In this issue

COVER STORY
Jackpot! Presumed Damages Gone Wild—and Unconstitutional .......................... 1
This article argues that presumed damages violate fundamental notions of fairness by chilling speech and punishing unpopular speakers who dare criticize government officials and public figures, running afoul of the First Amendment and the due process clause of the Fourteenth Amendment.

Click Here to Accept the Terms of Service .............................................. 4
This article addresses the key features of the most common types of online agreements—clickwrap and browswrap agreements—the circumstances under which courts have upheld such agreements, and best practices for ensuring the agreements are enforceable.

CDA No Bar to Failure to Warn Actions Against Website Operators ...................... 8
The Ninth Circuit Court of Appeals recently carved out a dangerous exception to CDA immunity that may be exploited by plaintiffs who seek to shift liability to website operators for injuries caused by other website users.

Access to Cloud-Based Public Records .................................................. 12
This article examines the issues that digitized government records pose for citizens and journalists who wish to mine the burgeoning data repository to discover “what their government is up to.”

Jurisdictional Issues in Anonymous Speech Cases ....... 23
Courts have traditionally paid less attention to the jurisdictional issues relating to the unmasking of anonymous speakers. But two recent cases highlight the importance of jurisdictional considerations in the protection of anonymous speech.

Jackpot! Presumed Damages Gone Wild—and Unconstitutional

SUSAN E. SEAGER

Las Vegas casino billionaire Steve Wynn recently hit a judicial jackpot in Los Angeles with a $17 million jury award for presumed damages in his slander per se lawsuit against Joe Francis, the volatile creator of the Girls Gone Wild video empire.

Never mind that Wynn presented no evidence that anyone believed Francis’s absurd statement. Even the newsman who reported the statement said he didn’t believe Francis, who blurted in court that he heard that Wynn had threatened to hit Francis “in the back of the head with a shovel and bury him in a hole in the desert,” due to Francis’s $2 million gambling debt. Wynn presented zero evidence to the jury of any actual reputational or economic harm to himself. Yet the judge instructed jurors with the standard California instruction for presumed damages that Wynn was “entitled to receive compensation for this assumed harm in whatever sum you believe is reasonable.” The jury decided $17 million was reasonable for presumed reputational damages, and awarded another $3 million for mental anguish.

In 2007, Illinois Supreme Court Chief Justice Robert Thomas won a $5 million jury award for presumed damages in his libel per se lawsuit against a small Chicago-area newspaper and reporter. The Illinois jury handed out the multimillion-dollar award despite the lack of any independent evidence of reputational or economic harm. To the contrary, reputation witnesses testified that Justice Thomas “still enjoy[ed] a good reputation,” had been honored by bar associations, and elevated to chief justice of the Illinois Supreme Court after the news report.

Posttrial evidentiary challenges to the two presumed damages awards met with little or no success. The trial court rejected Francis’s challenge to the size of the presumed damages award and affirmed the entire $17 million award. Justice Thomas’s presumed damages award was “reduced” as excessive by the trial court from $5 million to $3 million. No First Amendment or due process challenges were made to the presumed damages awards in either case. In sum, these presumed damages awards resemble casino jackpots more than carefully weighed court awards supported by hard evidence and subject to meaningful judicial review.

Presumed damages appear to be gaining popularity with public figures and public officials. In California, Wynn filed another lawsuit for slander per se in September 2014 against hedge fund manager James Chanos. In Illinois, a Chicago trial court judge expressly cited Justice Thomas’s big court win when the trial judge demanded $7 million in his 2011 defamation per se lawsuit, saying he was demanding the jury award won by Justice Thomas (who was awarded

(Continued on page 30)
WHAT CLIENTS WANT

DAVID J. BODNEY

Many things unite us as media lawyers. Perhaps what binds us together the most is our commitment to client service. We serve clients whose role in our democracy, and around the world, could not be more important.

What do media clients expect of their lawyers? What don’t they expect? And how have their expectations changed over the years?

Whether we have practiced communications law for decades or are only now beginning the journey, learning the answers to these three questions can help us serve our clients better. So I posed these questions in turn to three individuals who have dedicated their professional lives to journalism, and to building strong news organizations with their fair share of legal challenges.

A few lessons emerged:

Keep Pace with Changing Technology

“You’ve got to keep up with the changing technology and its implications,” said Sue Clark-Johnson, who served as vice president of Gannett Company’s publishing division and was responsible for more than 100 newspapers, along with websites and magazines.

“The changing technology is changing the very definition of ‘journalist,’” she noted, and the “rapidity of technological change” is not only transforming the content of news but also the legal climate that protects its distribution.

“There’s so much data coming at me, it’s like a Category 5 snowstorm,” said Michael Lacey, who, as executive editor of New Times, built a campus “underground” newspaper into the country’s largest chain of metropolitan newsmagazines with its acquisition of the Village Voice. Lacey described the Internet as “so bang-on stupid on so many levels,” and predicted that it will “drive how print and TV operate.” Consequently, lawyers must play a role in making sure that the Internet’s “dumbing-down” tendencies don’t lead to a lowering of standards for journalists who take their work seriously.

Len Downie, Jr., who began his career in 1964 as a reporter at The Washington Post, rose to become its executive editor and now serves as vice president at large, noted that “the basics [of journalism] haven’t changed very much, but the technology has changed.” As Downie observed, “there are new legal issues associated with the new technology.”

With “tweeting and blog posts not necessarily going through editors,” he added, reporters need to know the legal rules, and lawyers need to understand the changing technology to advise them.

Know Our Newsrooms and Our Business

Downie emphasized the importance of having lawyers who are “immersed in journalism, not just court decisions.” He described the media lawyer’s role as one of “collaboration” and “partnership” with the client. When editors and reporters meet with their counsel, it should not be “like you’re going to the principal’s office,” Downie said. Rather, media attorneys should “enjoy dealing with journalists,” and read what their media clients and journalists at other news organizations are publishing.

“The most interesting job at the paper should be the lawyer’s,” Lacey commented. Assuming the lawyer understood the “formulaic” world of journalism’s “inverted pyramid,” Lacey expected his lawyers to grasp the “laziness of the formula” and help ensure that it’s not replaced by the “laziness of the echo chamber.” To serve media clients well, lawyers need to understand what’s happening in journalism and encourage reporters to “take the extra step and find out what’s really happening” behind the headlines and public records.

“Google, Facebook, YouTube—they’re making the decisions that had been made by journalists,” observed Clark-Johnson. She noted ISIS’s beheadings in the Middle East, and the decision by media outlets to put video footage of atrocities on the web. “Can the lawyers address these issues?” she asked. To handle the work, attorneys must understand the changing news business, and the daily decisions that editors and publishers face across platforms.

Tell Us What You Really Think

“Tell me what you think — what do you THINK?” Clark-Johnson underscored. In today’s economic climate, it is not enough for the lawyer simply to acquaint the client with the risks.
Editors and publishers want to know if they can win a legal battle. If they can’t win, she said, the media client may not want to fight it.

