; *see also* Edmonds v. U.S. Dep't of Justice, 323 F. Supp. 2d 65, 79 (D.D.C. 2004) (dismissing civil action where "any effort . . . by the defendants to rebut [elements of plaintiff's claim] would risk disclosure of privileged information"), *aff'd*, 161 F. App'x 6 (D.C. Cir. 2005) (unpublished disposition); Patterson v. Fed. Bureau of Investigation, 893 F.2d 595 (3d Cir. 1990) (dismissing action where plaintiff could not receive any meaningful discovery in light of the FBI's assertion of the state secrets privilege).

19. 776 F.2d at 1243 n.11.

20. *See* DTM Research, L.L.C. v. AT&T Corp., 245 F.3d 327, 334 (4th Cir. 2001) (information subject to the state secrets privilege was "potentially relevant" but "not central to the question" of liability, and similar evidence was available elsewhere).

21. The privilege also has been applied outside the context of defamation actions. *See* Tilden v. Tenet, 140 F. Supp. 2d 623, 627 (E.D. Va. 2000) (summary judgment for defendant granted in an employment discrimination case where "there [was] no way in which th[e] lawsuit [could] proceed without disclosing state secrets"); Sterling v. Tenet, 416 F.3d 338, 346–47 (4th Cir. 2005) (affirming dismissal of CIA agent's employment discrimination suit both because plaintiff could not prove his case "without exposing at least some classified details of the covert employment that gives context to his claim" and because bar on state secrets evidence would also preclude government from presenting defense of legitimate nondiscriminatory reason for alleged adverse action); Tenenbaum v. Simonini, 372 F.3d 776, 777 (6th Cir. 2004) (affirming summary judgment for defendants in religious discrimination case because "the state secrets doctrine . . . deprive[d] Defendants of a valid defense"); Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 547 (dismissing plaintiff's wrongful death claim against missile system manufacturer because questions of liability could not "be resolved or even put in dispute without access to [privileged] data

regarding the design, manufacture, performance, functional characteristics, and testing" of the defendant's products); El-Masri v. Tenet, 437 F. Supp. 2d 530, 538–39 (E.D. Va. 2006) (dismissing plaintiff's suit against CIA for illegal detention under "extraordinary rendition" program because, inter alia, defendant's defense "risk[ed] the disclosure of specific details about the rendition argument"); *Edmonds*, 323 F. Supp. 2d at 79, 81–82 (dismissing First Amendment, Fifth Amendment, and Privacy Act claims in part because "the defendants are unable to assert valid defenses to [plaintiff's] claims without . . . disclosures" of state secrets).

22. In *Price v. Viking Penguin, Inc.*, 676 F. Supp. 1501 (D. Minn. 1988), *aff'd*, 881 F.2d 1426 (8th Cir. 1989), an FBI agent brought a defamation action against the author of a book about the federal government's treatment of Native Americans. Relying on *Fitzgerald,* 776 F.2d at 1243 n.11, the defendants moved for dismissal of the case after the court, on the basis of the common law informer's privilege, prohibited the plaintiff from disclosing the identity of any FBI informant. *Price*, 676 F. Supp. at 1514. However, the court expressed uncertainty concerning whether dismissal was appropriate "beyond contexts involving military or state secrets privileges" and concluded in any event that the information the defendants sought "was not itself the subject of the litigation" as was the case in *Fitzgerald. Price*, 676 F. Supp. at 1514–15.

23. Ulizzi v. Trellis, 20 Pa. D. & C.4th 300, 309 (Pa. Ct. Com. Pl. 1993).

24. *See, e.g.,* Schoffstall v. Henderson, 223 F.3d 818, 823 (8th Cir. 2000) ("Numerous courts . . . have concluded that, similar to attorney-client privilege that can be waived when the client places the attorney's representation at issue, a plaintiff waived the psychotherapist-patient privilege by placing his or her medical condition at issue.") (citations omitted); Maynard v. City of San Jose, 37 F.3d 1396, 1402 (9th Cir. 1994) ("[plaintiff] waived any privilege protecting his psychological records when he put his emotional condition at issue during the trial"); Heller v. Norcal Mut. Ins. Co., 8 Cal. 4th 30, 44 n.5 (Cal. 1994) (observing that rule of evidence provides that "the physician-patient relationship is waived 'as to a communication relevant to an issue concerning the condition of the patient if such issue has been tendered by . . . [t]he patient'") (citation omitted); Scheff v. Mayo, 645 So. 2d 181, 182 (Fla. Dist. Ct. App. 1994) (plaintiff who makes his mental or emotional condition an element of his claim cannot invoke the doctor-patient privilege); Fetterhoff v. Zalezak, 34 Pa. D. & C.4th 67, 70 (Pa. Ct. Com. Pl. 1996) (citing Rost v. State Bd. of Psychology, 659 A.2d 626, 629 (Pa. Commw. Ct. 1995)) ("[I]t is controlling appellate law under *Rost* that where a plaintiff in a civil suit places his or her mental condition directly at issue, the [doctor-patient] privilege is waived as to that condition and the plaintiff must either consent to the disclosure of the information at issue or be precluded from pursuing claims related to his or her emotional and mental condition.").

