# In this issue

# **COVER STORY**

A recent Ninth Circuit decision suggests that reporters should be able to avoid intrusion tort liability simply by avoiding questions that could elicit highly personal information and by limiting themselves to locations where they were actually invited, even if under false pretenses.

# Chair's Column .....2

Against the backdrop of *Grutter v. Bollinger*, Chair Tom Kelley discusses the Forum's ambitious efforts to promote diversity. The lack of "meaningful ethnic and racial diversity," he says, "will only sap our credibility and strength as advocates."

# Can the Spam.....3

Federal regulation of unsolicited bulk e-mail, otherwise known as spam, appears inevitable. The U.S. Supreme Court has been increasingly protective of commercial speech, proponents of regulation believe that the problem is so pressing that some type of effective regulation will permissible as long as it does not ban all e-mail advertisements.

# New Privacy Regs .....12

The regulations implementing the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 took effect in April, and journalists have encountered new obstacles to obtaining information on newsworthy issues surrounding health care.

# Skirting the Reporter's Privilege ......15

Under a loophole in the Uniform Witness Act, targets of subpoenas issued on behalf of out-of-state courts may not have an opportunity to argue that the asked-for materials are privileged. The authors discuss how some petitioners may attempt to circumvent the reporter's privilege altogether and potential strategies for dealing with such maneuvers.

# Intrusion Tort Liability and Undercover News Investigations

SHARON MCGOWAN

Enlightened choice by an informed citizenry is the basic ideal upon which an open society is premised, and a free press is thus indispensable to a free society.

— JUSTICE POTTER STEWART

In a democratic society, the press must be free to scrutinize and criticize public officials and government agencies. In addition to policing the government, however, the media serve an important role in exposing misconduct in the private sector. For example, in recent years, the media have revealed a range of dangerous corporate practices ranging from unsanitary food handling to faulty medical testing. In many of these cases, publicly available information about a company would not have suggested that such offenses were taking place, and reporters were only able to learn about the misconduct by employing undercover reporting techniques.

When using undercover newsgathering methods, media organizations often find themselves operating at the margins of well-established legal principles designed to protect individual privacy and property rights. As a result, those targeted by investigative reporting often claim that the press violated their rights in the course of investigating the story. Frequently they will sue for so-called invasion of privacy torts, which include trespass, intrusion on seclusion, and the publication of private facts. In light of the high standard that plaintiffs must satisfy to succeed on defamation claims, lawsuits alleging intrusion upon seclusion have, in many ways, become the new battleground in the ongoing war between individuals who wish to shield their actions from scrutiny and media organizations that seek to report news of importance to the public. This article

assesses the extent to which intrusion tort liability threatens to squelch undercover newsgathering by examining the significant intrusion tort cases in each major area of newsgathering activity. It then analyzes the Ninth Circuit's recent decision in *Medical Laboratories Management Consultants v. ABC*, and its potential impact on the development of intrusion tort jurisprudence.

The tort of intrusion upon seclusion penalizes "highly offensive" intrusions into areas that one would reasonably expect to remain private. This tort differs from publication torts in that the media can be held liable for actions taken in the course of gathering news, regardless of whether the press ever publishes the information. Most people suing for intrusion torts, however, only learn about the surveillance as a result of the media's publication of the private material about them. Notwithstanding the fact that intrusion and publication tort claims frequently arise from the same incidents, courts have attempted to keep these two causes of action analytically distinct. Therefore, it is essential that the media and their advocates understand the unique contours of the tort of intrusion upon seclusion in order to evade liability.

This article begins by offering a brief overview of privacy torts, including the tort of intrusion upon seclusion, and by explaining exactly what is meant by "intrusion." Second, the article describes the legal landscape of intrusion tort cases involving undercover investigative report-

(Continued on page 18)

# FROM THE CHAIR

# Ethnic and Racial Diversity and the Forum

When the printer hands over this issue of Communications Lawver to the U.S. Postal Service, the dog days of August will have come to baseball, Congress, and the ABA, and I will have completed my first year as your Chair. It has been a very good year, largely due to the efforts of your Governing Committee,

Division Chairs, and others who have contributed to our work.

The biggest challenge of the year was our diversity initiative. With the indefatigable will and skill of Paulette Dodson and the other members of our Diversity Committee (Jon Avila, Mary Snapp, and Andrew Mar), we have created for the first time a scholarship for a lawyer of color at our Annual Conference, dedicated a session of the 2003 conference to diversity issues, established a mentoring program, and written our in-house counsel membership seeking their help in encouraging diversity among outside counsel.

On June 5th, we topped off this year's diversity effort by presenting a program segment at the National Conference for the Minority Lawver in Philadelphia, sponsored by the Business Law Section and the Commission on Racial and Ethnic Diversity of the ABA. The conference was at the Union League, one of the nation's oldest and most prominent city clubs (founded in 1862 to support the policies of Abraham Lincoln) housed in a venerable historic building downtown. As a baby boomer who suffers from that generation's difficulty in thinking of themselves as adults, I struggled to feel that I had any business in such a place. But it seemed most hospitable and comfortable to the much younger crowd who assembled for the conference. John Avila worked tirelessly and creatively in recruiting (and in surgically replacing last-minute cancellations) an exciting panel of mi-

Forum Chair Thomas B. Kelley (tkelley@ faegre.com) is a partner in the Denver office of Faegre & Benson LLP.



Thomas B. Kelley

nority professionals from media, law enforcement, civil liberties, and criminal defense perspectives that included Ms. Dodson as the "media lawyer," cool, precise, and interesting. George Freeman moderated our session-a souped-up version of "Newsgathering in the Shadow of Terrorism" that was presented at last February's Annual

Conference. The discussion, which focused primarily on the civil liberties is-

sues associated with secret detentions of and proceedings against noncitizens as part of the war against terrorism, provoked animated exchanges among the panelists. Ours was one of three concurrent break-out sessions, and I noticed that our attendance was slightly less than one-third of the whole, the others preferring instead more financially oriented programs such as "Review of Developments in Business and Corporate Litigation." That is roughly how our esoteric specialty fares at the ABA's Annual Meeting, so I guess that

(Continued on page 25)



Communications Lawyer (ISSN: 0737-N7622) is published quarterly by the Forum on Communications Law of the American Bar Association, 750 North Lake Shore Drive, Chicago, IL 60611. POSTMASTER: Please send address corrections to ABA Service Center, 750 North Lake Shore Drive, Chicago, IL 60611.

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

The opinions expressed in the articles presented in Communications Lawyer are those of the authors and shall not be construed to represent the policies of the American Bar Association or the Forum on Communications Law

Copyright © 2003 American Bar Association. Produced by ABA Publishing.

Thomas B. Kelley (2004) Faegre & Benson tkelley@faegre.com

### Laura Lee Stapleton

Jackson Walker L.L.P. lstapleton1@jw.com

### Managing Editor

Wendy J. Smith ABA Publishing wjsmith@staff.abanet.org

### Maria Arias (2003) Paulette R. Dodson (2003) Harold W. Fuson Jr. (2004).

Jonathan Hart (2003)

# **Immediate Past Chair** George Freeman (2002)

The New York Times Company freemang@nytimes.com

# **Editors**

Deanne E. Maynard Jenner & Block dmaynard@jenner.com

### Forum Administrator Teresa Ucok

American Bar Association tucok@staff.abanet.org

### **Governing Committee**

Andrea Hartman (2003) Elizabeth C. Koch (2003) Robert D. Nelon (2004) David Schulz (2004)

Jerry S. Birenz Sabin, Bermant & Gould, L.L.P. jbirenz@sbandg.com

### **Kurt Wimmer**

Chair-Elect

Covington & Burling kwimmer@cov.com

### Designer

Liaison, Young Lawyers Division

Amy Neuhardt (2004)

Sonya Taylor ABA Publishing taylors@staff.abanet.org

# Charles D. Tobin (2004) Jack M. Weiss (2004)

Nicole A Wong (2004)

# **Division Cochairs**

Eastern Jerry S. Birenz Robin Bierstedt Henry Hoberman Elizabeth A. McNamara

Alan Lapter (2003)

Liaison, Law Student Division

# Central Paulette Dodson Richard M. Goehler James T. Borelli Gregory M. Schmidt

Western Jonathan Avila David J. Bodney Guylyn Cummins Jerald N. Fritz Kelli L. Sager

# The Commercial Speech Doctrine, Spam Regulation, and Penis Enlargement Proposals

BRUCE E.H. JOHNSON

As the fractured opinions in the U.S. Supreme Court's nondecision in Nike, Inc. v. Kasky1 clearly suggest, the Court's commercial speech doctrine remains unsettled. Thus, at the outset, it is fair to acknowledge that confident predictions about its treatment of even indisputably commercial speech are hard to make.

A number of Justices seem uncomfortable with the very existence of a distinction between commercial and noncommercial speech and have openly questioned the iconic standard for analyzing restrictions on commercial speech2 set out in Central Hudson Gas & Electric Corp. v. Public Service Commission of New York.3 The Central Hudson holds that the First Amendment protects commercial speech concerning "lawful activity" that is "not misleading" unless the asserted governmental interest in regulation is substantial, the regulation "directly advances" the stated governmental interest, and the abridgement of speech rights "is not more extensive than necessary to serve that interest."4 Nevertheless, Central Hudson has yet to be abandoned. Instead, the Court appears committed to a more fact-specific treatment of commercial speech, refusing to afford it full protection, but clearly indicating that commercial speech will receive careful treatment.5

Poised against the Court's increasing recognition of the rights of commercial speakers is the deluge of unwanted emails to which states have already responded and the federal government seems surely to do soon. Dubbed by Internet users as "spam," an appellation that seemingly captures the exasperated disregard that it inspires, unwanted e-

Bruce E.H. Johnson (brucejohnson@dwt. com) is a partner in the Seattle office of Davis Wright Tremaine LLP. The author wishes to thank Don Courtney, a student at UCLA Law School, for his invaluable contributions to this analysis. The opinions in this article are not necessarily the views of the author's firm or its clients.

mail advertising has increasingly incurred the wrath of users, reputable marketers, and legislators. Although much of the regulation enacted to date focuses on truthfulness in the labeling and origin of commercial e-mail, a number of existing laws and proposed regulations will pose interesting challenges for the courts.

The problem is undeniable—and growing. Current estimates peg spam at 46 percent of all e-mails sent. By December 2003, the number is expected to reach 50 percent,7 up from 7 percent in 2001.8 In 2001, the Federal Trade Commission (FTC) began to routinely collect spam forwarded by angry consumers.9 During that year, the FTC received an average of 10,000 forwarded messages a day.10 In 2002, the number rose to 47,000 a day.11 The number has gone to 130,000 e-mails a day this year.12 Microsoft Network (MSN) reports an even more dramatic rise: two months ago 8 percent of MSN mail was spam, and now it is 50 percent.13 Estimates of the total number of spam messages sent in 2003 are 2,000 percent greater than the estimates for 2002.14

# **Spam Costs Money**

These numbers translate directly into costs for businesses and consumers. Because spam is responsible for a large part of the increase in Internet traffic, more and more Internet hardware is required to support the transmission of emails. One practice in particular typifies the spirit behind spam that is both so costly and annoying: spammers often use applications called "dictionary attacks" that generate e-mail addresses by going through the entire alphabet in each letter placeholder of an address, changing one letter at a time and generating millions of addresses.15 Each of these addresses is sent an e-mail. The vast majority of these millions of emails bounce, generating a bounce notification for each e-mail and using even more processing power.

Internet service providers (ISPs) bear

the primary cost of spam and do the bulk of the work of filtering spam and prosecuting spammers. But the costs to companies that dedicate employees to fighting spam are significant. Spammers frequently falsify the return addresses and domain names of their e-mails. They often route their e-mails through servers other than their own to disguise the true source of their e-mail. End users pay for real-time detective work by ISPs track spammers before the trail evaporates through charges for Internet and e-mail connection services. There are also productivity costs associated with sifting through spam; the latest estimates put the total cost of spam to businesses at \$10 billion a year.16

# **States Move Against Spam**

These costs have spurred a number of states to enact antispam measures, most of which provide for civil penalties for spammers that provide misleading information in their e-mails. 17 Such laws include provisions for labeling commercial e-mails as advertisements and providing opt-out e-mail addresses or phone numbers for consumers to contact to prevent further e-mails from a sender. The national scope of the problem has led to increasing calls for a federal law against spam.18 Most of the major proposals, such as the CAN-SPAM Act of 2003, provide for restrictions similar to the state laws but with some differences.<sup>19</sup> Some critics charge that these measures do not go far enough and that unsolicited e-mails should be prohibited unless consumers opt in to receive them.20

The constitutionality of some of these provisions has not fully been explored with regard to the First Amendment and its protection of commercial speech. As the Court has applied an ever-tighter interpretation of the Central Hudson test, exceptions made for noncommercial emails and any severe restriction of advertising by e-mail may run afoul of the Constitution. Certainly, if the Court were to apply strict scrutiny and abandon the *Central Hudson* test in favor of a single First Amendment treatment for all speech, bulk e-mail, whether commercial or not, would likely have to be treated the same, and many other restrictions would likely be invalid. However, given the pressing need for action and the apparent popularity of antispam proposals, the Court may support some form of significant regulation.

# High-Tech Solutions to a High-Tech Problem?

The most successful battle against spam is being waged through technology by large companies and ISPs. Companies can employ various filtering techniques as e-mails are received, honing in on particular phrases or patterns. Because these techniques are more simplistic than a human being's determination of whether a particular e-mail is spam, employees must constantly check that the filtering is not eliminating legitimate emails. This becomes a large job with the expanding volume of e-mail and there is a constant concern about excessive filtering. Users often report e-mails from friends and relatives are lost or signifi-

Most enforcement against unwanted commercial e-mail historically has involved misrepresentation and fraud claims.

cantly delayed as filtering processes attempt to protect users from spam.

Brightmail is an e-mail filtering company employed by MSN, AT&T, and other very large networks.
Brightmail seeks out spammers by deploying thousands of dummy e-mail addresses over the Internet to attract spammers. Its employees investigate the results and block addresses of unwanted e-mailers. Brightmail licensing is too expensive for all but the largest companies, forcing smaller companies either to dedicate employees to filtering out spam or to endure larger amounts of it.

Internet e-mail services such as Hotmail or Yahoo often use a spam-reporting feature that allows users to declare an e-mail to be spam and have the address blocked for their personal account; Hotmail or Yahoo decides whether to block the address for all users. There are, however, limits on the number of addresses that these services will block for each user. Marketing companies express frustration with this feature because recipients use it as an "unsubscribe" mechanism, thus making false (or what the marketing company thinks are false) reports of spam to the ISP.<sup>21</sup>

Blacklists are another resource that companies use to block and filter spam. Blacklist organizations collect and maintain lists of senders of spam, based on reports and their own investigations. Other companies import these lists and block the addresses on them. Companies using these lists must place a high level of trust in them; there is always the chance that the blacklist's idea of spam may not correspond to that of the user. Furthermore, spammers often keep one step ahead by constantly shifting addresses and using temporary accounts.

Whitelists are an inverse of the blacklist idea: these are lists of legitimate senders from which e-mail is automatically accepted. Because e-mail from unrecognized senders is blocked, whitelists offer a partial solution at best. Some ISPs

are considering the use of the "challenge response" to supplement whitelists.<sup>22</sup> E-mails from unrecognized senders are made to generate a response from the sender.<sup>23</sup> The sender then has to reply to the message or perform same function on a website that cannot be done by an au-

tomated program, thus verifying that the sender is a live person. Besides the obvious problems that this method poses for legitimate senders, it is not viable for companies that deal with many e-mails from new senders.

One thing is very clear from an examination of these solutions: they are expensive. They require the dedication of employees to ensure that technology is not eliminating legitimate communications.

# Prosecution for False or Misleading E-mails

Most enforcement against unwanted commercial e-mail historically has involved misrepresentation and fraud claims under common law and state and federal statutes. The FTC has restricted itself to dealing with deceptive and fraudulent e-mails under the FTC Act,

which prohibits deceptive business practices. Indeed, with the FTC estimating that at least 66 percent of e-mails contain information that is false or misleading, there is no shortage of spam to be dealt with in this way.<sup>24</sup> States have also been pursuing spammers for providing false or misleading claims and information.