“Don’t tell me ‘on the one hand this, and on the other hand that,’” Lacey said. “I know I’m facing exposure no matter what I do,” he added. “Don’t tell me what I can’t do, but extend the borders of what I can do,” Lacey urged. He said he expects an honest answer to the question, “can you see your way to defend this?”

Of course, the client expects the lawyer to know the law. As Lacey put it: “The lawyer should see every dangerous story in a way I couldn’t see it.” Adds Downie: in pre-publication review, the client expects the lawyer to know “every aspect” of risk, and to identify not just the obvious adversary but also the story’s unintended plaintiffs. Clark-Johnson said the media client certainly needs to know she has “24-hour access” to her attorney – for example, when a reporter gets “thrown out of a city council meeting at seven o’clock at night.”

But the most revealing lesson from these giants of journalism may have been a fourth client expectation.

Help Us with Overall Fairness and Accuracy

Downie said lawyers often think about basic issues of “fairness” and “accuracy,” while reporters and editors may not be looking at the publication in quite the same way. He said a media lawyer should be expected to answer this question from the client: “I know there’s nothing ‘actionable’ in the story, but do you really think it’s fair?” Downie pushed the point, saying “good journalists want to hear about that [fairness issue] from good lawyers.” They want to know, he said, how to get the story published “without legal harm – and be fair and accurate.”

Lacey encapsulated the notion in another way. He described lawyers as “gatekeepers of the accord.” When asked to elaborate, he defined the accord as the “agreement governing the standards” of good reporting, and said lawyers are needed for the “enforcement of the standards.” For example, Lacey said the attorney should be asking whether the reporter and editor have challenged the contradictory information and assumptions in the draft story.

Clark-Johnson, like Downie, underscored the importance of lawyers who can educate their clients. “The educational component, due to the changing role of journalists and technology,” she noted, is essential to client service. With journalists “shooting video and taking pictures as opposed to using only notepad and paper,” there is a critical need to educate the media client. Not only episodic advice about “cameras and cell phones” in court and on the streets but also “periodic training” of media clients is vital.

Oh, and what would really be appreciated, Clark-Johnson added, is a “business model for newspaper survival.”

---

**NEW Media Lawyers Advocates Showcase**

**Fairmont Scottsdale Princess, Scottsdale, AZ**

February 6, 2015 • 4:45 pm — 6:00 pm

Presented by the Women in Communications Law (WICL)

The Showcase will be a presentation-centered training opportunity for lawyers who have been in practice for at least five, no more than ten years. Participants will plan and deliver a seven-minute presentation on a media-related topic, much as they might deliver in pitching business to a new or existing client.

For additional information on the Showcase, please contact WICL co-chairs Robin Luce-Herrmann at luce-herrmann@butzel.com or Rosemary Harold at rharold@wbklaw.com.

**Sponsors:** Ballard Spahr, Davis Wright Tremaine, Hiscox, Jackson Walker, Kelley Drye, Levine Sullivan Koch & Schulz, Sheppard Mullin, Richter & Hampton, Vinson & Elkins

To attend the Showcase, register for the Forum Annual Conference at www.americanbar.org/groups/communications_law.html.
“Click Here to Accept the Terms of Service”

ALLISON S. BREHM AND CATHY D. LEE

In today’s online-centered world, website owners and website users are necessarily reaching agreements, all the time. These agreements govern a variety of terms, from license agreements to privacy policies to choice of law. Courts typically have grouped these contracts into “clickwrap” or “browsewrap” agreements, depending on the manner in which the consumer has notice of or otherwise assents to the terms of the agreement. Given that the terms usually involve an exchange of rights and obligations between a website owner and user, disputes over the enforceability of such agreements abound.

Many times those disputes receive significant media attention, bringing a company’s particular policies and practices into sharp public focus. Indeed, one such online agreement that garnered media attention recently was Facebook’s data use policy, on which the company relied when defending the social experiment it conducted on hundreds of thousands of users’ newsfeeds. The public outcry that resulted illustrates the importance of clarity and fairness when forming contracts online, particularly when significant rights are at stake—for both the website owners and the users.

This article will address the key features of the most common types of online agreements—clickwrap and browsewrap agreements—the circumstances under which courts have upheld such agreements, and best practices for ensuring the agreements are enforceable.

How Clickwraps and Browsewraps Are Used

Clickwrap and browsewrap agreements differ in presentation and functionality. Clickwrap agreements require a user to affirmatively click a box on the website acknowledging agreement to the terms of service, which are often available in a scrolling text box, before the user is allowed to proceed. Browsewrap agreements have hyperlinked terms of use that are typically found on a separate webpage, which the user does not have to visit to continue using the website or its services.

Whatever the name, these agreements govern a variety of terms, including software licensing, terms of use for utilizing a website, privacy policies, terms of sale, subscriber agreements, and credit card applications. The agreements have real ramifications because they can dictate a variety of terms critical both to users and website owners. Among other things, the agreements may govern where a lawsuit can be adjudicated, whether arbitration will be mandatory, whether a prohibition on copying a website’s content will be enforceable, and whether a provision limiting use of the website for noncommercial purposes will be enforceable.

At bottom, many of these terms are no different from those seen in the brick and mortar world, and thus the basic legal landscape for enforcement is not much different. Indeed, Internet commerce “has not fundamentally changed the principles of contract.”

To determine the enforceability of a clickwrap or browsewrap agreement, courts apply traditional principles of contract law and focus on whether the plaintiffs had reasonable notice of and manifested assent to the agreement. There is no manifestation of assent unless a party intends to engage in the conduct and knows or has reason to know that the other party may infer from his or her conduct that he or she assents.

Against this backdrop, courts have considered the presentation, form, and functionality of browsewrap and clickwrap agreements in determining whether there is a clear manifestation of assent.

Cautionary Tales

Browsewrap Agreements

Generally, courts have declined to enforce browsewrap agreements because the fundamental element of assent is lacking. As an initial matter, because no affirmative action is required by the user to agree to the terms other than use of the website, the validity of a browsewrap turns on whether a user has actual or constructive knowledge of a site’s terms.

For example, in Be In, Inc. v. Google Inc., a social media developer alleged that defendants Google Inc., YouTube, and Google UK breached the CamUp website’s terms of service by visiting the CamUp website to copy and exploit the website for the defendants’ social network platform. The home page of the CamUp website included a link to the “Terms of Service,” which stated that “by using and/or visiting this Website . . . you signify your agreement to these Terms of Use, [and] CamUp’s Privacy Policy.”

A district court in the Northern District of California found that the plaintiff failed to allege a contract was formed because beyond the existence of a hyperlink, there were no other allegations showing that the defendants were on notice that the mere use of the website would be interpreted as an agreement to the terms of service. Specifically, the plaintiff did not allege the size or typeface of the link, the central or obvious location of the link on the webpage, or even the text of the link. Accordingly, the plaintiff’s browsewrap agreement was not binding on the defendants.

The reluctance to hold browsewrap agreements enforceable is further supported by the Ninth Circuit’s recent decision in Nguyen v. Barnes & Noble Inc. In Nguyen, the plaintiff purchased Touchpads on Barnes & Noble’s website, but then was notified that his order had been canceled due to unexpected high demand. The plaintiff filed a class action on behalf of consumers whose Touchpad orders had been canceled,
alleging deceptive business practices and false advertising. Barnes & Noble moved to compel arbitration, based on the arbitration agreement in the website’s terms of use. The district court denied the motion. On appeal, the Ninth Circuit affirmed.