25. 764 F. Supp. 34 (S.D.N.Y. 1991).

26. *Id.* at 35.

27. *Id.* at 38.

28. *Id.*

29. Lyons v. Johnson, 415 F.2d 540, 542 (9th Cir. 1969); *see also, e.g.*, *In re* Fin. Servs. of Fla., Inc., 259 B.R. 391, 407 (Bankr. M.D. Fla. 2000) ("[A] person may not seek affirmative relief in a civil action and then invoke the Fifth Amendment to avoid giving discovery, using the Fifth Amendment as both a 'sword and a shield.'"); Capanelli v. News Corp., 35 Med. L. Rep. (BNA) 1084, 1086 (N.Y. Sup. Ct. Jan. 26, 2006) ("A plaintiff who invokes the privilege [against self-incrimination] to deny a defendant substantive discovery to which it is entitled may not continue to maintain the action.") (citation omitted); Fremont Indemnity Co. v. Superior Court, 187 Cal. Rptr. 137, 140 (Ct. App. 1982) ("'[T]he gravamen of [plaintiff's] lawsuit is so inconsistent with the continued assertion of [the Fifth Amendment privilege against self-incrimination] as to compel the conclusion that the privilege has in fact been waived.'") (citation omitted).

30. *See, e.g.*, Black Panther Party v. Smith, 661 F.2d 1243, 1270–74 (D.C. Cir. 1981) (court should use balancing approach, weighing defendant's need for disclosure, possible alternatives such as a stay, and the resulting prejudice to the parties), *vacated sub nom.*, 458 U.S. 1118 (1982).

31. 608 F.2d 1084 (5th Cir. 1979).

32. *Id.* at 1089.

33. *Id.* at 1086.

34. *Id.* at 1088.

35. *Id.* at 1089.

36. *Id.*

37. *See, e.g.*, Kisser v. Coal. for Religious Freedom, No. 92 C 4508, 1997 WL 83296, at *1 (N.D. Ill. Feb. 19, 1997) (unpublished disposition) (refusing to dismiss plaintiff's complaint based on third party's refusal to testify and stating that "[t]here is no valid reason to hold a third party's assertion of his Constitutional right against self-incrimination against a party to an action.").

38. For example, in *Kisser*, the executive director of the Cult Awareness Network sued Church of Scientology defendants for, inter alia, libel based on statements "the gist of which state that Kisser advocates criminal activity and has personally engaged in criminal activity." 1997 WL 83296, at *1. After Kisser invoked the Fifth Amendment in response to questions "relating to the promotion, use or distribution of illegal drugs," the defendants sought dismissal. The court rejected the defendants' argument as irrelevant because "[t]he case, as it now stands, is clear on the point that the criminal activity that is the subject of the claimed libel relates to violent deprogramming activities that involve forcible restraint and assault." *Id.*

39. *See* Serafino v. Hasbro, Inc., 82 F.3d 515, 518 (1st Cir. 1996) ("[W]hile a trial court should strive to accommodate a party's Fifth Amendment interests[,] . . . it also must ensure that the opposing party is not unduly disadvantaged. After balancing the conflicting interests, dismissal may be the only viable alternative.") (citations omitted).

40. No. 02–08858 (Pa. Ct. Com. Pl., Chester County).

41. 42 U.S.C. § 1320d (2006).

42. 63 PA. CONS. STAT. § 425 (West 2006).

43. The court held that the act protected against the use of such information in an action against the doctor but did not entitle the doctor to rely on the act to withhold information he put in issue in the case. *Glunk*, No. 02–08858 (Sanchez, J.) (unpublished disposition). The court stated, "The Peer Review Protection Act was enacted to serve as a shield. The doctor, in this instance, is attempting to use it as a sword." *Id.*

44. Wash. Post Co. v. Keogh, 365 F.2d 965, 968 (D.C. Cir. 1966); *see also* McBride v. Merrell Dow Pharms., Inc., 717 F.2d 1460, 1466 (D.C. Cir. 1983) (defamation actions "should be controlled so as to minimize their adverse impact on press freedom"); Coles v. Wash. Free Weekly, Inc., 881 F. Supp. 26, 30 (D.D.C. 1995) ("given the threat to the first amendment posed by non-meritorious defamation actions, it is particularly appropriate for courts to scrutinize such actions at an early stage of the proceedings to determine whether dismissal is warranted.").

Officers, Governing Committee, and Editors 2006 – 2007

Communications Lawyer
Volume 25:1
Spring 2007

Communications Lawyer
American Bar Association
321 North Clark St.
Chicago, IL 60610-4714

Nonprofit Organization
U.S.Postage
PAID
American Bar
Association