The effectiveness of these prosecutions is debatable at best. In 2002, the FTC conducted an operation called "Spam Harvest" that resulted in settlements with four spammers. Considering that one person can send millions of emails in one day, the effectiveness of the FTC's actions against individual spammers is dubious. Given the continuing astronomical rise in spam, such prosecutions appear to be miserably ineffective.

# **Private Rights of Action**

Lower courts have declined to treat ISP networks as "public fora" under the First Amendment.<sup>26</sup> Thus, the First Amendment does not preclude ISPs from blocking and disabling the accounts of spammers, as ISPs are not state actors.<sup>27</sup> Companies, mainly ISPs, have begun pursuing a number of actions against spammers, winning million-dollar judgments and, more significantly, permanent injunctions.28 Most of these actions are under common law fraud, misappropriation, and misrepresentation theories as well as a number of computer-related statutes dealing with fraud and misuse of computer networks or equipment.29 These actions are time consuming and expensive, and invariably end in an injunction against only a single spammer. As a result, most ISPs deal with the problem through their own technological filtering solutions and by disabling the accounts of spammers.

Interestingly, plaintiffs have recently revived the "trespass to chattels" tort in claiming disruption and damage to their systems by large batches of e-mails. In many cases, however, damages are a difficult issue to prove, especially for large networks suing individual spammers. Because networks have upgraded their bandwidths in anticipation of heavy use, spammers are not disrupting service. In the much-anticipated case of *Intel v. Hamidi*, the California Supreme Court denied such a claim in the context of a mailing to a large network because it failed to actual damage or network dis-

ruption.<sup>31</sup> Thus, this cause of action likely will be limited to egregiously large and intentionally disruptive mailings.

# State Can-the-Spam Legislation

To date, thirty states have passed antispam statutes, primarily within most the last four years. <sup>32</sup> The states typically use a definition of spam that relies on "unsolicited commercial" e-mail. <sup>33</sup> Some states impose a "bulk" requirement, meaning that a certain number of e-mails (which can be as few as two) are required to be sent in a specified time period. <sup>34</sup> Virginia, the home state of AOL, loosely defines spam as "unsolicited bulk e-mail" and provides criminal penalties for sending it. <sup>35</sup>

State laws typically mandate a combination of requirements, including (1) truth-in-routing information, <sup>36</sup> (2) provision of an opt-out mechanism, <sup>37</sup> (3) labeling requirements, <sup>38</sup> and (4) truth-insubject lines. <sup>39</sup> The states also typically provide a framework for statutory damages per e-mail and may allow private rights of action.

# Unsolicited Commercial E-mail

The most common definition of the email subject to regulation by these statutes is e-mail whose primary purpose is to promote goods or services. The Utah statute defines "commercial" as "for the purpose of promoting the sale, lease, or exchange of goods, services, or real property,"40 and "unsolicited" as "without the recipient's express permission" except when "the sender has a preexisting business or personal relationship with the recipient."41 A preexisting business relationship is often defined as a "transaction or communication between the initiator and the recipient of a commercial electronic mail message" within some specified period of time prior to the receipt of the e-mail.42 Thus, under statutes like that in Utah, opt-out and other provisions will not apply to e-mails from senders deemed to be in a prior business relationship with the recipient.43

# Truth-in-Routing

Most statutes require that the sender of an e-mail covered by the statute not falsify the path that the e-mail took from the sender to the recipient in order to bypass filtering efforts or to otherwise legitimize the e-mail.<sup>44</sup> This is intended to prevent the use of false or stolen domain names as return addresses so that users will open the mail thinking it is from a legitimate source.

# Opt-out Mechanism

This option is standard in many commercial e-mails although it is usually not functional.45 It allows recipients to indicate that they no longer want to receive e-mails from the sender or would like to be removed from the mailing list, usually through an "unsubscribe" mechanism. The laws describing the opt-out provision are vulnerable to manipulation. Typically, the statute requires that an "entity or person" sending e-mails must stop sending them if the user reguests.46 It remains to be seen how susceptible the "entity" designation is to multiplication, enabling reuse of e-mail addresses that have opted out of previous mailings from other "entities" of the same sender.47

# Other Requirements

A state may require a mailing address, phone number, or e-mail address that remains valid in order to track the sender of the e-mail.<sup>48</sup>

Statutes typically require that some sort of tag be inserted in the subject line indicating that the message is either an advertisement or adult in nature. For example, California requires "ADV" to be appended to the subject line of commercial e-mails.<sup>49</sup>

Some state statutes require that the email to have truthful subject headings instead of a misleading heading, such as "Hey There," often used to trick recipients into thinking that it is a personal e-mail.

# Do State Laws Really Work?

Like the FTC and private prosecutions, the state laws do not seem to have dampened the tide of spam. Despite the requirements for an opt-out provision, the FTC recently found that 63 percent of return addresses for this purpose were not functional or operative.50 Similarly, despite the provisions for labeling requirements—including those of California, which contains a large percentage of Internet users, hardware, and companies—only 2 percent of spam contains the ADV label.51 However, because this entire problem is so recent, these laws may yet prove to be effective tools in fighting spam. In the current economic climate, however, states lack the resources for vigorous enforcement

of these laws, and it remains to be seen whether individual users will take advantage of small claims provisions.

Regardless of whether the state laws are enforced, there are inherent problems with a state-by-state framework. Most importantly, the anonymity and decentralization of the Internet means that individual jurisdictions may not have the resources to locate and prosecute even the most egregious spammers. Also, so-called legitimate e-mail marketers and more established companies that send out bulk e-mails are confronted with a wide variety of regulation and an almost impossible task of determining what jurisdiction a particular e-mail will go through and land in. Both vehement antispammers and traditional direct marketers have called for a national solution.

# **Federal Legislation**

The proposed federal legislation incorporates many of the features of state legislation. For example, both the CAN-SPAM Act of 2003,<sup>52</sup> proposed by Senators Burns and Wyden, and the Reduction in Distribution of Spam Act of 2003,<sup>53</sup> introduced by Representatives Burr, Tauzin, and Sensenbrenner, include requirements for opt-out provisions,<sup>54</sup> valid return e-mail addresses,<sup>55</sup> and labeling.<sup>56</sup> Both provide for criminal penalties.<sup>57</sup> Neither allows for a private right of action, although ISPs may sue spammers that send to their system or use their system to send spam.<sup>58</sup>

These bills introduce some provisions in addition to those found in current state laws:

# Electronic Harvesting

Both of these bills prohibit use of addresses that were harvested from the Internet electronically without the site owner's permission. <sup>59</sup> These addresses are harvested by programs called "bots" that trawl the Internet looking for e-mail addresses on websites, chat groups, and personal pages. These applications can collect thousands of addresses with little cost.

# Exceptions for Entity "Divisions"

The CAN-SPAM Act allows for different divisions within an entity to maintain separate lists for purposes of the opt-out mechanism.<sup>60</sup> This provision is vulnerable to significant manipulation because senders could establish innumerable different divisions and continue

spamming to those who have opted out from other divisions.

# **Detailed Opt-out Mechanisms**

Both of these bills allow the sender to request detailed questions about what type of e-mail the user wants to opt out of. This process, which can be based on products or divisions, has the potential to be confusing and deceptive. A sender can establish a bewildering array of e-mail lists based on multiple criteria so that users have little chance of removing themselves completely. At the very least, these bills will be rendered less effective in reducing spam to a particular user from a particular sender.

# Preemption

The CAN-SPAM Act has recently been modified so that it does not preempt state legislation.<sup>61</sup> Thus, legitimate electronic marketers will continue to be subjected to a vast array of different state-by-state requirements.

# Opt-in

Many consumer groups are calling for an "opt-in" provision. An opt-in provision would presumptively ban unsolicited commercial e-mail unless the user initiated contact with a marketer and requested to be put on a mailing list. This is, for the most part, the law in the European Union.62 A comprehensive bill currently pending in the California legislature would also ban unsolicited commercial e-mail unless a user had opted in or had a prior business relationship.63 This bill is by far the most ambitious proposed to this date and surpasses the existing California provision with its fairly typical labeling and optout requirements.64

To date, European users have not seen any reduction in the amount of spam that they receive. Prosecutions in Europe are, as in the United States, not comprehensive or constant, being left to individual countries. Another important reason is that most of the spam in Europe does not originate from the EU. An estimated 35 percent of spam in Germany originates in the United States, with the bulk of the rest coming from elsewhere in the world.65 With most spam outside of the range of European law enforcement agencies varying degrees of enforcement within Europe, it is hard to determine the actual effectiveness of the EU opt-in law.

Because a large percentage of Internet

users, companies, and traffic are in the United States, a fully enforced ban on spam in this country could be fairly effective. A U.S. law will, however, do nothing against spam originating outside of the country, and it is likely that foreign spam would increase in the event of a fully enforced, domestic antispam regime. But to the extent that the products and companies using spam to advertise are located in this country, e-mails being sent at their behest could presumably be regulated. Full enforcement, with dedicated funds, has not, so far, been seriously considered.

# E-mail Stamps

A novel, but surprisingly intuitive, approach to curbing spam is simply to charge the senders of e-mail a small price, likely a fraction of a centenough to provide a more equitable economic weight to sending millions of spam but not enough to cause a problem to noncommercial users of e-mail. This type of pricing system represents a drastic departure from the present system, and instituting pricing without the underlying actual costs for providing the service would suffer from the lack of a strong market foundation. Thus, competition might render such a pricing system short lived.

# "Do Not E-mail" List

This would function the same way as the FTC's "do not call" registry and similar registries in many states. 66 States or the federal government would maintain a list of e-mail addresses that have opted out of receiving e-mail from all of the entities and businesses participating in the system.

# Do These Proposals Pass Constitutional Muster?

Perhaps. One primary weakness of these proposals is in the U.S. Supreme Court's increasing skepticism of content-based distinctions between commercial and noncommercial speech. Although *Central Hudson* is still good law and thus a facial distinction between commercial and noncommercial speech is presumptively valid, the Court may be inclined to closely scrutinize the interests proffered in support of these regulations and whether they are served in light of the exceptions for noncommercial speech.

Another weakness of laws currently in the books involves labeling requirements. Given the filtering options offered by email software and ISPs, these requirements could amount to an outright blockage of most unsolicited advertising. Together with proposals for more stringent bans on e-mail marketing, such measures might raise significant questions in the Court. Because the Internet is so broad and democratic a medium, the Court has evinced strong concern with placing undue regulation on it.<sup>67</sup>

# Standard of Review

The *Central Hudson* test applies to commercial speech regarding lawful activities that is not misleading. The initial determiniation is whether the governmental interest asserted is substantial. If so, the government must show that its regulation directly and materially advances that interest and that it is no more extensive than necessary to serve the interest.

However, in many individual opinions from recent decisions, the Justices have expressed skepticism about the distinctions between commercial and noncommercial speech that are fundamental to the *Central Hudson* test. In *Lorillard Tobacco Co. v. Reilly*, Justices Kennedy, Scalia, and Thomas all openly questioned the continued use of the *Central Hudson* test.<sup>68</sup>

As the Court has grown increasingly dissatisfied with the Central Hudson approach, it has focused on the fit between speech restrictions and the proffered governmental interest.<sup>69</sup> In City of Cincinnati v. Discovery Network, Inc., the Court struck down a city ordinance that prohibited newsstands containing advertising publications but not those containing traditional newspapers.70 Although accepting the city's asserted interest in the aesthetics of the sidewalks, the Court found that the regulation was not a "reasonable fit" because both types of newsstands had the same effects; the only difference was their contents.

In the antispam context, the fact that the same governmental interests in cost reduction and cost shifting apply to noncommercial e-mails might prove problematic. The Eighth Circuit recently rejected similar objections to the ban on commercial faxes in the Telephone and Consumer Protection Act of 1991 (TCPA). The Eighth Circuit distinguished *Discovery Network*, arguing that

the distinction between commercial and noncommercial faxes is relevant to the asserted governmental interest. . . . The legislative history here shows that TCPA's distinction between commercial and noncommercial fax advertising is relevant to reducing the costs and interference associated with unwanted faxes.73

The Eighth Circuit's argument is vulnerable, however, because Discovery Network rejected the idea that the commercial newsstands could be banned simply because they were less valued. Thus, the governmental justification that a commercial fax is simply unwanted is not recognized as a strong one. The purpose of the reasonable fit qualification is to make sure that the government is not simply discriminating between speakers based on a preference for one type of content.

A more important difference noted by the Eighth Circuit is that the commercial newsstands in *Discovery Network* were a small fraction of the total, thereby casting suspicion on the effectiveness of the regulation in achieving the stated aesthetic goals. Given the Court's ad hoc approach to commercial speech, such practical differences assume importance. In the case of spam, the overwhelming majority of these e-mails are unquestionably commercial in nature, and thus restricting them specifically will achieve the stated goal of reducing spam.

Regardless of whether the Court rejects the Central Hudson standard altogether or simply circumvents it by questioning the distinction between noncommercial and commercial spam in the legislation, any exemptions for noncommercial e-mails could prove fatal. On the other hand, given the extent of the problem, and the overwhelming majority of spam that is commercial, it is quite likely that the Court would allow such distinctions.

# Constitutionality of the Various Proposals

For such universally ignored prose, spam certainly elicits the most heartfelt of human emotions. Although the typical recipient is concerned with the annovance or offensiveness of spam, the constitutional debates around spam (and junk fax legislation) do not focus on the primary motivation behind the laws. Discovery Network and the Court's First Amendment doctrine in general show us that those types of arguments are not persuasive before the U.S. Supreme Court.74 Accordingly, constitutional arguments (and this article) proceed mainly on the basis that spam is increasingly costly and that the costs are unfairly distributed.

Opt-in Provisions or Ban on Spam The TCPA, which banned unsolicited commercial faxes, presents a strong parallel to an outright ban on unsolicited commercial e-mail.75 The TCPA prohibits sending by fax an "unsolicited advertisement" by fax unless there has been an invitation or permission given.76 Two circuit courts have upheld the TCPA

against First Amendment challenges.77 A number of plaintiffs have tried to argue that the TCPA applies to unso-

licited e-mails. However, the Pennsylvania Supreme Court recently determined

that the TCPA, based on the plain meaning of the statute, could not be construed to include e-mails.78 It seems fairly clear that the U.S. Supreme Court would agree, given the wording of the TCPA, which clearly contemplates telephone and fax advertising only.79 While the TCPA does not apply directly to e-mails, an analogy to the TCPA is appropriate, albeit with several complications.

First of all, the Court analyzes each new communications medium on its own terms.80 The parallels to faxes are mixed. The circuit courts justified the TCPA on two primary grounds: one was that a fax coming in would occupy the line and prevent legitimate business activities, and the second was that unsolicited faxes shifted the costs of advertising to the recipient, forcing it to incur paper and toner charges.81

In contrast, e-mail does not block the Internet connection, at least for business users and those with personal accounts with large storage. Smaller users of free Internet accounts, however, may find their inboxes shut off by a large batch of spam and legitimate e-mails returned to the sender. A user of free Internet accounts can also hold multiple accounts, restrict the use of some of them, and reserve access to them for only trusted sources.

The second parallel to the TCPA is stronger; large volumes of e-mail do shift the cost of advertising to the consumer. The marginal cost of sending another e-mail from a free Internet account is negligible to the spammer; millions can be sent as easily as one.

However, each of those e-mails reguires the ISP to acquire increased bandwidth, filtering technology, and dedicated employees, all of which are paid for by the recipient. Nevertheless, it is unlikely that the Court will recognize a direct parallel with faxes in upholding an opt-in provision for unsolicited e-mails, despite the apparent strength the cost-shifting argument.

While the TCPA does not apply directly to e-mails, an analogy to the TCPA is appropriate.