The critical question was whether Nguyen assented to the terms of use—specifically, the arbitration clause. Nguyen had neither clicked the hyperlinked terms of use nor read them.22 Barnes & Noble argued that Nguyen was on constructive notice of the terms. Barnes & Noble contended the placement of an underlined, color-contrasting hyperlink that read “Terms of Use” on the bottom left of every page on the Barnes & Noble website, and the hyperlink’s close proximity to the buttons a user must click on to complete an online purchase, were enough to place a reasonably prudent user on constructive notice.24 The court disagreed, concluding that the proximity and conspicuousness of the hyperlink alone is not enough to give rise to constructive notice. The court instructed that a textual notice of the terms of use, such as a final checkout screen reminding the user to review the terms, would likely give rise to sufficient notice.25 In so holding, the court cautioned that website owners must ensure their sites put users on notice of any binding contractual terms in light of the “range of technological savvy of online purchasers.”26

Despite the fact that browsewraps are typically held unenforceable, one court recently deemed a browswrap enforceable. In AvePoint, Inc. v. Power Tools, Inc., the “Terms and Conditions” provided that “[u]ser[s] may access, print and download materials and information on this Site solely for personal and noncommercial use.”27 The plaintiff alleged that the defendant breached the terms and conditions in its browswrap agreement by downloading a copy of the plaintiff’s software for competitive and commercial purposes. The defendant moved to dismiss on the grounds that the plaintiff had not alleged an enforceable contract.28

A district court in the Western District of Virginia disagreed. The court reasoned that the plaintiff alleged additional facts to support that the defendant had actual or constructive knowledge of the terms and conditions, instead of merely alleging the existence of a link at the bottom of the plaintiff’s website. Specifically, the plaintiff contended that the fact that the defendant went to the trouble of creating a fictitious profile and e-mail account to download the software suggested that the defendant knew about the terms and conditions and was aware that they prohibit users from downloading materials for commercial use. The plaintiff also claimed that because the defendant had a similar browswrap agreement on its own website that restricts the use of downloaded software, the defendant should have known that the plaintiff’s website had similar terms.29

AvePoint demonstrates that while browswrap agreements are generally not enforceable, courts may enforce such agreements when there are factual allegations—indeed, independent of the presentation of the agreement on the website—that support a user’s actual or constructive knowledge of a site’s terms and conditions.

**Clickwrap Agreements**

Unlike browswrap agreements, courts have routinely upheld clickwrap agreements.30 The enforceability of these agreements turns not on the label of “clickwrap,” but rather whether the party had constructive notice of the terms of the agreement and thus agreed to be bound by them.31

A Tenth Circuit decision from 2012, Hancock v. American Telephone & Telegraph Co., illustrates this principle.32 In Hancock, AT&T consumers argued that the clickwrap agreement did not give them notice of and meaningful opportunity to assent to the forum selection and arbitration clauses in the terms of service. AT&T technicians presented customers with a printed copy of the terms and gave customers an opportunity to review the terms, to which customers agreed by clicking on the “I Acknowledge” button on the technician’s laptop for the TV/voice terms.33 Customers also clicked on the “I Agree” button to manifest assent to the Internet terms, which customers had an opportunity to review in a scrolling text box.34 The court found the clickwrap agreements enforceable.35

Clickwrap agreements have been enforced even when the consumer did not read the agreement. For example, in Davis v. HSBC Bank Nevada, N.A., the plaintiff alleged that HSBC and Best Buy defrauded customers by offering credit cards without disclosing an annual fee.36 After reading an advertisement stating that applicants would receive a $25 reward certificate, the plaintiff decided to apply for the credit card. While applying, the plaintiff was directed to the terms and conditions, which were available in a scrolling text box on Best Buy’s website. The plaintiff did not read the terms, but he checked the box stating that he agreed to the terms and conditions. After the plaintiff’s application was approved, the plaintiff received his credit card and an “Additional Disclosure Statement.” Upon reading the latter, the plaintiff learned that there was a $59 annual fee for using the card. At that point, the plaintiff revisited Best Buy’s website and discovered the annual fee.37

The plaintiff filed a class action complaint alleging false advertising, fraudulent concealment, and unfair competition. The plaintiff contended that the relevant portions of the terms and conditions were not visible without scrolling down.38 The Ninth Circuit affirmed the dismissal of the plaintiff’s complaint with prejudice.39 The court found that the plaintiff’s failure to read the terms and conditions before checking the box accepting the terms irrelevant to determining enforceability. The court reasoned that the annual fee was “within [the plaintiff’s] observation” because he was able to discover it when he revisited Best Buy’s website and scrolled through the terms and conditions.40

**Hybrid Clickwrap-Browswrap Agreements**

Online agreements do not always fit neatly within the clickwrap or browsewrap categories. Sometimes, the agreements display features of both. In Fieja v. Facebook, Inc., the District Court for the Southern District of New York considered the enforceability of the forum selection clause in the hybrid clickwrap-browswrap agreement between Facebook and its user, requiring that all disputes be litigated in California.41

The Facebook page stated, “By clicking Sign Up, you are indicating that you have read and agree to
The more an online agreement resembles a traditional clickwrap agreement, the more willing courts are to find constructive assent.

The court commented that Facebook’s terms of use are like a browsewrap in that the terms are only visible via a hyperlink, but also like a clickwrap in that the user must click “Sign Up” to assent to the hyperlinked terms. The court analogized Facebook’s terms to a sign next to a bin of apples that says, “By picking up this apple, you consent to the terms of sale by this fruit stand. For those terms, turn over the sign.” Applying that analogy to the instant case, the court saw no reason why the agreement should not be upheld simply because Facebook’s terms of use appear on another screen. The court concluded that the Facebook user consented to Facebook’s terms of use and also to the forum selection clause therein, and thus granted Facebook’s motion to transfer to the Northern District of California.

Fleja shows that the more an online agreement resembles a traditional clickwrap agreement, the more willing courts are to find the notice necessary to give rise to constructive assent. Specifically, a major factor for the Fleja court in holding the agreement enforceable was that Facebook informed the user of the consequences of clicking “Sign Up,” and showed the user where to click to understand those consequences.

Another recent case signals the enforceability of these hybrid agreements. In Tompkins v. 23andMe, Inc., a district court in the Northern District of California determined that just because the hyperlinked terms of service were not presented in the same screen does not mean that customers lacked adequate notice of the agreement. After the Food and Drug Administration informed the defendant that it was violating the law by selling genetics services without approval, the plaintiffs brought class actions alleging false advertising, unfair competition, and consumer protection claims. The plaintiffs’ receipt of genetic information took place in two steps: (1) the plaintiffs bought DNA kits online from the defendant, and (2) the plaintiffs created accounts and registered their DNA kits online and sent DNA samples to the defendant.