> Another consideration with an outright ban is that it effectively eliminates solicitation. In Edenfield v. Fane, the Court opined:

In the commercial context, solicitation may have considerable value. Unlike many other forms of commercial expression, solicitation allows direct and spontaneous communication between buyer and seller. A seller has a strong financial incentive to educate the market and stimulate demand for his product or service, so solicitation produces more personal interchange between buyer and seller than would occur if only buyers were permitted to initiate contact.82

The Court is likely to carefully balance the problems of cost shifting and productivity loss with this consideration.

In this case, solicitation must also be balanced with the overall utility of the medium. Despite the fact that the Court is unlikely to allow the Internet to be regulated as restrictively as the broadcast media, 83 a comparison to broadcast media would be relevant to arguments that the volume of spam is pushing legitimate commerce out of the marketplace. Given the remarkable statistics, this could be seen as a strong argument in favor of regulating spam. The Court has, however, recognized that the Internet is not an expensive or scarce medium.84 Unlike the original version of the argument, there is no danger that legitimate commerce will be shut out of the Internet as was the case with finite broadcast frequencies.

Nevertheless, it is easy to extend the argument that with enough spam, the medium itself will be rendered unusable and thus legitimate commerce will be

shut down. In a case upholding a ban on automatic telephone dialers in political campaigns, the Eighth Circuit recognized the problem that the power of technology can have on personal lives; the dialers were "becoming a recurring nuisance by virtue of their quantity." 85

Arguments in defense of legitimate commerce can be made the other way as well. A sweeping ban against Internet advertisers would also block e-mails from legitimate marketers—an incongruous situation in view of the fact that we allow handbills, flyers, and junk mail. If solicitation is effectively stopped on the Internet, a medium only growing in importance, the Court will certainly look at the options left to marketers when it applies the "reasonable fit" test of Central Hudson. The Court would likely find that a total ban suppresses more speech than necessary when the asserted governmental interest is saving money for companies and consumers.

The Court would likely consider an opt-out regime and labeling requirements as viable alternatives to an outright ban. One option that the Court is also sure to look at is the adequacy of current laws. The FTC Act, common law, and other statutes presumably prohibit false, deceptive, and misleading e-mail. <sup>86</sup> If the FTC is correct in estimating that two-thirds of spam falls in this category, <sup>87</sup> adequate enforcement of existing laws would address much of the problem.

# **Labeling Requirements**

By instituting requirements for subject lines, the government may face arguments relating to compulsory speech. While most of the cases involving compulsory speech involve areas of speech traditionally recognized as fully protected,88 in Pacific Gas & Electric v. Public Utilities Commission, the Court did strike down a government agency requirement that an electric utility include messages from an opposing consumer group on its envelopes.89 The type of labeling at issue here is, on its face, less burdensome than the requirement in Pacific Gas & Electric, but these laws would still require senders to include speech that directly counters their interests. This requirement resists comparisons to warning labels, which have been upheld, because the item is not dangerous.

Another strong constitutional argument against the labeling requirements

exists because of the way technology can use the labels. The function of a requirement like this is not far from a total ban on spam, as users can simply filter out messages with ADV in the subject heading. Thus, the Court may be persuaded by arguments that this requirement could effectively shut down solicitation by e-mail.

There is, however, one admittedly obvious, yet potentially important, distinction: the user, in the case of labeling requirements, is making the decision to get rid of the e-mail after having had the opportunity to receive it. Furthermore, there may be a significant portion of the population who elect not to filter out spam; the choice is left to them. But given the all-or-nothing approach, if the problem continues to escalate, most people will have little choice but to filter out spam on accounts that they check frequently.

Courts have upheld labeling requirements for attorney advertisements, and such requirements are present in the professional rules of a number of states.90 The U.S. Supreme Court has recognized in dicta that a "lawyer could be required to stamp 'This Is an Advertisement' on the envelope."91 The Court's discussions of labeling requirements have arisen only in the context of professional advertising and with implicit or explicit assumptions that there is a strong danger of the recipients being misled by sophisticated and targeted appeals. The Court balances the rights of professionals to advertise the governmental interest against fraud.

In the case of spam, there is little danger that an unsophisticated public is not prepared or informed enough to decipher the claims of spam. The governmental interest behind instituting a labeling requirement is in allowing recipients to be pre-informed of the content of the message so that they do not have to take the time to open the message and read it. Because there is little preexisting danger of deception, which was implicit in the Court's discussions of labeling requirements in professional advertising, the Court is not likely to extend the analogy to spam.

# **Opt-out Provision**

In *Rowan v. U.S. Post Office Dep't*, the Court upheld a system under which consumers were allowed to sign up at the post office to stop receiving junk

mail from a particular sender.92 Thus, an opt-out requirement is not likely to pose a significant constitutional issue. An opt-out regime that had some significant structure would also be a viable alternative to an outright ban or to labeling requirements. This provision would allow initial solicitations. An opt-out system is flexible, offering considerable leeway in enforcement. The more closely the definitions of "sender," "business division," and "prior business relationship" are restricted, the closer we will be to achieving the desires of users, but also to shutting down the media for a large body of advertisers. To the extent that the laws regarding the administration of the e-mail lists of all the e-mail marketers were uniformly enforced and predictable, the Court would likely find that consumer and business needs could be balanced with that of advertisers. This would only occur, of course, if a significant governmental effort was devoted to maintaining and enforcing an opt-out system.

# "Do Not E-mail" List

If, as expected, the current round of legislation or its enforcement proves ineffective in reducing spam, a national "do not e-mail" list with an exhaustive list of commercial entities will probably be proposed, especially if the FTC's "do not call" list for telephone marketers survives court challenges.93 A "do not email" list would seriously reduce solicitation by e-mail. Surely any exceptions or exemptions included in this list that discriminate based on lines of business or any other quality particular to the sender would be vulnerable to challenge. However, the fact remains that a "do not e-mail" list, like an opt-out requirement, or filtering by recipients based on the "ADV" subject heading, still involves a choice by recipients. Furthermore, if indeed some of the current legislation is passed and remains ineffective, there will be a strong argument that this solution is not overly restrictive and is, in fact, the least restrictive method available to save the medium.

# **Prior Business Relationship**

The proposed legislation exempts e-mails if the recipient has had a prior business relationship with the sender. Defined with varying time provisions, these exemptions are problematic because of the Court's regard for the value of initial solicitation and

its concern for smaller and newer players.94 In Martin v. Struthers, the Court concluded that "door to door distribution of circulars is essential to the poorly financed causes of little people."95 To the extent that the definitions of the relationship are relaxed, more established companies and marketers will be allowed to continue sending e-mails without labeling requirements—although many might continue their current practice of providing clear subject headings and valid opt-out mechanisms. Under a regime with a labeling requirement, if more established marketers are allowed significant leeway in avoiding the requirement and getting their e-mails beyond the filters, they may obtain a significant business advantage over smaller, newer competitors.

# **Electronic Harvesting**

The courts have been willing to entertain private rights of action based on trespass for use of "bots."96 Although ultimate level of judicial recognition of this cause of action is still not decided, courts have recognized that these applications can use significant computing power of the website that they are combing over and thus shift costs to others. If courts recognize these applications as a significant intrusion on property rights, this justification alone may demonstrate a strong enough governmental interest to justify restricting them. In Red Lion Broadcasting Co. v. FCC, the Court justified a higher level of regulation for broadcast media based on the limited number of airwaves and the potential for the medium to be rendered useless by their monopolization. Similarly, if electronic harvesting is left unregulated, the resulting spam and the slower server times may lead to a significant impairment of the medium.

In EBay v. Bidder's Edge, the defendant trawled the plaintiff's online auction site daily, culling data for display on its own site. The court rejected the defendant's argument that it was simply using the website like another member of the public, concluding that the defendant had exceeded the scope of a limited license that EBay gave to the public to use its servers. Extending this argument to the Internet as a whole may be problematic, given the high degree of protection that the Court seems willing to give the Internet.

Moreover, these provisions are not content-neutral. Google and other

Internet search engines also use bots to provide results. Their activities could cause a similar slowing of servers and response times, but would be allowed. If the Court applies the Central Hudson test rigidly, the exception of these businesses from the bots restrictions may be unreasonable given a proffered interest of preventing slowdowns in server response times and hardware costs. Here, the distinction drawn is not that between commercial and noncommercial but between commercial actors based on the activities of their business. This may prove to be a more problematic set of distinctions. But the Court may be willing to accept the more general governmental interest of reducing spam in upholding these provisions, because entities like Google do not spam and because the provisions only prohibit using the botharvested addresses to send spam and do not prohibit using the bots themselves.

The interest at stake here, gathering large volumes of e-mail addresses, is not likely to be taken as an activity deserving serious First Amendment protection.98 No matter how much the Court values this activity, these laws do not actually bar collecting and spamming addresses harvested from the web; in the event electronic harvesting is barred, a company may still employ people to search manually for e-mail addresses. Coming full circle to Van Bergen v. State of Minnesota, where the Eighth Circuit upheld restrictions on automated dialers, courts do understand the power of technology to exceed the scope of tolerance for activities that would be legal if a person does them.

# Return Address and Truth-in-Routing

There may be a potential constitutional argument that these provisions violate the Court's protections of anonymous speech. However, the cases where the Court has protected the anonymity of speakers arose outside the area of commercial speech.99 As fraud and misrepresentation are standard justifications for the decreased First Amendment protection of commercial speech,100 and allowing the consumer to find further information about the other party in a proposed commercial transaction seems clearly related to the goals of reducing fraud, the Court is not likely to extend anonymous speech protection to commercial speech.

# Federal Regulation and Possible Supreme Court Reaction

Of all the predictions one can make about spam, a safe bet is that there will soon be some type of federal regulation of bulk email. Further, although the U.S. Supreme Court has been increasingly protective of commercial speech, proponents of regulation believe that the problem is so pressing that some type of effective regulation will likely be allowed. Given the acceptance so far of the TCPA by the courts, it seems possible that the Court will support a significant degree of restrictions short of a total ban. However, the Court is likely to look very closely at any regulatory framework. Exemptions for prior business relationships and noncommercial e-mails will have to be strongly supported. Finally, unless a significant degree of resources are devoted to enforcement of these laws, they are not likely to be effective because of the ease and anonymity of spamming technology.

# **Endnotes**

- 1. 123 S. Ct. 2554 (2003).
- 2. See, e.g., Trans Union LLC v. FTC, 536 U.S. 915 (2002) (dissent from denial of certiorari by Kennedy, J., joined by O'Connor, J.); see also Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 571–72 (2001) (Kennedy, J., concurring in part and concurring in the judgment, joined by Scalia, J.); id. at 572 (Thomas, J., concurring in part and concurring in the judgment).
  - 3. 447 U.S. 557, 566 (1980).
  - 4. *Id.* at 566.
- 5. Thompson v. W. States Med. Ctr., 122 S. Ct. 1497 (2002); see also *Lorillard Tobacco Co.*, 533 U.S. at 525; Greater New Orleans Broad. Ass'n v. United States, 527 U.S. 173 (1999).
- 6. Associated Press, Lawmakers and Technology Industry Call for National Law to Control Junk E-mail (May 21, 2003), *available at* www.bayarea.com/mld/mercurynews/business/5913848.htm.
  - 7. *Id*.
  - 8. *Id*.
- 9. Hearing on Spam (Unsolicited Commercial E-Mail) Before the Senate Committee on Commerce, Science and Transportation, 108th Cong., 1st Sess. (May 21, 2003) (statement of Marc Rotenberg, Executive Director of Electronic Privacy Information Center), available at www.epic.org/privacy/junk\_mail/spam/testimony5.21.03.html.
  - 10. *Id*.
  - 11. *Id*.
  - 12. *Id*.
- 13. Chris Taylor, *Spam's Big Bang*, TIME, June 16, 2003, at 52.
  - 14. *Id*.
  - 15. For example, aaaaaa@aaa.com,

- aaaaaa@aab.com, aaaaaa@aac.com, etc.
- 16. Lawmakers and Technology Industry Call, *supra* note 6.
- 17. See a state-by-state summary of spam laws and copies of individual statutes at www.spamlaws.com/state/index.html.
- 18. Marianne Kolbasuk McGee, *Schumer: Consumers Favor No-Spam Registry*, INFO. WK., July 24, 2003, *at* www.informationweek.com.
- 19. As it evolves through Congress, the proposed federal legislation is responding to increasing dissatisfaction with spam with stronger provisions. *See, e.g.,* CAN-SPAM Act of 2003, S. 877, 108th Cong. (originally exempted all further e-mails from a sender from its opt-out and labeling provisions if the user had forgotten to opt out of the initial e-mail); *see also* Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong; REDUCE Spam Act of 2003, H.R. 1933, 108th Cong.
  - 20. See Rotenberg statement, supra note 9.
- 21. Brian Morissey, *AOL Claims Progress in Spam War*, Internetnews.com (Feb. 1, 2003), *at* www.Internetnews.com/ IAR/article.php/1593831 (good summary of technological filtering approaches).
- 22. Earthlink, the nation's third largest Internet provider, is in the testing phase of a challenge-response system. If users respond positively, it is likely to be followed. See Jonathan Krim, EarthLink to Offer Anti-Spam E-Mail System (May 6, 2003), available at www.washingtonpost.com.
- 23. Consumer software is also available for the individual user to set up a challenge-response system. *See, e.g.*, Hal Plotkin, *Not a Moment Too Soon: Digiportal's Innovative New Choice-mail Program Means the End of Spam* (July 30, 2002), available at www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2002/07/30/choicem.DTL.
- 24. Federal Trade Commission, False Claims in Spam 3 (2003), *available at* www. ftc.gov/reports/spam/030429spamreport.pdf.
- 25. Press Release, Federal Trade Commission, Federal, State, and Local Law Enforcers Tackle Deceptive Spam and Internet Scams (Nov. 13, 2002), available at www.ftc.gov/opa/2002/11/netforce.htm.
- 26. See, e.g., Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996); see also CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).
  - 27 Id
- 28. For an engaging account of Earthlink's pursuit of a notorious spammer, see Julia Angwin, *Hunting Buffalo: Elusive Spammer Sends Web Service on a Long Chase*, WALL St. J., May 7, 2003, at A1.
- 29. For example, in the aforementioned case involving AOL and Cyber Promotions, AOL filed a complaint alleging false designation of origin, trade name infringement, trade name dilution, false advertising, unfair

- competition, and violations of the Virginia Consumer Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Virginia Computer Crimes Act.
- 30. See, e.g., EBay v. Bidder's Edge, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); see also Intel Corp. v. Hamidi, S103781, 2003 Ca. LEXIS 4205 (Cal. June 30, 2003).
  - 31. Hamidi, 2033 Ca. LEXIS 4205, at \*1.
- 32. To see a list of states that have passed spam legislation, see www.spamlaws.com/state/index.html.
- 33. See, e.g., Colo. Rev. Stat. § 6–2.5–102 (5); see also Me. Rev. Stat. tit. 10, § 1497 (1) (c); N.C. Gen. Stat. § 14–453.
  - 34. See, e.g., Idaho Code  $\S$  48–603Е (а).
  - 35. VA. CODE ANN. § 18.2–152.3:1.
- 36. See, e.g., Colo. Rev. Stat. § 6–2.5–103 (1).
  - 37. See, e.g., id. § 6–2.5–103 (5).
- 38. *See*, *e.g.*, Cal. Bus. & Prof. Code § 17538.4 (g).
- 39. See, e.g., 815 ILL. COMP. STAT. 511/10–10 (a).
  - 40. Utah Code Ann. § 13–36–102 (1).
  - 41. *Id.* § 13–36–102 (8).
- 42. ARK. CODE ANN. § 4–88–602 (10). The Utah Code does not define what a "preexisting business relationship" is. The version of the CAN-SPAM Act that emerged on June 19, 2003, from the Senate Commerce Committee included a clarification that a "preexisting business relationship" was not formed by a mere visit to a website.
- 43. California's current law, CAL. Bus. & PROF. CODE § 17538.4, is one example of another spam statute that covers only unsolicited e-mail. For an elucidating discussion of the effects of exceptions for prior business relationships, see Gilman v. Sprint Communications Co., No. 020406640 (Utah 3d Dist. Salt Lake County Feb. 28, 2003) (holding that a company with a prior business relationship is not bound to provide an opt-out mechanism and noting that the Utah statute did not provide a mechanism to disenroll from a prior business relationship). It is unfortunate, from the perspective of this article, that the litigants in Gilman did not contest the issue of whether there was, in fact, a "preexisting business relationship."
- 44. *See*, *e.g.*, Colo. Rev. Stat. § 6–2.5–103 (1).
- 45. Federal Trade Commission, *Fact Sheet on "Remove Me" Surf Results, at* www.ftc.gov/bcp/conline/edcams/spam/pubs/removeme.ppt.
- 46. See, e.g., Cal. Bus. & Prof. Code § 17538.4 (a).
- 47. This problem is more explicit in the exception for "divisions" of a sender contained in the CAN-SPAM Act, discussed below in the section entitled "Proposed Federal Legislation." CAN-SPAM Act, § 3(9).
- 48. *See*, *e.g.*, Cal. Bus. & Prof. Code § 17538.4 (b).

- 49. Id. § 17538.4 (g).
- 50. FTC Fact Sheet, supra note 45.
- 51. Press Release, Federal Trade Commission, FTC Measures False Claims Inherent in Random Spam (Apr. 29, 2003), *available at* www.ftc.gov/opa/2003/04/spamrpt.htm.
- 52. CAN-SPAM Act of 2003, S. 877, 108th Cong.
- 53. Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong.
- 54. S. 877, § 5 (a)(3); H.R. 2214, § 101 (a)(1).
- 55. S. 877, § 5 (a)(3); H.R. 2214, § 101 (a)(1)(c).
- 56. S. 877, § 5 (a)(5)(a); H.R. 2214, § 101 (a)(1)(a). Neither of these bills specify what and where the "conspicuous" label should be. If this decision is left to the sender, the user may find that filtering is more difficult.
  - 57. S. 877, § 4; H.R. 2214, § 201(a).
  - 58. S. 877, § 6(f); H.R. 2214, § 102.
  - 59. S. 877, § 5(b); H.R. 2214, § 101(d).
- $60. S. 877, \S 3(9).$  Author: Please verify citation.
  - 61. Author: Please verify citation.
- 62. For an exhaustive compilation of European spam laws and other European spam-related legal information, see www.spamlaws.com/eu.html.
- 63. California S.B. 12, § 17529 (as amended 6/10/03), *available at* http://info.sen.ca.gov/pub/bill/sen/sb\_0001-0050/sb\_12\_bill\_20030610\_amended\_asm.h tml.
  - 64. Cal. Bus. & Prof. Code § 17538.4.
- 65. Associated Press, Europe Imports an American Problem: Spam (June 1, 2003), available at
- http://edition.cnn.com/2003/TECH/Internet/06/01/american.spam.ap/.
- 66. See 16 C.F.R. § 310.4(b)(1)(iii)(B) (FTC Do-Not-Call Registry). See also N.Y. GEN. BUS. LAW § 399-z; FLA. STAT. § 501.059(3)(a); 815 ILL. COMP. STAT. 413/15(b)(3).
  - 67. Reno v. ACLU, 521 U.S. 844 (1997).
- 68. Central Hudson Gas & Electric v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980).
- 69. See, e.g., Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 571–72 (2001); see also City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993).
  - 70. Discovery Network, 507 U.S. at 410.
- 71. See, e.g., Greater New Orleans Broad. Ass'n v. United States, 527 U.S. 173 (1999).
- 72. Missouri v. Am. Blast Fax, Inc. 323 F.3d 649 (Mar. 21, 2003). *See also* Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995) (also upheld TPCA).
  - 73. Am. Blast Fax, 323 F.3d at 655.
- 74. See, e.g., Terminello v. Chicago, 337 U.S. 1 (1949) (where the Court dispensed with the notion that, except for prohibited categories of speech, the subjective view of a particular audience about the content of speech could play any serious role in its reg-

ulation).

75. 47 U.S.C. § 227.

76. Id.

77. *Am. Blast Fax*, 323 F.3d at 655; *Destination Ventures*, 46 F.3d at 54.

78. Aronson v. Bright-Teeth Now, L.L.C., 824 A.2d 320 (Pa. Super. Ct. 2003).

79. 47 U.S.C. § 227 (b)(1)(c).

80. Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969).

- 81. See Am. Blast Fax, 323 F.3d at 649.
- 82. Edenfield v. Fane, 507 U.S. 761, 766 (1992).
- 83. See ACLU v. Reno, 521 U.S. 844 (1997).

84. Id.

85. Van Bergen v. State of Minnesota, 59 F.3d 1541, 1555 (8th Cir. 1995). In Van Bergen, the Eighth Circuit cited Breard v. Alexandria, 341 U.S. 622 (1951), in which the U.S. Supreme Court upheld an ordinance permitting door-to-door commercial solicitations only with prior consent of the householder partly based on the justification that increasing housing density had made these calls a much more frequent nuisance. Breard was, however, decided before the Court had begun giving commercial speech First Amendment protection in Bigelow v. Virginia, 421 U.S. 809 (1975), and in Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

86. 15 U.S.C. § 45.

- 87. FALSE CLAIMS IN SPAM, *supra* note 24.
- 88. See, e.g., W. Va. State Bd. of Ed. v. Barnette, 319 U.S. 624 (1943) (striking down compulsory recital of the Pledge of Allegiance).
- 89. Pacific Gas & Electric Co. v. Public Utilities Comm'n, 475 U.S. 1 (1986).
- 90. State Bar Rules, V.T.C.A., Government Code Title 2, Subtitle G App., Art. 10, § 9, Rules of Prof.Conduct, Rule 7.05(b)(2).
- 91. In Re R.M.J, 455 U.S. 191, 206 n.20 (1982) (suggesting that the labeling would be used to prevent fear in receiving an unannounced letter from a lawyer); see also Shapero v. Kentucky Bar Ass'n, 486 U.S. 466 (1988) (suggesting that targeted solicitation letters specific to their recipients could be required to bear a label identifying them as advertisements).
- 92. Rowan v. U.S. Post Office Dep't, 397 U.S. 728 (1970).
- 93. The challenges to the FTC registry have focused on the availability of less restrictive means, the numerous exceptions for various lines of business that do not have to register, and the insufficiency of privacy as a substantial governmental interest. The analysis for e-mail would differ in that the interest asserted is primarily the cost of unwanted e-mail as opposed to privacy. Privacy is a less straightforward interest to prove in that the damage cannot be reduced to dollars-and-cents figures.

94. Discussing attorney advertising in *Bates v. State Bar of Arizona*, 433 U.S. 350, 378 (1977), the Court noted that "in the absence of advertising, an attorney must rely on his contacts with the community to generate a flow of business. In view of the time necessary to develop such contacts, the ban in fact serves to perpetuate the market position of established attorneys." In a large, anonymous national marketplace, there is little potential for community contacts so the very livelihood of some of these senders depends on spam.

95. Martin v. Struthers, 319 U.S. 141, 144–46 (1943).

96. EBay v. Biddder's Edge, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

97. Id.

98. Although speaker and content-based distinctions are traditionally abhorrent to the Court, much of the Court's analysis often depends on the potential value of the activity in question. In door-to-door solicitation cases, the Court has characterized this line of its jurisprudence as discussing "extensively the his-

torical importance of door-to-door canvassing and pamphleteering as vehicles for the dissemination of ideas." Watchtower & Bible Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 161 (2002). In the case of bots, the same historical and cultural value is difficult to place on automated collection of e-mail addresses for purposes of mass advertising—especially when it is still legal to e-mail using manually collected addresses.

99. See, e.g., Talley v. California, 362 U.S. 60 (1960) (where the speech in question was handbills urging protest against alleged employment discrimination); see also McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (leaflets urging voting against a school levy).

100. See, e.g., Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 576 (2001) (Thomas, J., concurring) (maintaining that restrictions or mandatory inclusions in commercial speech are "limited to the peculiarly commercial harms that commercial speech can threaten—i.e., the risk of deceptive or misleading advertising").

# SIGN ME UP

☐ <b>I'm a lawyer</b> Annual dues in the Forum on Communications Law are \$45. Membership dues in the Association, its Sections, Divisions, and Committees are not deductible as charitable contributions for federal income tax purposes. However, such dues may be deductible as a business expense.				
The Forum publishes a newsletter, <i>Communications Lawyer</i> , and an annual membership directory, and sponsors one or more programs per year, as well as a breakfast for its members during the ABA Annual Meeting.				
ABA Sections of which I am a member:				
☐ I'm not a member of the ABA. Please send membership information.				
Please make your check payable to the American Bar Association. Lawyers should return this form to the Forum on Communications Law, American Bar Association, 750 North Lake Shore Drive, Chicago, Illinois 60611-4497.				
☐ <b>So I'm </b> <i>not</i> <b>a lawyer</b> Nonlawyers interested in issues that involve the law and the media can receive <i>Communications Lawyer</i> four times a year. A one-year subscription costs \$45.				
Name				
Firm				
Address				
City/State/Zip				

# New Federal Health Privacy Protections: A Prescription for Diminished Access?

AMY LEVINE

Gains in personal privacy often come at the expense of the First Amendment. As legal protections allow more information to be kept private, the press and the public that the First Amendment serves tend to have access to less information. This tendency is often increased if the law provides penalties for violating privacy rights. The threat of penalties creates a "chilling effect," in that those in charge of protected data may be overly conservative about revealing information that should be publicly available for fear of violating the law and being subject to damages, fines, or employment penalties.

The first federal law to protect patient privacy may be creating just such a chilling effect in the crucially important field of health and medical reporting. The Department of Health and Human Services (HHS) regulations implementing the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)1 went into effect on April 14, 2003, and journalists around the country have encountered new obstacles to obtaining information on newsworthy issues surrounding health care. For example, some photojournalists have been told by health care providers or hospitals that, under HIPAA, they must prevent photographers from taking pictures of patients' faces, whether the patient is being treated in a facility or by a rescue squad in the field.<sup>2</sup> Although HIPAA does require health care providers to take steps to protect patients' health information (including their pictures), this is just one example of an overreaction to HIPAA's requirements.

Given these types of reactions by health care providers to the new privacy rule, journalists and the lawyers who represent them may wish to have a brief primer on exactly what HIPAA provides.

Amy Levine (alevine@cov.com) practices in the media law group of Covington & Burling in Washington, D.C. She thanks her colleagues Anna Kraus and Emily Hancock, who practice in the health care and privacy areas, for their assistance with this article.

This article attempts to answer the most important questions raised by the regulations implementing HIPAA. Familiarity with what the law actually requires should permit journalists to more effectively work with hospitals and health care providers to ensure that the flow of information relating to health issues is not overly constricted by HIPAA.

# Who Is Covered?

HIPAA directly regulates health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with certain transactions, such as processing health care claims or determining eligibility for benefits. HIPAA indirectly applies to companies that perform certain functions on behalf of, or provide certain services (e.g., accounting or legal services) to, covered entities pursuant to a business associate agreement.<sup>3</sup> Importantly, journalists are not covered entities and are not required to comply with HIPAA.

# What Information Is Protected?

HIPAA regulates covered entities' use of protected health information (PHI), which includes information that relates to an individual's health or that identifies the individual.<sup>4</sup> For example, PHI includes an individual's name, address, full-face photographic images, birth date, and Social Security number. PHI does not include health information from which all individually identifying information has been removed.<sup>5</sup> Examples of this type of information, which should remain accessible, are aggregate statistics about the number of individuals with a particular illness.

# Are Journalists Liable?

Journalists do not appear to be liable under HIPAA for the use or disclosure of any health information. It is a crime, however, for health plans, hospitals, or other health care providers to knowingly violate HIPAA's provisions. Violators can be fined up to \$250,000

and jailed for up to ten years.6

Because of the way HIPAA is written, it is possible that some health plans, hospitals, or doctors may believe that HIPAA imposes fines and penalties on any individual, including a journalist, who violates its provisions. But it is much more likely that the language of HIPAA's criminal penalty provision applies only to health plans, hospitals, or other health care providers. This interpretation is supported by HHS's interim final rule on HIPAA's civil monetary penalty provision. The interim rule states that civil monetary penalties are to be imposed only on covered entities such as health plans, hospitals, or other health care providers because HIPAA applies only to these entities. While the civil monetary penalty and criminal penalty provisions reside in different sections of HIPAA, both sections contain similar language concerning applicability, which means that neither provision appears to hold noncovered entities, such as journalists, liable.

The best interpretation, then, is that journalists should not face liability under HIPAA for disclosing an individual's health information. This conclusion is tentative, however, pending HHS's publication of a rule on the criminal penalties for wrongful disclosures of health information. Of course, any disclosure of sensitive personal information can be the subject of legal liability under other causes of action under state law—particularly invasion of privacy.

# What Can Be Disclosed?

HIPAA imposes several restrictions on how, when, for what purpose, and to whom health plans, hospitals, or other health care providers may use and disclose certain types of health information. Of the permitted disclosures, those most likely to be relevant to journalists include:

Patient Condition/Facility Directory Information. Under HIPAA, journalists may be given access to a patient's name, location, and condition as long as the patient has not objected to the release of

such information. If a patient is unconscious or otherwise unable to decide whether to object to such a disclosure, a doctor or other health care provider may make such a decision based on what is believed to be in the patient's best interests.

For example, unless a patient objects, a hospital may list the above information in a facility directory that would be accessible to any person, including a journalist. Similarly, if a journalist (or any person) asks about the patient by name (a HIPAA requirement), a hospital or doctor may, but is not required to, disclose the above information. In cases where a journalist is covering the story of a person who has been critically injured and the person is unconscious or otherwise incapacitated, hospitals and doctors likely will be reluctant to share the pa-

tient's information because the patient may later allege that the hospital or doctor was wrong not to object to such a disclosure on the patient's behalf.

Information About Deceased Individuals. Hospitals, doctors, or other health care providers may disclose health information about deceased patients to law enforcement officials, coroners, medical examiners, and funeral directors. Because HIPAA does not apply to these third parties, they may make further disclosures of any health information that they receive. This means that journalists can, under HIPAA, obtain health information about decedents from third parties.

*Information from Whistleblowers.* If a whistleblower were to disclose health information to a journalist, the whistle-

blower's employer (e.g., a hospital, health plan, or other covered entity) could be found to have violated HIPAA. However, the journalist would face no liability under HIPAA for receiving health information from the whistleblower.

Public Health or Safety Threats. A covered entity may disclose health information to members of the press in order to alert the public to a health threat or to pass along information to help keep members of the public safe.

Incidental Disclosures. A journalist may use health information gathered as a result of an incidental disclosure by a health care provider. For example, a journalist might learn a patient's name by listening when a nurse calls out patients' names in a waiting room or might learn about a patient's condition

# A REPORTER'S GUIDE TO HEALTH PRIVACY

This quick reference guide lists the top five areas of the new federal health information privacy law—the Health Insurance Portability and Accountability Act, or HIPAA—that will affect journalists' ability to obtain health-related information about individuals and to photograph hospital or other patients. Various state laws, which may also have an impact on patient privacy, are not covered in this brief guide.

**HIPAA does not apply to journalists.** The Act does not restrict journalists or photographers from, or hold journalists criminally liable for, gathering, using, or disclosing individuals' health information. Some hospitals have indicated that journalists could be fined or jailed for HIPAA violations, but this interpretation of the statute is incorrect.

HIPAA generally restricts health care providers from sharing information. Hospitals, doctors, clinics, health plans, and other "covered entities" under HIPAA are generally barred from sharing health information that identifies an individual, including the person's name, Social Security number, photograph, address, prescription number, or birth date. In some cases, as noted below, health care providers are permitted to disclose health information. But it is possible that, for fear of potential legal liability, health care providers will interpret HIPAA conservatively and restrict more information than is necessary.