At the purchasing stage, the terms of service were accessible via a hyperlink at the bottom of the defendant’s homepage under “LEGAL,” but customers were not required to view the terms or to click to accept the terms. At the subsequent account creation and registration stage, the webpage required customers to check a box next to the statement, “Yes, I have read and agree to the [blue hyperlinked] Terms of Service and Privacy Statement.”

The defendant filed a motion to compel arbitration, arguing that the arbitration provision in the terms of service was enforceable. The court concluded that the plaintiffs had not agreed to the terms of service at the purchasing stage, but that the terms of service took effect upon the account creation and registration stage. After considering various defenses to arbitrability, the court granted the defendant’s motion to compel arbitration.

One recent case underscores that the visibility of the hyperlink to an agreement is critical in determining enforceability. In Harris v. comScore, Inc., before consumers could download and install comScore’s software, the purchasers had to click a box acknowledging that they agreed to the terms of the license agreement, which terms could be accessed through a hyperlink. The terms contained a forum selection clause. A dispute arose when the plaintiffs claimed that comScore had improperly obtained and used personal information from the plaintiffs’ computers after they downloaded and installed the software.

The defendant moved to dismiss the plaintiffs’ complaint on the ground of improper venue, claiming the dispute should be adjudicated in Virginia because of the forum selection clause in the license agreement. The plaintiffs disagreed, contending that the terms of service were obscured during the installation process in such a way that the average consumer would not notice the hyperlinked terms.

The court agreed with the plaintiffs, explaining that the defendant had not provided sufficient detail about how the hyperlinked agreement was presented to the user. It was not clear that the user could reasonably find the hyperlink to the terms or manifest assent to it during the installation process. The court noted that it must accept the complaint’s factual allegations as true, and thus declined to infer that clicking a box acknowledging that a user had read an agreement indicates that the agreement was reasonably available to the user, particularly when the plaintiffs alleged that the hyperlink to the agreement was obscured. The court concluded that the forum selection clause was not reasonably communicated and denied the defendant’s motion.

Best Practices for Ensuring Enforceability

A review of the decisions addressing online agreements—whether clickwraps, browsewraps, or a combination of both—reveals that there are a variety of ways to increase the likelihood that the agreements will be enforced, and these can be easily followed by website owners:

• There is a check-box that users must click adjacent to an affirmation similar to, “By clicking on the box, you are indicating that you have read and agree to the Terms of Use”;
• The webpage is designed so that if the user does not check the box manifesting assent to the terms, the user cannot proceed in the transaction;
• In addition to a check-box that users must click, the terms of use are available either in a nearby scrolling text box or a nearby hyperlink;
• Any hyperlink of the terms is obvious, e.g., “Terms of Use” is underlined and has decent size lettering and visible coloring (not small lettering and not obfuscatory coloring);
• Any hyperlink of the terms has
a central or obvious location on the webpage, e.g., the hyperlink is directly below the “I Agree” button (not relegated to the bottom of the webpage, which would require the user to scroll down to a submerged portion of the webpage);

- Any hyperlink of the terms immediately displays the terms (instead of requiring the user to click on a series of hyperlinks to view the terms);
- The terms of use are evident in every webpage on the website (rather than visible on only one webpage), in addition to requiring users to attest that they have read the terms of use;
- The terms are in readable font (at least 12 point); and
- The agreement contains all requisite elements of an enforceable contract (e.g., consideration, sufficiently definite material terms, etc.).\(^{58}\)

Both website owners and users stand to benefit from such clear presentation of the terms. The owners have more certainty in knowing that the agreements will be upheld, and the users have a greater understanding of the terms dictating their use of the website or any commercial transaction. Ultimately, the more that an agreement looks like a clickwrap (i.e., requiring users to check the box next to the statement, “I have read and agree to the Terms of Use”), the more willing courts will be to find the notice necessary to give rise to constructive assent and enforce the agreement.\(^{59}\)

Endnotes

1. The phrases “terms of use” and “terms of service” are often used interchangeably. See Be In, Inc. v. Google Inc., No. 12-CV-03373-LHK, 2013 WL 5568706, at *6 (N.D. Cal. Oct. 9, 2013).
6. Id. at *8.
16. Be In, 2013 WL 5568706, at *6 (citing Restatement (Second) of Contracts § 19 (1981)).
20. Id. at *8.
21. Id. at *9.
22. 763 F.3d 1171, 1173 (9th Cir. 2014).
23. Id. at 1174.
24. Id. at 1177.
25. Id. at 1178.
26. Id. at 1179.
28. Id. at 509.
29. Id. at 510–11.
32. 701 F.3d 1248, 1251 (10th Cir. 2012).
33. Id. at 1253.
34. Id. at 1254.
35. Id. at 1258.
36. 691 F.3d 1152, 1157 (9th Cir. 2012).
37. Id. at 1158.
38. Id. at 1159–60.
39. Id. at 1159, 1171.
40. Id. at 1163.
42. Id. at 835.
43. Id. at 838.
44. Id. at 839.
45. Id. at 841.
47. Fteja, 841 F. Supp. 2d at 840.
49. Id. at *1–2.
50. Id. at *3.
51. Id. at *2–3.
52. Id. at *3.
53. Id. at *1, *5.
55. Id. at 925.
56. Id. at 925–26.
57. Id. at 926–28.
58. See Davis v. HSBC Bank Nev., N.A., 691 F.3d 1152, 1158 (9th Cir. 2012);
59. See Davis v. HSBC Bank Nev., N.A., 691 F.3d 1152, 1158 (9th Cir. 2012);

Ninth Circuit Court of Appeals Holds that Communications Decency Act Does Not Bar Actions against Website Operators for Failure to Warn

ROBERT L. ROGERS III

For years, courts across the United States have consistently held that the Communications Decency Act (CDA) immunizes website operators from liability for negligently failing to protect website users from other website users. However, in a recent opinion reversing the dismissal of a negligent failure to warn action against modelmayhem.com, the Ninth Circuit Court of Appeals carved out a dangerous exception to this CDA immunity that may be exploited by plaintiffs who seek to shift liability to website operators for injuries caused by other website users.

Claims Asserted against Internet Brands by “Jane Doe No. 14”

Doe No. 14 v. Internet Brands, Inc. involves disturbing allegations about the rape of a member of modelmayhem.com. Model Mayhem is “a networking site for professional and aspiring models to market their services” owned and operated by the defendant, Internet Brands. It has over 600,000 members. The plaintiff, “Jane Doe No. 14,” an aspiring model who listed contact information on the Model Mayhem site, claims that nondefendants Lavont Flanders and Emerson Callum found her profile on the website, contacted her in 2011, and falsely claimed to be talent scouts. She further claims that they lured her to an “audition,” drugged her, raped her, and filmed the rape with the intent to sell the recording as pornography.

Doe further asserts that Flanders and Callum had drugged, raped, and filmed the rapes of other models before they assaulted her. She contends that Internet Brands knew about these activities for years, as they had sued the prior owner of the website in 2010 for “failing to disclose the potential for civil suits arising from the activities of Flanders and Callum.” In fact, Flanders and Callum were convicted and sentenced to life in prison in 2012 for drugging and raping models, filming the rapes, and selling the films as pornography.