# Health care providers may share some health information:

- Aggregate health information. For example, a hospital or doctor could tell a journalist how many people have a certain illness in a specific area.
- *Public health information*. Hospitals or doctors are allowed to disclose health information to journalists to alert the public to health threats.
- Patient condition information. A health care provider—most likely a doctor or hospital—may disclose a patient's name, location, and condition if such information is in the form of a facility directory listing. Additionally, if a patient's name is known, a health care provider may disclose that patient's location or condition upon request. However, a patient, or a doctor or hospital on behalf of an incapacitated patient receiving treatment, may prevent this disclosure.

# Other permissible ways of learning about someone's health information:

- A journalist is not restricted from using or disclosing health information that is legally obtained through informal channels (in the course of overhearing a discussion, for example).
- HIPAA does not apply to law enforcement officials, coroners, medical examiners, or funeral directors (or any other individuals who do not qualify as "covered entities"). These individuals may share with a journalist health information that they have received from a doctor or hospital.
- Individuals may give a health care provider written permission to disclose their health information to the media, or they
  may communicate with a journalist directly.

**Photographs.** Hospitals have no right to restrict photographers from taking pictures when they are on public property, even when the patient is located on a health care facility's property. Hospitals may restrict the ability of photographers to take pictures within a hospital but, again, photographers would not be held liable under HIPAA for doing so.

by overhearing the conversation of two emergency room doctors. The doctors, hospital, or other health care providers in such situations would not be held liable for the disclosure as long as reasonable safeguards were in place to prevent such incidental disclosures.<sup>7</sup>

# Is a Picture Worth a 1,000 Words?

HIPAA does not apply to photojournalists, so a photographer will not be liable for taking a patient's picture regardless of where the patient or photographer is located when the picture is taken. Again, state tort law for invasion of privacy or trespass may apply. Although HIPAA does not give hospitals or health care providers greater rights to prevent photographers from taking pictures of patients in their facilities than the hospitals or health care providers possessed prior to HIPAA's effective date, HIPAA does create a standard of care for hospitals and health care providers: they must reasonably protect patients' health information, including individually identifying photographs, from disclosure. As a result, hospitals likely will institute policies restricting photographers from taking pictures of patients without their consent.

Such a hospital policy, however, will not be effective in preventing photographers who are located on public property from taking photographs of patients. For example, if a photographer is across the street from an emergency room entrance and is attempting to photograph a patient who is being wheeled into the hospital, the hospital can take steps to shield the patient from the camera lens, but the hospital is not empowered by HIPAA to prevent the photographer from taking the photograph. Similarly, if a photographer at an accident scene is trying to take a picture of a victim who is being treated by paramedics, the paramedics may take whatever reasonable steps they may have taken prior to HIPAA to protect the patient's privacy, but HIPAA itself does not provide any free-standing right for such health care professionals to attempt to prevent the photographer from taking the picture.<sup>8</sup>

# What About General Health Information?

HIPAA permits the disclosure of information that is not personally identifiable (i.e., health information with a list of eighteen specific "direct identifiers" removed), and journalists can gather aggregate data, such as the number of people with certain health conditions or health plan enrollment statistics. In the case of a mass accident, hospitals generally may release the number of patients treated, their genders and age groups, and nonpatient-specific information on medical condition. HIPAA also allows the disclosure of somewhat more detailed aggregate data under a so-called limited data set mechanism, which requires that the recipient sign a data use agreement. But it is highly unlikely that health care providers and journalists will enter such agreements, particularly because HHS has commented that the purposes of limited data sets and the restrictions contained in data use agreements are at odds with journalists' need for access to patient information.

# Can Individuals Restrict Information Allowable Under HIPAA?

Yes. Even if health plans, hospitals, or doctors are permitted to disclose health information under HIPAA, in certain situations people may request that the use of their health information for certain purposes be restricted. Such health care entities are not required to agree to the restriction, but if they do agree, then they are bound by such an agreement. Thus, agreed-to restrictions may have the effect of limiting, in some situations, the health information that a journalist may be able to uncover.

Journalists do not appear to face potential liability under HIPAA or its implementing rules for the use or disclosure of health information. Journalists may, however, encounter increased obstacles to accessing information about patients, such as crime or accident victims, due to the

restrictions that HIPAA places on covered entities and due to the likelihood that covered entities—and perhaps even noncovered entities who may deal with health information, such as members of law enforcement—will misunderstand HIPAA's requirements or will refuse to disclose information even when it is permitted to avoid any potential liability under HIPAA or state law.

Of course, all reporting requires cooperation. Whether journalists will continue to obtain meaningful information on health-related issues in the long term will depend, as it always has, on cooperation and trust among reporters, photojournalists, and health care professionals. New privacy regulations may inject new elements of uncertainty and potential liability into this relationship, but working through these issues in a cooperative manner with due regard for what HIPAA actually requires, rather than what it is rumored to require, should contribute toward this process.

### **Endnotes**

- 1. Pub. Law No. 104-191 (1996).
- 2. Overbroad interpretations are not limited to journalistic issues. Even family members have reported being unable to access information about relatives due to expansive interpretations of HIPAA, which has prompted an HHS spokesperson to acknowledge that "many, many hospitals are erring very, very conservatively" in privacy procedures following the effective date of HIPAA. See Tom Graham, Not Her Sister's Keeper, WASH. POST, July 22, 2003, at H-2.
  - 3. See 47 C.F.R. § 160.103 (2003).
  - 4. See id.
  - 5. See 47 C.F.R. § 164.514 (2003).
- 6. See 47 C.F.R. §§ 160.300–160.312 (2003); see also HIPAA, 42 U.S.C. §§ 1320d-5, 1320d-6.
- 7. See 47 C.F.R. § 164.502(a)(1)(iii) (2003).
- 8. The information being captured by the photojournalist in this hypothetical situation does not constitute "protected health information" under HIPAA. *See* 47 C.F.R. § 160 103 (2003)
- 9. See 47 C.F.R. §§ 160.502, 160.508 (2003).

# The Uniform Witness Act: A Way Around the Reporter's Privilege?

SAUL B. SHAPIRO AND NICOLAS COMMANDEUR

ABC News recently found itself in the uncomfortable position of being compelled to turn over confidential outtakes from reporters' interviews without ever having the chance to argue before a court that those materials were privileged. That predicament was the result of a loophole in the Uniform Witness Act<sup>2</sup> that potentially allows a party to subpoena and obtain evidence from journalists regardless of whether those materials are privileged.

# Does the Privilege Attach to **Subpoenaed Documents?**

The Act allows parties to criminal cases pending in one state to demand discovery from reporters in other states, including New York. Designed as a means of obtaining testimony or evidence that otherwise would not be subject to subpoena,<sup>3</sup> the Act has been adopted by all fifty states, Puerto Rico, the Virgin Islands, and the District of Columbia. Significantly for journalists, news organizations, and their lawyers, the Act begs the procedural question of where and under what law the responding party can object to the subpoena on privilege grounds.4

In New York, where ABC News is headquartered, the state's highest court has held in *In re Codey* that with some undefined exceptions, the courts from the requesting state where the evidence is to be admitted should resolve questions of privilege and admissibility.5

Underlying Codey, which dealt with a subpoena demanding the production of a witness and documents, was the assumption that the party could assert its privilege arguments in the requesting state when the witness appeared in compliance with the subpoena. Codey failed to re-

Saul B. Shapiro (sbshapiro@pbwt.com) and Nicolas Commandeur (ncommandeur @pbwt.com) are respectively a partner and an associate at Patterson, Belknap, Webb & Tyler LLP in New York City. They represented ABC News Inc. in In re Frey, Index No. 30174/02 (N.Y. Sup. Ct.).

solve the question of how a court should proceed when a party seeks documents or outtakes from a reporter, as opposed to a witness, and the news organization is ordered to produce the materials with no opportunity to make privilege arguments in either state before the reporter fully complies with the subpoena.

# Caught in the Loophole?

ABC faced that dilemma when it was subpoenaed for the outtakes of interviews with Wilbert Rideau. ABA correspondents interviewed Rideau, who is currently serving time at the Louisiana State Penitentiary at Angola, for two programs, a 1989 broadcast of 20/20 and a 1990 broadcast of Nightline. During those interviews, he never denied his guilt in a 1961 murder and attempted murder in Louisiana. Louisiana juries have convicted him of those crimes on three separate occasions, but the conviction has been thrown out each time on appeal. Rideau gained prominence based primarily upon his accomplishments in prison, where he has educated himself and won awards for his writing and editorial work on the critically acclaimed prison magazine, The Angolite. He has become a focal point for the debate over whether prisoners convicted of the most heinous crimes can be rehabilitated and return as productive members of society.6

Following the most recent reversal of Rideau's conviction, the district attorney for Calcasieu Parish filed charges once again and made an ex parte application to the Louisiana court for a certificate to be used for an application in New York State court under the Act for all outtakes and transcripts from the ABC interviews. ABC learned of the Louisiana application only after it reached the New York courts.

After the Louisiana court granted the application, the district attorney in New York petitioned on behalf of his Louisiana counterpart for an order to show cause why such a subpoena should not issue. ABC opposed that pe-

tition on the grounds that the district attorney had failed to make a sufficient showing for such a subpoena under the Act's requirements<sup>7</sup> and that the New York court should refuse to issue the subpoena in any event because the materials were privileged. ABC argued that the proposed subpoena in this case, unlike the one in *Codey*, only sought documents. As a result, ABC asserted that if the New York court did not consider its reporter's privilege and issued the subpoena, ABC's compliance with the subpoena would preclude any court from considering the privilege. The New York Supreme Court rejected ABC's arguments and issued the subpoena, leaving the network to fight the subpoena in Louisiana.8

Although ABC may yet have its day in court in Louisiana, this case highlights a potentially serious problem for journalists and news organizations that are subject to subpoena under the Act. A New York court, ostensibly following Codey, could decide to issue a document subpoena without considering any privilege objections, leaving those for a court in the requesting state. But a court in the requesting state might decline to consider whether it should quash a subpoena from another jurisdiction (barring some explicit caveat in the issuing court's order, as ABC had in the Rideau case). Therein lies the rub: compliance with a subpoena for the production of documents moots any privilege.

# **Options Available Under the Act**

Lawyers have several options, each with different consequences, when litigating privilege issues arising under the Act, as demonstrated by the following discussion of how the Act works:

A party seeking a subpoena under the Act must first obtain a certification from a court in the requesting party's state that (1) there is a pending criminal case or grand jury investigation, (2) the person requested is a material witness, and (3) his or her presence will be required.9 The Act does not require that

the target of the subpoena be given notice that the court in the requesting state is considering such a certification. This happened in the Rideau case where ABC had no notice of the Louisiana court's action.<sup>10</sup>

The requesting party must then present that certificate to a court in the state where the witness lives or the custodian of the evidence is located and demand that a subpoena be issued. The court in the witness's state must then set a hearing to determine that the witness is "material and necessary" and that it will not cause undue hardship for the witness to attend. This is generally the first time that the target of the potential subpoena learns of the request.

# By its terms, the Act only applies to witnesses, not documentary evidence.

Although courts have an obvious inclination to defer to the findings of the requesting tribunal, which is presumably in a better position to determine whether the evidence will be material and necessary, the law requires the witness's home court to conduct a vigilant review of the record before issuing a subpoena. As Justice Bellacosa of the New York Court of Appeals explained in his 1984 practice commentary to New York's codification of the Act, "applications under this section are not automatically or easily granted."

The certificate of the judge in the requesting state is merely prima facie evidence of the facts stated therein; a court in the sending state must make its own independent evaluation before issuing the requested subpoena.12 The potential impact of any subpoena on the prospective witness influences the court's decision whether to issue one. As the New York Court of Appeals has recognized, the "process for securing the presence of an out-of-State witness has been termed 'drastic' because it represents an incursion upon the liberty of a prospective witness, who, although accused of no crime or wrongdoing, is required to attend a criminal proceeding in another State."13

# **Importance of** *Codey*

By its terms, the Act only applies to witnesses, not documentary evidence.

However, the New York Court of Appeals, relying upon the U.S. Supreme Court's decision in *New York v.*O'Neil,<sup>14</sup> which recognized the constitutionality of the Act, ruled in *Codey* that the Act applied to document requests as well.<sup>15</sup> *Codey* is an especially important decision for media lawyers because the court refused to apply the reporter's privilege when considering a petition to issue a subpoena under the Act.

In *Codey*, the petitioner sought a subpoena compelling the custodian of records for ABC to appear before a New Jersey grand jury with video outtakes and a reporter's notes from an interview that was relevant to the grand jury's investigation. ABC argued, inter

alia, that the petitioner could not meet the Act's requirements that the discovery was material and necessary: because the outtakes were privileged and inadmissible, they could not be "necessary"

to the grand jury investigation. <sup>16</sup> In ruling that privilege questions should be left to the New Jersey courts, the *Codey* court explained that "evidentiary questions such as privilege are best resolved in the State—and in the proceeding—in which the evidence is to be used." <sup>17</sup> Justice Bellacosa wrote a strongly worded dissent, arguing that the court's decision potentially exposed New York journalists to harassing discovery requests in contravention of New York's firmly established policy of protecting the work of reporters. <sup>18</sup>

In *Codey*, the court understood that ABC would have an opportunity in the New Jersey court to assert its privilege when the custodian of records appeared in New Jersey. Moreover, although ABC argued that New Jersey's reporter's privilege was not as protective as that of New York, the State of New Jersey did at least afford some protection.

The court also left open the, so far essentially unrealized, possibility that some future case might present a situation where New York's "strong public policy" might justify not issuing a subpoena, even if the "material and necessary" test was satisfied. Indeed, the practice commentary to New York's codification of the Act highlights this caveat to the *Codey* holding: "Thus the Court was not confronted with a situation where evidence that would be ab-

solutely privileged by statute would be completely unprotected in the demanding state."<sup>20</sup> This is precisely the situation that ABC faced in opposing the Louisiana district attorney's demand for outtakes from the Rideau interviews.

# **Protecting the Reporter's Privilege**

The law as it presently stands allows the possibility for abuse of the Act. A party seeking privileged materials may circumvent the privilege by requesting a subpoena only for documentary evidence. In that way, neither the requesting court nor the sending court will have an opportunity to consider privilege arguments.

Reporters and news organizations have several options. They can demand that any subpoena under the Act require the appearance of an actual witness, even if simply to deliver documents. In this way, they can preserve the opportunity to object. This position finds support in the language of the Act that only refers to witnesses, not documentary evidence.21 Requiring the appearance of a witness would also make it more difficult for the requesting party to obtain the discovery because such a requirement increases the burden on the witness, a factor to be considered by judges before issuing the requested subpoena.

Courts have not embraced such a literal interpretation, instead reading the Act to apply to document requests,<sup>22</sup> even when those requests do not also demand the appearance of a witness.<sup>23</sup> Such an argument is also obviously unappealing as a practical matter because it may force the target of the prospective subpoena to travel in order to fight the discovery. Witnesses also would forfeit any opportunity to raise privilege arguments in their home states, thereby offering a valuable concession if they live in states with strong protections for journalists.

Perhaps a more appealing tack, although one rejected by the New York court in the Rideau case, is to argue that because subpoenas for documents effectively preclude any opportunity to raise privilege arguments, the sending court should consider such arguments before issuing the subpoena. This position circumvents *Codey*'s general prohibition against the sending state's consideration of privilege arguments by confining itself to *Codey*'s exception for considering evidentiary privileges when required by a strong public policy interest. New

York certainly has a strong interest in ensuring that its journalists have access to at least some forum for protecting privileges. This also allows the news organization to litigate in its own state before a potentially more sympathetic court and under more protective law.

Of course, realizing that they otherwise will have to litigate privilege issues in New York courts, parties seeking document discovery may petition for subpoenas compelling the appearance of a witness. But at least in that case the target is still assured of some opportunity to be heard on its privilege claims. The more troubling aspect of this approach is that if the sending state rejects the reporter's argument and issues the subpoena without considering privilege issues, the reporter is left with a subpoena compelling the production of potentially privileged materials, and no forum in which to complain.

Another option is to request that the sending state deny the application for the subpoena and remand the case to the requesting state for a hearing regarding whether the asked-for materials would be privileged. Assuming that the requesting court determines that they are not, it would issue a new certificate that the petitioner could present to the sending state in support of a renewed application for a subpoena.

Another way to achieve the same result would be for the sending state to issue the subpoena but specifically leave to the requesting state a determination of whether the materials are privileged. In such a case, the reporter will not have to comply with the subpoena until an order is issued by the requesting state. The procedural obstacles are obvious: one court cannot force another in a different jurisdiction to make any findings of fact or determinations of law. However, as a practical matter, a request by one court, even if it has no legal effect, will presumably be given weight by another. Moreover, petitioners will be much more eager to persuade a court in the requesting state to conduct a hearing with notice to the target of the subpoena if they realize that it is the only way to obtain or enforce the subpoena from the sending state. Such a

procedure is not especially appealing for the potential target of the subpoena who is forced to litigate before a tribunal that theoretically should have considered the privileged status of the materials sought before issuing the certificate in the first place.

None of these options is particularly comforting for journalists, who are still exposed through the Act to discovery that potentially is not only burdensome but also violative of the reporter's privileges against the disclosure of confidential information. In such cases, the lawyer's primary goal should be to ensure that the Act is not manipulated into a vehicle for circumventing the reporter's privilege altogether.

# **Endnotes**

- 1. In re Frey, Index No. 30174/02 (N.Y. Sup. Ct.) (Soloff, J.).
- 2. The Uniform Witness Act is more formally known as the "Uniform Act to Secure the Attendance of Witnesses From Without a State."
- 3. See Ex rel. Codey v. ABC Corp., 82 N.Y.2d 521, 525-26, 605 N.Y.S.2d 661, 664-65 (1993).
- 4. New York recognizes a constitutionally protected right of journalists to protect from disclosure nonpublic information about their stories such as notes and outtakes. See O'Neill v. Oakgrove Constr., Inc., 71 N.Y.2d 521. 527, 528 N.Y.S.2d 1, 3 (1988) ("the courts in New York and elsewhere, Federal and State, have recognized a reporter's qualified privilege under the First Amendment guarantee of free press and speech").
  - 5. Codey, 82 N.Y.2d at 521.
- 6. Daniel Bergner, When Forever Is Far Too Long, N.Y. TIMES, June 17, 2003.
- 7. In particular, ABC argued that the broadcasts of the interviews, which contained Rideau's acknowledgement of culpability, and Rideau's numerous public confessions rendered the outtakes duplicative and unnecessary to the prosecution.
- 8. ABC appealed the New York Supreme Court's order, and that appeal is pending as of this writing. ABC also filed an application in Louisiana to contest production of the outtakes. That application presently is in abeyance pending the outcome of a motion to transfer the underlying criminal case to another parish in Louisiana.
  - 9. N.Y. C.P.L.R § 640.10(2). 10. Id. § 640.10(3).
- 11. Bellacosa, McKinney Practice Commentary, N.Y. C.P.L.R. § 640.10 (1984).

- 12. See New Jersey v. Bardoff, 92 A.D.2d 890, 891, 459 N.Y.S.2d 878, 879 (2d Dep't 1983) ("The court of the state where the witness resides is obliged to determine for itself whether the witness is material and necessary."); In re Connecticut, 179 Misc. 2d 623, 630, 687 N.Y.S.2d 219, 224 (N.Y. County Ct. 1999) ("the application, while considered prima facie evidence of the factual assertions contained therein, does not in and of itself, in view of the credible contradictory evidence adduced at the hearing, sustain the heavy burden of proof which rests with the state to establish [the witness's] materiality").
- 13. People v. McCartney, 38 Misc. 2d 618, 622, 381 N.Y.S.2d 855, 857 (1976) (citing State v. Emrick, 282 A.2d 821 (Vt. 1971)).
  - 14. 359 U.S. 1 (1959).
- 15. Ex rel. Codey v. ABC Corp., 82 N.Y.2d 521, 525–26, 605 N.Y.S.2d 661, 664 (1993) (pursuant to Uniform Witness Act, "a party to a criminal proceeding in one State can either obtain the presence of a witness residing in another State or can compel the production of evidence located in another State"). See also Superior Court v. Farber, 94 Misc. 2d 886, 887, 405 N.Y.S.2d 989, 990 (Sup. Ct. 1978) ("There is no doubt that CPL 640.10 subd. (2) comprehends subpoenas duces tecum as well as subpoenas ad testificandum.").
- 16. Codey, 82 N.Y.2d at 525, 528-29, 605 N.Y.S.2d at 665-66.
  - 17. Id. at 530, 605 N.Y.S.2d at 667.
- 18. Id. at 533-35, 605 N.Y.S.2d at 669 ("This Court's hortatory pronouncement regarding this interstate evidence-gathering tool creates the potential for considerable inappropriate manipulation of judicial process. After all, evidentiary expeditions are not unknown when the quarries are rich media resource materials.").
- 19. Id. at 530 n.3, 605 N.Y.S.2d at 667 n.3 ("Our holding should not be construed as foreclosing the possibility that in some future case a strong public policy of this State, even one embodied in an evidentiary privilege, might justify the refusal of relief under CPL 640.10 even if the 'material and necessary' test set forth in the statute is satisfied.").
- 20. Preiser, McKinney Practice Commentary, N.Y. C.P.L.R. § 640.10 (1995).
- 21. The Uniform Witness Act defines "witness" as including "a person whose testimony is desired in any proceeding or investigation by a grand jury or in a criminal action, prosecution or proceeding." N.Y. C.P.L. § 640.10(1).
- 22. See, e.g., Codey, 82 N.Y.2d at 525, 605 N.Y.S.2d at 664.
- 23. See, e.g., Superior Court v. Farber, 94 Misc. 2d 886, 887, 405 N.Y.S.2d 989, 990 (Sup. Ct. 1978).

# Liability and Newsgathering

(Continued from page 1)

ing. Against this backdrop, the article scrutinizes the Med Lab decision and reexamines the outcomes of earlier cases using the *Med Lab* analysis. Finally, this article argues that, although the test adopted by the Ninth Circuit in Med Lab provides sufficient protection for newsgatherers in most situations, the Ninth Circuit erred by failing to require the plaintiff to demonstrate that his harm was caused by the intrusion rather than by the publication. Thus, under the Med Lab analysis, a plaintiff may be able to circumvent the traditional protections afforded to media defendants against liability for publication damages. Even though the Med Lab court did not specifically incorporate such a threshold inquiry, media defendants should nevertheless continue to press courts to scrutinize carefully the basis for a plaintiff's damages. Otherwise, intrusion torts will significantly chill legitimate and valuable newsgathering activity.

# **Newsgathering and the Constitution**

In order to inform the public on the issues of the day, the press must be able to gather news as well as publish it. In fact, the U.S. Supreme Court has acknowledged that "without some protection for seeking out the news, freedom of the press could be eviscerated."2 Although matters of public record can be easily obtained by the media, when the information is not generally available, newsgatherers often must resort to less conventional measures to uncover information that others work vigorously to hide. Many of these efforts test the boundaries of laws that were enacted for purposes wholly unrelated to, and in

Sharon McGowan (sharon\_mcgowan@hotmail.com) served as an associate at Jenner & Block, LLC, in Washington, D.C., at the time that she wrote this article. She will join the ACLU's National Legal Department in New York in September as the William J. Brennan First Amendment Fellow. The author wishes to thank Matthew Hersh and Kerry Quinn for their invaluable comments. The views expressed in this article are those of the author and not necessarily those of Jenner & Block, the ACLU, or their clients.

many cases without regard to their effect on the media. Despite the fact that these provisions can impede important newsgathering efforts, courts have remained unwilling to exempt the media from such generally applicable laws.

The legal doctrine that subjects news agencies to generally applicable laws emerged from a cluster of cases where the media had engaged in questionable employment practices, such as union busting and wage-and-hour law violations. In those cases, the press in those cases argued that its privileged constitutional position should free it from the burdens imposed by federal labor laws and general taxes.<sup>3</sup> The U.S. Supreme Court rejected these arguments for a media exemption and reaffirmed that these laws applied equally to media and nonmedia employers alike.

In one of the earliest cases, in which a media employer was accused of retaliating against workers who were trying to unionize, the U.S. Supreme Court commented caustically that "the publisher of a newspaper has no special immunity from the application of general laws. He has no special privilege to invade the rights and liberties of others."4 Even in later cases involving wholly different factual scenarios, this pronouncement has served as the linchpin of a jurisprudential structure under which courts subject the media to generally applicable laws, regardless of whether such laws impede newsgathering. The U.S. Supreme Court has continued to stand by this principle in recent years, most notably in Cohen v. Cowles Media Co.,5 in which it held that the First Amendment did not exempt the media from state contract laws.6

Although the U.S. Supreme Court has technically left the question open,<sup>7</sup> as a general matter, the media cannot be held liable for the publication of truthful information. With regard to newsgathering, however, the Court finds less troublesome state laws that impede the ability of the media to obtain newsworthy information. From the standpoint of many in the media, this divide between reporting and investigating may seem like a distinction without a difference. Courts, however, differentiate torts based on publication from those based on newsgathering activities by characterizing the former as speech or content based and the latter as conduct or content-neutral. For that reason, in the context of intrusion torts, lower courts—both state and federal—ostensibly treat news organizations as though they were any other defendant. Even so, however, many courts clearly remain cognizant of the important role that the media play in a democratic society, and have on occasion adjusted their analysis so as to shield the media from liability.

# **Intrusion Torts**

Among the generally applicable laws that lower courts have applied to media defendants is state tort law, which in most jurisdictions includes the torts addressing invasion of privacy, such as intrusion upon seclusion. The notion that individuals have a right of privacy, or a right to be left alone, is a relatively new development in the law, as compared, for example, to property rights. In the first published articulation of the right of privacy, Samuel Warren and Louis Brandeis wrote an 1890 article in the Harvard Law Review, titled "The Right to Privacy."8 As members of two of Boston's most elite and gossiped-about families,9 Warren and Brandeis argued vigorously for the creation of a private zone where people could act free from public scrutiny. The notion that individuals have enforceable privacy rights received a boost in the 1960s when scholar William Prosser published an influential article on privacy torts.10 Ultimately, privacy torts were included in Restatement (Second) of Torts, published in 1972. Accordingly, although the specific contours of privacy rights vary from state to state, most jurisdictions currently recognize some version of the right.

The Restatement identifies four distinct types of privacy invasions that may be actionable: (1) the unreasonable intrusion upon the seclusion of another; (2) the appropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public.11 Although each tort attempts to isolate a unique harm, these four categories frequently overlap, such that one particular act may implicate two or more of these torts. Nevertheless, this article focuses on the first of these privacy torts—the unreasonable intrusion upon the seclusion of others, also known as the invasion or intrusion tort.

As a general matter, a party commits commits the tort of intrusion upon the seclusion of another when it "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his [or her] private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."12 This tort has been compared to trespass, and occasionally described as a quasi-trespass tort, because it typically involves a physical invasion of a person's property.13 Although an invasion of privacy may involve a trespass, not every trespass is an intrusion upon seclusion. Only when the intrusion is highly offensive to the reasonable person does the trespass also qualify as an invasion of privacy.

Although courts disagree about the specific conduct that triggers liability under this tort, they tend to focus on certain general considerations when considering these types of cases. To begin with, privacy, at least as contemplated by this tort, is a right that attaches to a person and not to a corporation.14 Furthermore, people have no reasonable expectation of privacy with regard to information that is a matter of public record.15 In addition, the media are entitled to capture on video anything "visible to the public." This phrase, however, is something of a term of art. For example, depending on who else is present, some semipublic spaces may still be characterized as "public," so as to diminish an individual's expectation of privacy while inhabiting that space.16 As a general matter, as long as reporters do not engage in criminally harassing behavior when tracking the public movements of their targets,17 their newsgathering efforts will generally not be hampered by the courts. But once the media invade private property to investigate a news story, their exposure to tort liability increases significantly.

Finally, intrusion torts have become defined in large part by what they are not — most notably by their difference from defamation torts. Because defamation torts often involve the same underlying conduct as intrusion torts, some plaintiffs try to use the intrusion tort to recover damages caused by the dissemination of private information. This strategy is motivated by the fact that intrusion torts, as opposed to publication torts, do not make truth an absolute defense. Because the defamation stan-

dard clearly offers greater protection for the press, courts have refused to allow plaintiffs to reframe publication torts as privacy torts. <sup>19</sup> But unless courts closely scrutinize the source of plaintiffs' damages to ensure that plaintiffs do not, in fact, allege publication damages when bringing intrusion torts, the protections afforded by defamation torts will quickly become meaningless.

# The Legal Landscape of Undercover Investigative Reporting

When publicly available information fails to provide the whole story, reporters often must resort to unconventional tactics. They may pose as customers, patients, or job applicants, so that they can gather information from inside an organization. While recognizing that these techniques can be effective tools for gathering news, courts have not been willing to sanction them wholeheartedly. Rather than announce any bright-line rules, many judges prefer to work on a case-by-case basis so that they can selectively determine whether reporters have been unduly abusive in their fact-gathering techniques.

# Posing as a Customer/Patient

An effective method for ferreting out substandard service is to send a healthy or prediagnosed patient to a health care institution and then rate the institution's quality of care. Because

duanty of care. Because such reports severely damage the reputation of a business and those associated with it, the target of the investigation often responds to the publication of embarrassing information by filing lawsuits that allege a host of tort claims, including trespass, fraud,

misrepresentation, and, in some circumstances, intrusion on seclusion. Particularly when the target of the investigation cannot dispute the truth of the damaging information, invasion torts frequently provide the only viable avenue for recovery.

Generally, when an establishment holds itself out as open to the general public, courts have been unwilling to impose liability on reporters who posed as would-be customers. For example, in *Desnick v. ABC*, <sup>20</sup> *Prime Time Live* sent seven test patients to ophthalmology offices in Wisconsin and Indiana to deter-

mine whether the doctors were performing unnecessary cataract surgery. When the doctors realized that their examinations had been recorded in connection with an investigative report, they sued the network, insisting that the testers had violated the doctors' right to privacy by securing entry into the clinic by misrepresenting their identity. Had the doctors known who these people really were, they argued, they would have refused to treat them. While recognizing that the testers had deceived the clinic staff by pretending to be patients, the court insisted that the privacy interest asserted by the doctors was not one that the tort of trespass seeks to protect.21 In this case, the testers had only recorded their own conversations with the clinic's physicians. The court determined that, because the reporters in this situation had acted no differently than restaurant critics or fair housing testers, they could not be held liable for trespass or intrusion.<sup>22</sup>

In a similar case, *American Transmission, Inc. v. Channel 7 of Detroit, Inc.*, <sup>23</sup> reporters from a local news station visited auto repair shops, claiming that they were having transmission problems. The mechanics did not realize, however, that the only problem with the reporters' vehicles was a purposefully disconnected vacuum hose. The reporters videotaped the auto me-

Although an invasion of privacy may involve a trespass, not every trespass is an intrusion upon seclusion.

chanics as they examined the cars and identified numerous "problems" that would be expensive to fix. On two successive nights, this tape was broadcast on the local news. In response to this investigation, the auto repair shop plaintiffs sued for defamation, fraud, and trespass. Recognizing the similarities between this case and the ophthalmology investigation, the court dismissed the claims against the reporters. <sup>24</sup> In doing so, the court noted that the reporters had stayed in the areas of the auto repair shop that were open to the public and had not disrupted the shop's opera-

tions.<sup>25</sup> More importantly, the reporters had not intruded into anyone's private space or revealed any intimate details about the shop's employees.<sup>26</sup>

As long as the recorded discussions stay focused on the newsworthy topic and do not delve into personal matters, courts appear willing to let reporters operate undercover. In McCall v. Courier-Journal, the Kentucky Court of Appeals rejected a lawyer's claim for intrusion upon seclusion brought against an undercover reporter who posed as a potential client.27 During a conversation recorded by the reporter, the lawyer insinuated that he could "fix" the client's case for \$10,000. In dismissing the claims against the reporter, the court commented that the parties had only discussed the purported client's legal problems and how the attorney would handle the case. According to the court, "[n]othing was learned about [the lawyer] which was private or personal."28

As long as the recorded discussions do not delve into personal matters, courts appear willing to let reporters operate undercover.