In her lawsuit against Internet Brands, the plaintiff asserted a single count for negligent failure to warn under California common law. The U.S. District Court for the Central District of California dismissed Doe’s action with prejudice solely on the grounds that Internet Brands was immune from her claim under the CDA. However, the Ninth Circuit Court of Appeals reversed, holding that Doe’s failure to warn action was not barred by the CDA because she “does not seek to hold Internet Brands liable as a ‘publisher or speaker’ of content someone posted on the Model Mayhem website.”

The Ninth Circuit’s decision in Doe No. 14 turned on several unique facts that appear infrequently in cases in which website operators seek defensive protection under the CDA. However, the court’s broad holding could be exploited by future plaintiffs seeking to avoid limitations imposed by the CDA in a wider variety of actions against website operators.

CDA Section 230 and Liability of Website Operators

The CDA immunizes website operators for content posted on their websites by others by prohibiting providers of “interactive computer services” from being treated as “the publisher or speaker of any information provided by another information content provider.” The CDA also immunizes website operators for their editorial activities, including actions to “restrict access to or availability of material that [they] consider[] to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.”

Courts have construed these provisions to bar lawsuits seeking to hold website operators liable for their “exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content.” Courts have also long held that website operators are not liable for defamatory posts by website users merely because they invite visitors to post potentially defamatory statements, even if they refuse to remove offensive or defamatory content from their sites.

Ninth Circuit’s Holding in Doe No. 14

In Doe No. 14, the Ninth Circuit refused to apply CDA protection to Internet Brands because of two unusual facts that the court believed distinguished Doe’s negligence action from others rejected under CDA analysis.

First, Flanders and Callum did not post content on the Model Mayhem website. Instead, they trolled models’ profiles posted on the website looking for potential rape victims and contacted the models directly, without posting messages on the website. The Ninth Circuit therefore observed that Doe “does not seek to hold Internet Brands liable as a ‘publisher or speaker’ of content someone posted on the Model Mayhem website, or for Internet Brands’ failure to remove content posted on the website.” Instead, Doe attempts to hold...
Internet Brands liable only “for failing to warn her about how third parties targeted and lured victims through Model Mayhem,” either by posting a notice about Flanders and Callum on the Model Mayhem website, or by sending its 600,000 users an e-mail warning them about Flanders and Callum.15

Second, Internet Brands knew before Doe was raped about “the potential for civil suits arising from the activities of Flanders and Callum” in relation to other models who had posted profiles on the Model Mayhem website.16 In other words, Internet Brands knew before Doe was drugged and raped that other models had claimed they were drugged and raped by Flanders and Callum.

Based on these facts, the Ninth Circuit held that the CDA does not bar Doe’s negligent failure to warn action because:

Posting or emailing such a warning could be deemed an act of publishing information, but section 230(c)(1) bars only liability that treats a website as a publisher or speaker of content provided by someone else: in the words of the statute, “information provided by another information content provider.” A post or email warning that Internet Brands generated would involve only content that Internet Brands itself produced. An alleged tort based on a duty that would require such a self-produced warning therefore falls outside of section 230(c)(1). In sum, Jane Doe’s negligent failure to warn claim does not seek to hold Internet Brands liable as the “publisher or speaker of any information provided by another information content provider.”17

The Ninth Circuit further opined that the “core policies” underlying the CDA—to prevent litigation against website operators from chilling third-party content because her “failure to warn claim has nothing to do with Internet Brands’ efforts, or lack thereof, to edit or remove user generated content.”19 Notably, the court conceded that its decision could have a chilling effect on the Internet by increasing the expense of operating an Internet business, but it characterized that chilling effect as “marginal.”20

The court also characterized the CDA provisions immunizing website operators from tort claims as “narrow,” and held that “[b]arring Jane Doe’s failure to warn claim would stretch the CDA beyond its narrow language and purpose.”21

**Erroneous Holdings in Doe No. 14 and Their Impact on Website Operators**

The Ninth Circuit’s decision in *Doe No. 14* contradicts a long line of cases holding not only that the CDA immunity provisions are to be construed broadly, but also that the CDA bars negligence actions seeking relief for failure to warn or protect.22 The court also places mistaken emphasis on Flanders and Callum’s decision to communicate directly with Doe instead of through the Model Mayhem website. Its holding should also be questioned for suggesting that website operators will be only “marginally” affected by its ruling.

**Immunity for Editorial Decision to Publish Warning on Website**

Courts in other circuits have long held that the CDA immunizes website operators for actions claiming that they negligently failed to protect website users from harm caused by other users. For example, in *Green v. America Online (AOL)*, the Third Circuit held that the CDA immunized AOL from liability for negligently failing to police its services and protect one of its users from another user who transmitted a “punter” signal that disabled the plaintiff’s computer, even after the plaintiff complained to AOL about the activity.23 In *Doe v. MySpace, Inc.*, the Fifth Circuit held that the CDA immunized MySpace from liability for negligently failing to “institute and enforce appropriate security measures” that would have prevented an underage user from meeting and being sexually assaulted by another user.24 In *Beckman v. Match.com*, the U.S. District Court for the District of Nevada held that the CDA immunized Match.com from liability for negligently failing to warn and protect a user “from individuals trolling the website to further criminal activity,” including an alleged “serial murderer” who brutally attacked the plaintiff after the two met through the website.25

One might argue that each of these cases can be distinguished from *Doe No. 14* because Flanders and Callum never posted content on the Model Mayhem website, whereas the sender of the punter signal in *Green*, the alleged rapist in *MySpace*, and the “serial murderer” in *Beckman* all posted content on the websites at issue. But this distinction is irrelevant. The CDA’s protections do not apply solely to defamation actions seeking relief for statements posted on websites by users.26 The CDA also immunizes website operators for other functions related to their management of their websites, including actions taken to enable users to restrict access to their own content.27

The CDA’s protections do not apply solely to defamation actions seeking relief for statements posted on websites by users.

Other circuit courts have construed the CDA broadly to immunize website operators from liability for their “exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content.”28 Few decisions could be more quintessentially related to Internet Brands’ traditional editorial functions than its decision about whether to post a message on modelmayhem.com about possible harm posed to users by Flanders and Callum.

The Ninth Circuit therefore was not compelled by the CDA to reject the immunity recognized by the district court simply because Flanders and Callum never posted content on
The implications and potential burdens imposed on website operators by the decision are far-reaching and considerable.

Considerable Chilling Effect of Doe No. 14
One must also question the Ninth Circuit’s dismissal of the potential chilling effect of its decision and its impact on the operation of websites as “marginal.” The court seemed reassured in reaching this conclusion by the fact that Internet Brands could have protected Doe, and thereby avoided the lawsuit, merely by sending a single e-mail or posting a single message on its website about two specific persons known to have been accused of violent crimes. But the implications and potential burdens imposed on website operators by the decision are far-reaching and considerable. Even Doe’s own reasoning leads inescapably to the conclusion that the burden posed by the court’s decision is more than “marginal.”