Likewise, an Oklahoma court dismissed trespass claims brought against reporters who, posing as parents, secretly recorded their tour of a day care facility for an investigative report on the state of local child care.<sup>29</sup> Motivated by a similar understanding of the privacy interests that trespass law is meant to protect, the court concluded that the network's "peaceful and non-disruptive news gathering methods" would not subject the network to liability.<sup>30</sup>

Under similar circumstances, however, the media have been held liable for invasions of privacy. For example, in Dietemann v. Time, Inc.,31 the Ninth Circuit affirmed a judgment against Life magazine for invasion of privacy stemming from an incident where its reporters secretly videotaped the untraditional medical practices of a self-described "doctor." By pretending to be patients, the reporters gained entry to the doctor's office, which was in the den of his home. In this situation, the court found the magazine liable for invasion of privacy, holding that the plaintiff's "office" was "a sphere from

which he could reasonably expect to exclude eavesdropping newsmen."32 The court disparaged the reporters' argument that secret recording devices were an essential newsgathering tool. According to the court, "[i]nvestigative reporting is an ancient art; its successful practice long antecedes the invention of miniature cameras and electronic devices."33 Concluding that the reporters had violated the plaintiff's privacy, the court affirmed the \$1,000 damages award for the injury to the plaintiff's "feelings and peace of mind."34 Over time, however, the Ninth Circuit's decision in Dietemann has been limited to the facts of that case.35

# Posing as an Employee

In order to conduct inside investigations of businesses suspected of wrongdoing, news agencies occasionally send reporters into the company as employees.

Courts have viewed these schemes with skepticism, but have been willing to let the media employ such tactics in limited circumstances. When courts believe that the media's purpose for such trickery is "legitimate" reporting, they have, for all practical purposes, ac-

quiesced to such newsgathering methods. If a reporter solicits personal or embarrassing information from an unsuspecting fellow employee, however, courts consistently impose liability on the news agency and/or the individual reporter involved.

Two relatively recent cases demonstrate this point. In Food Lion, Inc. v. Capital Cities/ABC, Inc.,36 two ABC employees went to work at a supermarket to expose unsanitary and illegal food-handling practices in the delicatessen department. Once the reporters were hired, they learned that the company placed barbeque sauce on chicken past its expiration date so that it could be resold, and mixed spoiled meat with fresh ground meat to avoid having to throw out the expired food products. The investigative report by ABC was devastating to Food Lion's reputation, but in light of the fact that it could not dispute the truth of the information published, the supermarket chose not to bring a defamation claim.37 Instead, Food Lion sued for trespass, breach of contract, breach of the duty of

loyalty, and fraud.

The Fourth Circuit affirmed the jury's findings that the undercover reporters had trespassed on private property and breached the duty of employee loyalty by using their positions in the supermarket to obtain footage that was directly adverse to Food Lion's interests.38 They also found that the reporters had breached their duty of loyalty by failing to disclose on their application for employment the fact that they were simultaneously employed by ABC.39 Despite these rulings against the network, ABC effectively prevailed because the court decided that Food Lion could only recover nominal damages for trespass and that it would have to satisfy the stringent New York Times standard of proof in order to recover damages for any harm attributable to the broadcast of the investigative report.40

On the other hand, in a case decided only months earlier, the California Supreme Court ruled that ABC could be held liable for invasion of privacy due to the actions of a reporter who had gone undercover as an employee with a psychic telephone hotline.41 Specifically, the court held that an employee may sue a reporter who covertly tapes her conversations with co-workers.42 The court noted that, even though others authorized to be in the office may also have overheard the discussion, the area where these employees' workstations were located was not generally accessible by the public, and therefore the plaintiff had an "expectation of limited privacy" that his workplace comments about his personal aspirations and his psychic reading would not be retransmitted to the public at large.43 In other words, the court held that a reasonable person could find that this employee could expect that his personal thoughts, which he had shared with colleagues whom he thought he could trust, would remain at least relatively private. The jury clearly agreed, awarding the plaintiff \$335,000 in compensatory damages and \$300,000 in punitive damages. The court did, however, leave open the possibility that a media defendant could defend itself from such a claim by proving that its actions were "justified by the legitimate motive of gathering the news."44

A third undercover employee case, *Russell v. ABC, Inc.*, 45 also hinged on the nature of the recorded discussions. A reporter posing as a fish market employee was sued by her manager, whom

she had caught on tape instructing her to tell customers that the fish was "today fresh" and advising her that fish too old to be sold as "fresh" could still be cooked and then sold. Although finding that the manager's claim for false-light publicity had merit, the federal court ruled that Illinois did not recognize a cause of action for intrusion upon seclusion.46 Even assuming that Illinois recognized the intrusion tort, the court opined, the manager would not be entitled to recover on such a claim based on "a conversation she willingly had with a co-worker at her place of business."47 While the manager was allowed to proceed with her false-light publicity claim, the court dismissed the intrusion claim. The opinion left open the possibility that the analysis might have been different had the discussion between the co-workers involved a topic more personal in nature.

# Reporting in "Real Time"

One final case that has played a critical role in the development of intrusion tort jurisprudence is Shulman v. Group W Products,48 which analyzed tort liability in the context of a media ride-along.49 In Shulman, the California Supreme Court ruled that reporters who were accompanying medical personnel in an emergency response helicopter were entitled to film the wreckage of an automobile accident to which the helicopter was responding.50 Not only are automobile accidents of interest to the general public, the court commented, but also, more importantly, accident victims cannot reasonably expect that they will be able to keep private an incident occurring on a public thoroughfare.

Despite its willingness to let the media record footage of the car wreck, the court decided that the network should not have recorded and broadcast dramatic images of an injured woman crying out, delirious with pain, to the nurse who was attending to her.51 It found that the victim "was entitled to a degree of privacy in her conversations with [the nurse] and other medical rescuers at the accident scene, and in [the nurse's] conversations conveying medical information regarding [the victim] to the hospital base."52 The court decided that, even though the public has an interest in learning about the automobile accident, a reasonable jury could find it highly offensive that a reporter used a microphone to record the statements of a vulnerable and confused woman, solely "for the possible edification and entertainment of casual television viewers."53

# The Med Lab Decision

Against this legal landscape, the Ninth Circuit recently decided Med Lab.54 The facts in Med Lab are similar to Desnick, the case involving the undercover investigation of the opthamology clinic. In Med Lab, Prime Time Live sent reporters into a laboratory to determine whether technicians were reading pap smears too quickly, in violation of federal law. In order to gain access, the reporters purported to be cytotechnologists and claimed that they were interested in opening up a similar laboratory in their home state. Based on these representations, the director of the laboratory agreed to give the reporters a tour of the facility, and on this tour, he talked about current issues facing the industry and his efforts to stay competitive. The reporters secretly videotaped the tour by using a camera hidden in a wig worn by an ABC

employee. Although neither the name of the lab nor the names of any of the people at the company were used in the *Prime Time Live* report, the director of the lab recognized the footage that appeared in the broadcast and sued for,

among other things, intrusion upon seclusion.

In rejecting this intrusion claim,55 the district court noted that the plaintiff had freely invited these strangers to inspect his facility and had spoken with them only about business matters.56 The reporters did not attempt to glean personal information from him,57 and to the extent that any business matters discussed were proprietary, the court noted that the lab director never asked his guests to sign any type of confidentiality agreement.58 When the reporters wandered into private areas of the facility, the plaintiff instructed them that certain areas were off limits, and they immediately moved on without protest.59 Based on these considerations, the court determined that the undercover reporters had not violated any reasonable expectation of privacy held by the plaintiff.

As an alternative basis for its deci-

sion, the district court found that the plaintiff had failed to demonstrate that any harm stemmed from the alleged invasion rather than from the publication of the video. 60 Although its analysis was somewhat cursory, the court strung together a number of citations in support of the principle that "a plaintiff fails to state a claim for invaded seclusion if the harm flows from publication rather than intrusion."61 As the plaintiff failed to show that his damages arose from the intrusion as opposed to the publication, the court indicated that for this reason alone the defendants would be entitled to summary judgment.

The Ninth Circuit affirmed the district court on a number of grounds. The court first rejected the notion that the plaintiff had a reasonable expectation of privacy, reasoning that the plaintiff had invited the reporters into the spaces where the tour took place and that the parties had only discussed business issues. The court next addressed whether the plaintiff had an "expectation of limited privacy" against surrepti-

A plaintiff fails to state a claim for invaded seclusion if the harm flows from publication rather than intrusion.

tious recording, as had been recognized by the California Supreme Court in Sanders v. ABC. At the outset, the court ruled that Arizona did not recognize a privacy right as broad as the one announced in Sanders. 63 The court also decided that, even assuming that Arizona would recognize a privacy interest coextensive with that found under California law, the plaintiff's expectation of privacy against secret recording still would not have been reasonable. In reaching this conclusion, the court placed great emphasis on the nature of the disclosure made in the California cases. In both instances, the plaintiff had revealed deeply intimate information, whether about personal hopes and aspirations or the desire to go on living in the face of serious injuries. By contrast, in Med Lab, as in Desnick, the information captured on the video related solely to the business that the reporters

had been investigating. 64 The court placed these various cases into two categories—"external" and "internal" workplace communications. The former involves a workplace insider and a customer, and therefore is "more probably business-related and thus not sufficiently private and personal in character to make any privacy expectation reason-

been serving an important public interest by gathering news about "a medical issue with potential life and death consequences affecting millions of women." Therefore, for these reasons—the lack of any reasonable expectation of privacy on the part of the plaintiff and the fact that the intrusion had not been highly offensive—the

The Ninth Circuit's decision in Med Lab should provide sufficient protection for the media to continue its undercover newsgathering activity. court affirmed the district court's ruling. As a result of this holding, the court commented in a footnote that it would not reach the district court's alternative holding that the plaintiff had failed to state a claim for intrusion because he could not identify damages from the intrusion that were

independent of the damages resulting from publication.<sup>69</sup>

able."65 The latter, on the other hand, involves coworkers and is more likely to involve conversations that are personal in nature. Concluding that the communications in *Med Lab* fell in the first category, the court ruled that the plaintiff had no reasonable expectation of privacy against recording.

In an attempt to reconcile its holding with Dietemann, in which the Ninth Circuit had found that the "doctor" had a reasonable expectation of privacy against surreptitious recording by undercover reporters, the court explained that *Dietemann* was unlike the typical "external communications" cases because the intrusion in that case had been into the plaintiff's home, the site where privacy interests are "most potent."66 Furthermore, the court emphasized that, in Dietemann, the plaintiff's "quack healing of nonexistent ailments . . . was his private hobby, not a professional business service."67 Therefore, the court concluded, Dietemann posed no obstacle to the court's decision that the plaintiff in Med Lab had no reasonable expectation of privacy that his conversation would not be recorded.

Turning to the second prong of the intrusion tort inquiry, which asks whether the intrusion was "highly offensive" to a reasonable person, the court emphasized that the motives of the intruder must be examined in order to determine whether the intrusion was "highly offensive." Unlike cases where the media had been motivated by a morbid curiosity or desire to titillate their audience, the reporters in this case had

# Newsgathering Post-Med Lab

The Ninth Circuit's decision in Med Lab should provide sufficient protection for the media to continue its undercover newsgathering activity. In fact, reporters should be able to avoid intrusion tort liability in most cases simply by avoiding questions that could elicit highly personal information and by limiting themselves to locations where they were actually invited (even if under false pretenses). The analysis in Med Lab, however, is insufficient in some important ways. First, the court placed great weight on the distinction between "internal" and "external" communications, apparently on the assumption that parties will adjust their privacy expectations based on the identity (or assumed identity) of the participants to the conversation. Yet, while ostensibly focusing on the identity of the parties involved, the court in fact concentrated on the nature of the disclosures made in the conversations. In other words, the panel in Med Lab seems to have been motivated by the belief that one could reasonably expect that comments about hopes and dreams will be kept in confidence, whereas remarks about seedy business practices will likely be passed around.

This "content" test, rather than a "participants" test, explains not only the decisions in *Sanders* and *Shulman*, but also the outcome of the fish market case in *Russell*. Under the "participants" test, the conversation between co-workers in *Russell* would be classified as "internal,"

meaning that the media would have been found liable. By contrast, the "content" test can explain the court's decision in *Russell* because the plaintiff in that case would not have a reasonable expectation of privacy in discussions about unsanitary fish-handling practices. Thus, the "content" test brings together the decisions in both *Russell* and *Med Lab*.

Second, even though the "content" test will usually produce results that protect investigative reporting, the Ninth Circuit's analysis does not resolve the tension that inherently exists in the intrusion tort liability standard. In particular, the two-pronged test articulated by the Restatement and applied by the Ninth Circuit tries to capture both a subjective and an objective component: the former by asking, in the first prong, whether the individual expected that the communication would be private, and the latter by asking, in the second prong, whether the breach of that trust would be highly offensive to some hypothetical reasonable person. But these two elements are not as distinct as the test seems to suggest. In fact, through its decisions about when to impose liability, courts create the expectation of privacy that they claim merely to be recognizing. Because of this circularity, the intrusion torts are not grounded in any extrinsic doctrine or principle—one that could be used to predict the outcome of the cases. Instead, the decisions in intrusion tort cases often seems to reflect judges' personal assessments as to whether the media's conduct warrants punishment or praise.

Finally, the Ninth Circuit failed to determine as a preliminary matter whether the case was, in fact, an intrusion tort case or merely a publication tort case masquerading as an intrusion case. Rather than evading this issue, the court should have paid greater attention to the alternative ground offered by the district court, which required the plaintiff to show that his damages resulted from the intrusion itself rather than from the publication. Only by conducting such an analysis can courts ensure that the media defendants receive the full range of constitutional protections to which they are entitled in publication cases. In fact, both the district court and the Ninth Circuit appeared to view this source-of-damages test as an alternative and ancillary inquiry, rather than as an important threshold matter. The district

court jumped from its statement of the law—the harm must flow from the intrusion rather than from the publication—to its conclusion that plaintiff had failed to make that showing, without providing any additional discussion as to what a plaintiff would need to demonstrate in order to satisfy this initial burden. The Ninth Circuit, by refusing in a footnote to reach this basis for the district court's holding, left this question unanswered.

Although the Ninth Circuit avoided this issue, other courts have recognized the importance of assessing whether a plaintiff's injury stems from the intrusion or from publication. For example, in Frome v. Renner, a federal district court in California refused to impose liability on an undercover reporter posing as a patient, even though the reporter had given a false name and presented a false insurance identification card in order to gain access to the target doctor's office as a patient. In reaching this conclusion, the court emphasized that any damages suffered by the doctor resulted from the broadcast of the investigative report and not from the misrepresentations made by the reporter. 70 Likewise, in Russell, which involved the undercover investigation of the fish market, the court emphasized that the harm suffered by the plaintiff stemmed from the broadcasting of the secret video rather than from the filming itself.71 By conducting a source-of-damages analysis from the outset, both of these courts avoided making subjective value judgments about the privacy interests that society should recognize.

Media defendants must continue to remind courts that the main function of this source-of-damages inquiry is to separate true intrusion tort cases from those that are, in fact, simply disguised publication tort cases. This sorting mechanism will only be effective, however, if courts conduct this analysis as a preliminary matter in every case. Only after the plaintiff has satisfied this threshold burden should courts examine whether the intrusion upon the plaintiff's seclusion was so highly offensive that damages are warranted. Once this sorting has taken place, courts can apply the Med Lab test, which, although still somewhat subjective, will balance the privacy concerns of individuals against the public interest in vibrant investigative news reporting.

Although the Ninth Circuit failed to conduct this important threshold source-of-damages inquiry, the court's decision in Med Lab nevertheless provides significant protection to media defendants. By focusing on the contents of the disclosure and the motivations of the reporter, the Ninth Circuit has created a de facto newsworthiness defense to intrusion tort liability. But rather than exacerbating the confusion between intrusion and publication torts by creating a newsworthiness defense to intrusion claims, the Ninth Circuit instead should have policed the distinction between intrusion and publication torts by requiring lower courts to conduct a source-ofdamages analysis in every case.