Take first only the facts alleged by Doe against Internet Brands. She alleges, not that Internet Brands knew that Flanders and Callum had actually drugged and raped other users of the Model Mayhem website, but instead that Internet Brands knew that other members of the website had claimed Flanders and Callum drugged and raped them. Although Flanders and Callum had been arrested on charges related to such crimes in 2007, those charges were dropped, and Flanders and Callum were not actually convicted of drugging and raping any women until December 2011.

Therefore, before Internet Brands could have e-mailed or posted any statement about Flanders and Callum, it would have had to investigate the claims made by other users. Such an investigation would have required an exertion of time, energy, and financial resources by Internet Brands that would have been more than “marginal.” Furthermore, even if Internet Brands had concluded after such an investigation that Flanders and Callum had actually committed the crimes, Internet Brands would have had to weigh the risk of exposing itself to liability for potential defamation claims by Flanders and Callum if Internet Brands chose to warn its users about them (because the CDA clearly would not have shielded Internet Brands from liability for any statements it made about Flanders and Callum to its users).

When one looks beyond the unique facts of this specific lawsuit, the large burden imposed by the court’s decision becomes more clear. A website like Model Mayhem with 600,000 members could easily receive hundreds or thousands of complaints about persons with whom those members connected through the website. Must Internet Brands investigate all of those complaints, in order to determine which ones merit a warning to its users and which ones do not? Is Internet Brands required to risk liability for defaming the subjects of those complaints, simply to warn users of its website about potential risks posed by such persons, based simply on the conclusion of investigations that may be mistaken? The framers of the CDA could not have wanted website operators to be compelled to make such expensive investigations or to expose themselves to such liability. The costs of such investigations and liability—particularly for websites like Match.com designed to connect strangers for romantic interactions—could easily deter such websites from operating. The chilling effect of the Ninth Circuit’s decision in Doe No. 14 is therefore anything but marginal.

Conclusion
The Ninth Circuit seems to suggest that any failure to warn action, including those not involving rapists or violent crimes, is not subject to CDA immunity. Plaintiffs will therefore probably be tempted to try to extend the reach of the Ninth Circuit’s holding beyond the unique facts of Doe No. 14. The chilling effect on the operation of websites could be great if other courts continue to chip away at CDA immunity.

Endnotes
1. See, e.g., Doe v. MySpace, Inc., 528 F.3d 413, 419–22 (5th Cir. 2008) (affirming the dismissal with prejudice, based on immunity under the CDA, of negligence and gross negligence actions against MySpace for failing to enforce procedures that would have prevented the plaintiff from being sexually assaulted by another user); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122–25 (9th Cir. 2003) (affirming the dismissal, based on CDA immunity, of a negligence action against Metrosplash.com for failing to prevent users from misrepresenting the plaintiff’s identity and posting private information and invitations for sex on its website under her name); Green v. Am. Online (AOL), 318 F.3d 465, 470–72 (3d Cir. 2003) (affirming the dismissal, based on immunity under the CDA, of a negligence action against AOL for failing to police its services and protect a user from another who had sent the plaintiff a “punter” signal); Beckman v. Match.com, No. 2:13-CV-97, 2013 WL 2355512, at *3–7 (D. Nev. May 29, 2013) (dismissing with prejudice, based on immunity under the CDA, actions for negligent failure to warn and negligent misrepresentation against Match.com for failing to protect a user from an alleged “serial murderer” who trolled the website looking for victims); Doe v. SexSearch.com, 502 F. Supp. 2d 719, 724–28 (N.D. Ohio 2007) (dismissing, based on immunity under the CDA, actions against SexSearch.com for negligent misrepresentation and failure to warn for failing to prevent a user from having sex with a minor who had misrepresented her age, resulting in felony charges against the plaintiff).
Because it dismissed solely based on CDA immunity, the district court did not consider the merits of Doe’s action, including whether she had actually alleged a duty under California law that could support the negligence action she attempted to assert.

8. Id. at 897.
9. See id. at 897–98.
11. Id. § 230(c)(2).
14. Doe No. 14, 767 F.3d at 897.
15. Id. at 897–98.
16. See id. at 896.
17. Id. at 898 (citation omitted).
18. Id. at 898–99.
19. Id. at 898.
20. Id. at 899.
21. Id.
22. See supra note 1.
24. 528 F.3d 413, 419–22 (5th Cir. 2008).
26. Doe v. SexSearch.com, 502 F. Supp. 2d 719, 726 (N.D. Ohio 2007); see also Carafano v. Metrosplash.com, 339 F.3d 1119, 1123 (9th Cir. 2003) (recognizing that “reviewing courts have treated § 230(c) immunity as quite robust”).
28. See Green, 318 F.3d at 471; see also MySpace, 528 F.3d at 420; cf. Langdon v. Google, Inc., 474 F. Supp. 2d 622, 630–31 (D. Del. 2007) (dismissing actions against Google, Yahoo, and Microsoft seeking relief for their refusal to run the plaintiff’s advertisements, on the grounds that such actions are barred by the CDA because they seek to hold the website operators liable for their exercise of “traditional editorial functions”).

29. See Doe No. 14 v. Internet Brands, Inc., 767 F.3d 894, 899 (9th Cir. 2014).
30. See id. at 896.
31. See Kyle Munzenrieder, Emerson Callum and Lavont Flanders Convicted of Making Rape Form, Miami New-Times Blogs (Dec. 9, 2011), http://blogs.miaminewtimes.com/riptide/2011/12/ emerson_callum_and_lavont_flan.php. 32. The Ninth Circuit itself may have best explained the chilling effect of its subsequent decision in Doe No. 14 when it said in Carafano v. Metrosplash.com, Inc.: The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect. 339 F.3d 1119, 1124 (9th Cir. 2003) (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997)). The same reasoning applies to the burden of screening each complaint received from website users about other users and weighing whether each complaint merits a warning that could expose the website operator to liability for defamation.
Cloud-Based Public Records Pose New Challenges for Access

STEVE ZANSBERG

New York Governor Andrew Cuomo authorizes all state employees to destroy tens of thousands of e-mail records in which public business is discussed.1 Florida Governor Rick Scott and his staff use “private” Gmail accounts to keep their official communications from being publicly scrutinized on the governor’s highly touted “Project Sunburst” transparency website.2 Pennsylvania Governor Tom Corbett deletes his e-mails every two weeks, specifically so that they will not be subject to that state’s Right to Know Law (RTKL).3 Corbett’s key higher education adviser deleted his e-mails daily and later resigned after he responded to RTKL requests by producing only five e-mails for his entire first year in office.4 Colorado’s state legislature adopts a “read and delete” policy for all legislative staff e-mails.5 It seems every day brings forth another crafty maneuver by government officials to evade accountability and transparency mandates through data destruction, manipulation, or obfuscation.6

More information concerning the operations of government is being generated on a daily basis today than at any time previously—for example, in the predigital age, when pen, paper, and typewriter were the methods of written communications.7 And, in many instances, the cost of providing copies of that information has plummeted to practically zero. Yet, despite the exponential growth in the amount of data and the ease of storing and accessing it, ironically, these communications and data storage technologies have simultaneously raised new barriers to citizens’ ability to inspect those records under freedom of information (FOI) laws.

This article examines three related issues that digitized government records pose for citizens and journalists who wish to mine the burgeoning data repository to keep tabs on “what their government is up to”:9 (1) are e-mails and texts discussing public business, that are exchanged or housed on nongovernmental servers or devices, subject to disclosure under open records laws?; (2) what obligation do government employees have to retain e-mails and other electronically stored information so that they are available for inspection?; and (3) are citizens entitled to inspect and obtain copies of digital records in their “native format,” including database files and “metadata”?

Control: Whose Records Are They? Government entities across the nation are allowing, and even encouraging, public employees to utilize handheld devices not paid for by the government to communicate about public business; these governmental bodies are also retaining third-party vendors (e.g., Gmail, Yahoo!, etc.) to provide and maintain e-mail or text messaging accounts that are completely separate from, and inaccessible to, government servers.10 Thus, increasingly, courts and state attorneys general are being called upon to answer whether electronic records housed on such “private” communications devices and servers are subject to the states’ public records statutes, or are simply beyond their reach.

As with many issues discussed in this article, the application (or non-application) of various records laws to a particular category of record (here, e-mails discussing “public business” that are housed exclusively on a nongovernmental server or device) depends, in large part, on how the relevant statute defines “public record.” Most states have a version of a definition that defines public records as (1) any “writing,” usually defined quite broadly to include any written communication “regardless of physical form or characteristics”; (2) that is “made, maintained, or kept” by a government employee or over which a government agency has either physical custody or a right of access; and (3) whose content bears some logical connection to the conduct of public business.12 Thus, electronic communications that address “purely private,” nongovernmental matters, have been found not to be “public records,” even if they are exchanged over, and/or housed upon, government-funded communications devices (because all three conditions above must be satisfied).13

This article addresses whether the converse is true: is a record that is “made, maintained, or kept” by a government employee, acting in an official capacity, and whose content does concern his or her official conduct, a “public record” even though it does not reside (and perhaps never did reside) on a government-provided or–funded device or data repository? (See table 1.)

There are two subcategories within public business records kept on privately funded systems: (1) records kept or maintained on a server or in a records repository operated and controlled by an “outside vendor,” beyond the physical possession or actual custody of the government (e.g., Gmail, Verizon, BlackBerry, or Sprint Communications) but on behalf of a government agency; and (2) records kept or maintained exclusively in a “personal” account or device belonging to a public official or employee.
but not accessible to the government employer, other than through that official’s or employee’s consent. Both sets of cases will be discussed below.

Under traditional notions of which public records “belong” to the government, and therefore to the public, the answer to the question posed above Table 1 is emphatically and unequivocally, “yes.” To understand why, you need only consider how the answer would be determined in another context, before the advent of electronic communications. Suppose a governor, mayor, or city police chief transmits official government communications—e.g., orders or directives to subordinate public employees or policy statements to constituents—using his or her own personal stationery (not official government letterhead), envelope, and stamps, and thereafter maintains copies of all such written correspondence only in a personal filing cabinet at his or her private residence or, alternatively, off government premises at a privately owned document warehouse. Without question, all such writings were (1) “made, maintained, or kept” by a government official, acting in his or her official capacity; (2) their content is directly related to official governmental functions; and (3) those writings are within the possession, custody, or control of the government employee (and therefore, under the traditional rules of agency, are available to the government employer). Thus, under the three-part test that generally applies under public records statutes, those writings—though not transmitted via, nor stored within, government-provided media—are nonetheless “public records.” Not surprisingly, several courts that have addressed this question in the context of digitized records have resorted, by analogy, to “life before the digital era,” and have reached the same conclusion.16

The key question in these cases—whether e-mails (and other electronic records) stored on servers and/or devices not owned by the government—turns, in large measure, on whether under the applicable statutory text those records are deemed to be within the possession, custody, or control of the government entity from whom the records are sought. With respect to the records residing only on individuals’ “personal” accounts or devices, there is also an ancillary question whether a governmental search of a government official’s or employee’s “personal” account and/or device would constitute an unreasonable search or seizure in violation of the Fourth Amendment.

### Table 1: Public vs. Private Records

<table>
<thead>
<tr>
<th>Location of the Record</th>
<th>Content of the Record</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purely “Private” No Official Business</strong></td>
<td><strong>Public Business</strong></td>
</tr>
<tr>
<td>On Publicly Funded Device or System</td>
<td>(Generally) Not a Public Record15</td>
</tr>
<tr>
<td>On Privately Funded Device or System</td>
<td>Not a Public Record</td>
</tr>
<tr>
<td>On Third-Party Vendor’s System</td>
<td></td>
</tr>
<tr>
<td>On Government Employee’s “Personal” Drive</td>
<td></td>
</tr>
</tbody>
</table>

**“We’d Love to Give You Those Records, but We Don’t Have Them”**

There is a fair degree of consensus in the case law that public records stored on nongovernmental accounts on behalf of the government entity, to which the government retains a contractual right of access, are that entity’s public records. Flagg v. City of Detroit17 provides one of the most extensive and well-reasoned explanations of why e-mails, text messages, and other electronic “public records” maintained by a third-party vendor for the benefit of a government entity are within the “control” of the government, and are therefore required to be produced by that government entity in response to a records request.

Flagg involved a records request under civil discovery rules on the City of Detroit for text messages sent or received by former Mayor Kwame Kilpatrick, all of which resided in a message archive on the servers of Skytel, a private messaging service provider. None of the messages at issue resided on any city-owned server. U.S. District Court Judge Gerald E. Rosen found that because, presumably, the city had a contractual right to access the archived messages maintained by SkyTel, the city had sufficient “control” over those messages to require the city to produce them in response to a records request. Although the ruling arose under the federal rules governing civil discovery, the court expressly drew upon case law applying Michigan’s Freedom of Information Act (FOIA):

Because at least some of the text messages maintained by SkyTel are “public records” within the meaning of Michigan’s FOIA, it would be problematic, to say the least, to conclude that the City lacks a legal right to obtain those records as necessary to discharge its statutory duty of disclosure. Such a conclusion also would be contrary to the pertinent Michigan case law. First, the Michigan courts have
held that the FOIA duty of disclosure, like the Rule 34 duty of production, extends to public records within the possession or control of a public body.\(^{18}\)

After summarizing that case law, the court concluded:

[Case law applying Michigan’s FOIA] provides a compelling basis for concluding that the Defendant City has control, within the meaning of Rule 34(a)(1), over any “public records” that might be retained by third party SkyTel under its contract with the City.

[While the record does not disclose the terms of the City’s contracts with SkyTel, . . . the Court assumes that the City has at least some sort of contractual right of access to the text messages preserved by SkyTel in the course of its contractual relationship with the City.]

Thus, in jurisdictions where the definition of “public records” or “agency records” includes an explicit or implicit “possession, custody, or control” criterion, the fact that a government entity has a contractual right to access records maintained on its behalf by an outside vendor (whether a paper records “cold storage” warehouse, or a cloud-based provider like Gmail) should require the government entity to exercise its right of access to make available such records in response to a request for inspection from the public.