Courts' ambivalence about the application of intrusion torts to media defendants—an ambivalence that is clearly apparent in Med Lab-reflects judicial discomfort with making highly subjective value judgments about when people should reasonably expect their communications to remain private, and when the media's newsgathering efforts should be regarded as highly offensive. By pressing courts to examine the source of plaintiffs' alleged injuries from the outset, media defendants can steer courts away from these difficult issues. In the process, they will help to ensure that courts continue to respect fully the constitutional safeguards against publication tort liability.

# **Endnotes**

- 1. 306 F.3d 806 (9th Cir. 2002), *aff* g 30 F. Supp. 2d 1182 (D. Ariz. 1998).
- 2. Branzburg v. Hayes, 408 U.S. 665, 681 (1972).
- 3. Oklahoma Press Publ'g Co. v. Walling, 327 U.S. 186 (1946) (Fair Labor Standards Act); Associated Press v. United States, 326 U.S. 1 (1945) (Sherman Act); Associated Press v. Nat'l Labor Relations Bd., 301 U.S. 103 (1937) (National Labor Relations Act); Murdock v. Pennsylvania, 319 U.S. 105 (1943) (nondiscriminatory taxes).
  - 4. NLRB, 301 U.S. at 132–33.
- 5. 501 U.S. 663, 670 (1991) ("enforcement of such general laws against the press is not subject to stricter scrutiny than would be applied to enforcement against other persons or organizations").
- 6. Bartnicki v. Vopper, 532 U.S. 514, 529 (2001) ("Our refusal to construe the issue presented more broadly is consistent with this Court's repeated refusal to answer categorically whether truthful publication may ever be punished consistent with the First Amendment."); Cox Broad. Corp. v. Cohn, 420 U.S.

- 469, 491 (1975) (purposefully avoiding the "broader question whether truthful publications may ever be subjected to civil or criminal liability consistently with the First and Fourteenth Amendments.").
- 7. The Court evaded this issue in *Cohen* by suggesting that compensatory damages in a contract action are not punishment but rather are more comparable to a court-mandated bonus paid to a confidential news source. *Cohen*, 501 U.S. at 670.
- 8. Samuel Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
- 9. See Andrew Jay McClurg, Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places, 73 N.C. L. Rev. 989, 1009–10 (1995) (noting that "Dean Prosser gave credence to the theory that the Warren and Brandeis article was motivated by Warren's annoyance with the Boston newspaper coverage of parties hosted by his socialite wife and by publicity given to the wedding of a family member").
- 10. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
- 11. RESTATEMENT (SECOND) OF TORTS § 652A.
  - 12. Id. § 652B.
- 13. See, e.g., Brady v. Brady, No. 222875, 2001 WL 879011, at \*2 (Mich. Ct. App. 2001) (intrusion on seclusion analogous to trespass) (unpublished opinion); Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 458 (Ga. Ct. App. 2001) (accord); Doe v. United States, 83 F. Supp. 2d 840, 841 (S.D. Tex. 2000) (describing intrusion on seclusion as "quasi-trespass").
- 14. RESTATEMENT (SECOND) OF TORTS § 652I ("[T]he right protected by the action for invasion of privacy is a personal right, peculiar to the individual whose privacy is invaded. . . . [Consequently,] a corporation, partnership or unincorporated association has no personal right of privacy."). Corporations may have trade secrets or other proprietary/confidential information that they legitimately wish to protect. This tort, however, is not designed to serve those interests.
- 15. See, e.g., Wolf v. Regardie, 553 A.2d 1213, 1218 (D.C. 1989) ("it is hardly persuasive to argue that appellant's seclusion is somehow intruded upon by a person's consultation of public records concerning him").
- 16. People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1279 (Nev. 1995).
- 17. Galella v. Onassis, 487 F.2d 986, 993 (2d Cir. 1973).
- 18. New York Times v. Sullivan, 376 U.S. 254, 279–80 (1964).
- 19. Hustler Magazine v. Falwell, 485 U.S. 46, 54 (1988).
  - 20. 44 F.3d 1345 (7th Cir. 1995).
  - 21. Id. at 1352.
  - 22. Id.

- 23. 609 N.W.2d 607 (Mich. Ct. App. 2000).
- 24. Id. at 612-14.
- 25. Id. at 614.
- 26. Id.
- 27. McCall v. Courier-Journal, 6 Med. L. Rep. 1112, 1113 (Ky. Ct. App. 1980), *rev'd on other grounds*, 623 S.W.2d 882 (Ky. 1981) (reversing lower court's dismissal of claim for false-light publicity).
  - 28. Id.
- 29. Willis/Kids on Broadway, Inc. v. Griffin Television, LLC, Case No. 91, 812 (Okla. Civ. App., Mar. 5, 1999).
- 30. *Id.* The court did, however, allow the plaintiffs to pursue claims for defamation and false-light publicity.
  - 31. 449 F.2d 245 (9th Cir. 1971).
  - 32. Id. at 249.
  - 33. *Id*.
  - 34. Id. at 247.
- 35. But see Buller v. Pulitzer Publ'g Co., 684 S.W.2d 473, 483 (Mo. Ct. App. 1985) (allowing a psychic to bring invasion tort claim against news reporter who had concealed his identity when he came for a reading on the grounds that the psychic only gave private readings for clients and had not predicted any world disaster or other major event that would have otherwise cast her into the public eye).
  - 36. 194 F.3d 505 (4th Cir. 1999).
  - 37. Id. at 510.
  - 38. Id. at 517-19.
  - 39. Id. at 516.
- 40. *Id.* at 522–23. Food Lion was not even permitted to recover the wages paid or the

- costs incurred while training the undercover reporters as supermarket employees. *Id.* at 514.
- 41. Sanders v. ABC, 978 P.2d 67 (Cal. 1999).
- 42. Id. at 73-74.
- 43. Id. at 74.
- 44. Id. at 77.
- 45. 23 Med. L. Rep. 2428 (N.D. Ill. 1995).
- 46. Id. at 2434.
- 47. Id.
- 48. 955 P.2d 469 (Cal. 1998).
- 49. In light of the U.S. Supreme Court's decision in Wilson v. Layne, 526 U.S. 603 (1999), law enforcement will likely cut back on the opportunities for the media to accompanying them when performing their duties. A comprehensive discussion of the legal developments regarding media ride-alongs and other issues arising from real-time reporting is beyond the scope of this article. See generally Sheila M. Lombardi, Media in the Spotlight: Private Parties Liable for Violating the Fourth Amendment, 6 ROGER WILLIAMS U.L. REV. 393 (2000).
  - 50. Shulman, 18 Cal. 4th at 231.
  - 51. Id. at 234.
  - 52. Id. at 233.
  - 53. Id. at 238.
- 54. Medical Laboratory Management Consultants v. ABC, 306 F.3d 806 (9th Cir. 2002), *aff* g 30 F. Supp. 2d 1182 (D. Ariz. 1998).
- 55. The court rejected a host of other claims in its first summary judgment ruling, 931 F. Supp. 1487 (D. Ariz. 1996).
- 56. Med. Lab. Mgmt. Consultants v. ABC, 30 F. Supp. 2d 1182 (D. Ariz. 1998).

- 57. Id. at 1188-89.
- 58. *Id.* at 1188.
- 59. Id. at 1185-86.
- 60. Id. at 1191.
- 61. *Id.* (quoting Thomas v. Pearl, 998 F.2d 447, 452 (7th Cir. 1993)); *see also id.* (citing additional cases).
  - 62. Med Lab, 306 F.3d at 813-14.
- 63. *Id.* at 815; *see also* Sanders v. ABC, 20 Cal. 4th 907 (1999).
- 64. The court also compared the facts in *Med Lab* to *Wilkins v. NBC*, 84 Cal. Rptr. 2d 329 (Cal. Ct. App. 1999), in which television producers posing as potential investors secretly videotaped a business meeting with a salesperson from a telecommunications company. *Med Lab*, 306 F.3d at 817. The court's analysis in *Wilkins*, however, had also been influenced by the fact that the meeting was held in a public place, i.e., the open patio of a public restaurant. *Wilkins*, 71 Cal. App. 4th at 1078.
  - 65. Med Lab, 306 F.3d at 817.
  - 66. Id. at 818 n.6.
  - 67. Id.
- 68. *Id.* at 819 (quoting Medical Laboratory Management Consultants v. ABC, 30 F. Supp. 2d 1182, 1193 n.11 (D. Ariz. 1998)).
  - 69. Id. at 820 n.7.
- 70. 26 Med. L. Rep. 1956, 1958 (C.D. Cal. 1997) (citing Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999)).
- 71. Russell v. ABC, Inc., 23 Med. L. Rep. 2428, 2434 (N.D. Ill. 1995).

# Communications Lawyer Editorial Advisory Board 2003-2004

# C. Thomas Dienes

George Washington University Law School tdienes@main.nlc.gwu.edu

# George Freeman

New York Times Co. freemang@nytimes.com

# Karlene Goller

Times Mirror Co. Los Angeles karlene.goller@latimes.com

# Elizabeth C. Koch

Levine, Sullivan & Koch, L.L.P. *bkoch@lsklaw.com* 

# Thomas S. Leatherbury

Vinson & Elkins tleatherbury@velaw.com

# Lee Levine

Levine Sullivan & Koch, L.L.P. *llevine@lsklaw.com* 

# George K. Rahdert

Rahdert, Steele, Bryan & Bole, P.A. *gkrahdert@aol.com* 

# Judge Robert D. Sack

U.S. Court of Appeals for the Second Circuit robert\_sack@ca2.uscourts.gov

# Kelli L. Sager

Davis Wright Tremaine LLP kellisager@dwt.com

# Bruce W. Sanford

Baker & Hostetler LLP bsanford@bakerlaw.com

# Richard M. Schmidt, Jr.

Cohn and Marks LLP rms@cohnmarks.com

# Rodney A. Smolla

T.C. Williams School of Law University of Richmond rsmolla@richmond.edu

# **Mark Stephens**

Finers Stephens Innocent *mstephens@fsilaw.co.uk* 

# Daniel M. Waggoner

Davis Wright Tremaine L.L.P. danwaggoner@dwt.com

# Barbara W. Wall

Gannett Co., Inc. bwall@gannett.com

# Solomon B. Watson IV

New York Times Co. watsons@nytimes.com

# Steven J. Wermiel

American University Washington College of Law swermiel@wcl.american.edu

# Richard E. Wiley

Wiley Rein & Fielding LLP rwiley@wrf.com

# From the Chair

(Continued from page 2)

it should not come as a surprise. The good news was that the audience we did have was riveted.

Our presentation at the Minority Lawyer conference was preceded by a plenary session entitled "The World According to Bakke: We Can't Define Affirmative Action, But We Know It When We See It." This panel focused on the Grutter v. Bollinger case over affirmative action in the University of Michigan Law School admissions program that had been argued before the U.S. Supreme Court but not decided at the time of the meeting. That discussion, as well as the other pre-decisional harangue in various media, revealed how the issue of affirmative action has become realigned in the twenty-five years since Bakke. The administration generally opposes it; GM, 3M, and other major corporations filed amici briefs supporting it, at least when it is part of a nuanced selection process; amici military leaders declared that diversity in armed forces in leadership was essential to national security; and spokespersons for Asians and Jews opposed it, arguing that racial preferences frustrate diversity and the flourishing of individual merit when they result in quotas, like those used in recent history, to cap the number of Jewish or Asian students. Some of the views expressed by amici were entrenched well before Bakke. Forum member Chuck Simms filed an eloquent brief for an impressive group of liberal arts colleges and universities led (in alphabetical order) by his (and that of your current and immediate past chairs) alma mater, Amherst, showing those institutions' steady commitment to and positive experience from diversity since the 1960s, and demonstrating how diversity is indispensable to their educational missions.

The decision in Grutter, two weeks old at the submission of this column. lauded diversity in general and embraced it in particular as a basis for racial and ethnic preferences in the context of higher education. However, the

Court did so based in unarticulated part upon deference to the expertise of the academy in determining what makes that educational process work best. Tacit in the O'Connor majority's willingness to defer is the intuitive notion that the intrinsic and "compelling" value of diversity is something very difficult to prove in court (notwithstanding the submission of studies that the Court found worthy of mention). As First Amendment advocates, I suppose, we should not be anxious to see the Court take starch out of strict scrutiny by recognizing forms of compelling interests that are not fully substantiated. Yet it seems to me that ethnic diversity in our institutions is so basic to the society we want that it should qualify as one of those "self-evident" truths-much like the "marketplace of ideas" or the "chilling effect" of content-based sanctions, worthy of acceptance under our Constitution without scientific proof of validity or deference to expertise.

Justice O'Connor's observations concerning the importance of diversity in legal education have much applicability to the legal profession because the absence of meaningful racial and ethnic diversity saps our strength and credibility as advocates and leaders. By "meaningful diversity," I am referring to achievement of a "critical mass" for each underrepresented group, which means, among other things, a sufficient number to permit lawyers of color to participate as individuals, and not merely as representatives of a group. As demonstrated at the diversity break-out sessions at the last Annual Conference, our bar seems willing to accept the intrinsic value of diversity in our profession as an article of faith.

If you found the Court's compulsion to defer unsatisfying, you must have winced at the Court's pronouncement that "we expect that twenty-five years from now, the use of racial preferences will no longer be necessary to further the interest approved today." Right. Is this an attempt to instill a "can-do" attitude (as in, "Houston, we have a little problem up here"), or is someone failing to recognize how profoundly our society's

opportunities remain a function of membership in an ethnic or racial group?

The favored argument of those who oppose racial preferences is as articulated by Justice Thomas, as principal dissenter in Grutter, that whenever government "makes race relevant to the provisions of burdens and benefits, it demeans us all." Even in the private sphere, opponents of affirmative action complain that it perpetuates "racethink." Was our last Annual Conference, in which we dedicated a workshop to discussion of diversity with reference to lawyers of color, shortsighted, demeaning, and counterproductive? I think not. More importantly, I believe that the converse is true; not only does colorblindness slow movement from the status quo, but it also glosses over the fact that our society is still suffering from deep wounds wrought by "discrimination" (for much of what happened, this term is a euphemism for the infliction of unspeakable suffering based upon race). To insist upon colorblindness at this point—at best an intermediate stage of the healing process—not only ignores the lasting effects of discrimination, but also forces the wounds to heal from within, randomly and defectively, without the beneficial effects of sunlight and oxygen, to borrow some Brandeisian imagery. Just as we presume that more speech is better than less, the best way to realize the beneficial effects of racial and ethnic diversity is by openly seeking them. Justice Blackmun said it well in his concurrence in Bakke. "In order to get beyond racism, we must first take account of race. There is no other way."

The ABA year wound up with its Annual Meeting in San Francisco in August. On Friday, August 8th, we presented (with TIPS, the Litigation Section, and others) a Presidential Showcase program entitled "Celebrities and the Right of Publicity: Joe Montana Takes the Field." George Freeman moderated a panel made up of legal stars and, of course, Joe Montana.

Meanwhile, your Annual Conference planning committee will be working on what promises to be a most interesting program for Boca Raton in January. See you there.

# **COURTSIDE**

# head

PAUL M. SMITH, DONALD B. VERRILLI, JULIE CARPENTER, AND DEANNE E. MAYNARD

# TO COME

Paul M. Smith (psmith@jenner.com), Donald B. Verrilli (dverrilli@jenner.com); Julie Carpenter (jcarpenter@jenner.com); and Deanne E. Maynard (dmaynard@jenner.com) are partners in the Washington, D.C., office of Jenner & Block.

Summer 2003	☐ Communication	s Lawyer 🛭 27

# PLAN NOW TO ATTEND!

American Bar Association
Forum on Commmunications Law
Eighth Annual Conference
January 22-24, 2004
Boca Raton, Florida

For details contact Teresa Ücok at 312 • 988 • 5658



Nonprofit Organization U.S.Postage PAID American Bar Association