This approach has been followed by courts applying the federal FOIA, which provides public access only to “agency records” but does not define what is an agency record.\(^{20}\) Under that statute, several courts have held that when an executive branch agency has the right to obtain a document from a nongovernmental outside vendor, the agency has “constructive control” over such records, rendering them “agency records” subject to the FOIA.\(^{21}\)

“Those Records Belong to Me, Not to My Government Employer”

The far more contentious issue to date is whether records discussing public business maintained exclusively on an individual government official’s personal account and/or device is a public record of the government employer. As demonstrated below, the majority of courts that have addressed the issue have determined that all records generated or received by a public official acting in his or her official capacity, in which official public business is discussed, are the appropriate “property” of the government employer; thus, such records, even if housed on nongovernmental devices or accounts, should properly be deemed the public records of the government, not the individual. However, not all courts have reached this conclusion.

Applying the federal FOIA, one federal court held that e-mails maintained by a government employee exclusively in his nongovernmental (university) account were not “agency records” because they were not within the agency’s “control” as defined by the court.\(^{22}\) This ruling is at odds with other courts’ recognition that there is “no basis” in the FOIA or its legislative history to view an agency employee as “distinct from his [or her] department [or agency] for FOIA purposes.”\(^{23}\) Under these precedents, if a federal agency employee creates, receives, or maintains an electronic record in the course of fulfilling or carrying out his or her duties on behalf of the agency,\(^{24}\) those records are subject to a FOIA request on the agency, even if the record is maintained exclusively in the employee’s “personal” account or device.\(^{25}\) Summarizing this body of case law, two commentators recently concluded: “Common sense, case law, and FOIA’s plain language compel the conclusion that, irrespective of federal executive branch agencies’ employees’ reasons for using personal e-mail accounts or personal communications devices to conduct agency-related business within the scope of their employment, their work-related communications must be subject to FOIA’s disclosure provisions.”\(^{26}\)

Judges in nine states (Alaska, Arizona, Arkansas, Illinois, New York, Ohio, Pennsylvania, Virginia, and Washington)\(^{27}\) and the District of Columbia have held that if the content of an e-mail, text message, or other electronic record sent or received by a government employee relates to the conduct of governmental business, it is subject to those states’ open records acts; the actual physical location of such a writing is immaterial.

In July 2014, the Superior Court for the District of Columbia, applying D.C.’s FOIA,\(^{28}\) held that D.C. councilmembers’ e-mails maintained exclusively on so-called “private” accounts were public records subject to the Act.\(^{29}\) Judge Stuart G. Nash held that e-mails of Dianne Barnes, maintained in her personal e-mail account while acting in her capacity as commissioner of D.C.’s Advisory Neighborhood Commission, were “prepared, owned, used, in the possession of, or retained by a public body” and were therefore “public records” of the Commission under the Act.

In addition to the above judicial opinions, the attorneys general in 10 states (Alaska, Florida, Illinois, Maryland, New Mexico, North Dakota, Oklahoma, Oregon, Texas, and Wisconsin) have issued formal opinions stating that e-mail messages created, sent, or received by government officials that discuss public business are public records under those states’ FOI laws, regardless of the physical location or records repository where such e-mail messages reside.\(^{30}\)

Recently, the Texas Court of Appeals twice addressed whether e-mails of government employees maintained exclusively in personal accounts are subject to that state’s Public Information Act (PIA).\(^{31}\) In Adkisson v. Abbott, the court of appeals affirmed both the Texas attorney general’s and the Travis County District Court’s ruling that a county commissioner’s e-mails in which he discussed public business were public records under the PIA.\(^{32}\)

If the information in the official-capacity e-mails contained in the Commissioner’s personal e-mail accounts 1) is collected, assembled, or maintained for the County; 2) is connected “with the transaction of official business” for the County; and 3) the County either owns or has a right of access to the information, then the information is...
public information under the statutory definition.33

Commissioner Adkisson did not contest that the e-mails requested by the San Antonio Express-News were connected with the transaction of official business; instead, he argued that they were not collected, assembled, or maintained for Bexar County and that Bexar County had no right to access his official-capacity e-mails stored off of county computers.34 The court rejected Adkisson’s first argument:

To conclude otherwise would lead to the absurd result that the Commissioner could conduct all his official County business correspondence through his personal e-mail accounts without it being subject to the PIA, even if the same correspondence would be subject to the PIA if he used his County e-mail account.35

Relying on the county’s records management administrative policy, the court further concluded that:

any local government records collected, assembled, or maintained in the Commissioner’s e-mail accounts belongs to the County, not to the Commissioner in his individual capacity. Conducting County business through a personal e-mail account instead of through an official County e-mail account does not change the County’s ownership of the local government records created or received by the Commissioner as a County government officer.36

The court also rejected Adkisson’s claim that inspection of the official business e-mails in his personal account would constitute an invasion of his personal privacy, noting that Adkisson had failed “to explain how the release of documents concerning the transaction of official business could be confidential.”37

But how much pressure can a government agency bring on its employees to provide the records that reside entirely outside of the government’s filing systems? In the second of the two rulings, the Texas Court of Appeals answered by saying, essentially, “none.” After a citizen, Stephanie Allala, asked to inspect the e-mails of the City of El Paso’s councilmembers, and specifically “any public business emails that may have been conducted on the personal email accounts of these individuals,” the state’s attorney general opined that such records were, in fact, subject to the Texas PIA.38 Accordingly, the City of El Paso produced to Allala all of the e-mails it had retrieved, upon request, from the city councilors, and then stated it had fully complied with her request. Allala challenged the city’s representation, and sought discovery to determine how assiduously the city councilors—one of whom had stated in writing he would not produce his “private emails” absent a court order—had complied with the City’s request that they search their personal e-mail accounts and produce responsive records. The court of appeals stated that the city could not compel the city councilors to comply with its request, and so the city had satisfied its burden to produce its responsive records to Allala.

Both the Adkisson and Allala cases were decided under the prior (2010) version of the Texas PIA. In 2013, that statute was amended expressly to clarify that:

“public information” means information that is written, produced, collected, assembled, or maintained . . . by an individual officer or employee of a governmental body in the officer’s or employee’s official capacity and the information pertains to official business of the governmental body; [in addition, this definition] applies to and includes any electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business.39

Absent such a legislative “fix” to this ruling, perhaps the appropriate—and necessary—procedural step is to name each of the agency’s employees (or here, the individual city councilors) as defendants, and ask the court to order each of them, individually, to retrieve the “public records” in their personal possession, just as the El Paso city councilor had stated would be necessary to compel his compliance with the law.

Notwithstanding this trend of recent cases favoring the public’s right to know, in March 2014, California’s Court of Appeals ruled to the contrary, reversing a trial court’s determination that the e-mails sent and received by the mayor of San Jose, California, exclusively over a nongovernmental exchange server, were “public records” of the city under the California Public Records Act (CPRA). The case began in August 2009, when the San Jose Mercury-News received two e-mails from a San Jose city councilmember indicating that councilmembers were communicating during and after city council meetings in regard to a proposal to give “millions of city redevelopment dollars to former Mayor Tom McEnery.”40 The Mercury-News filed a complaint asking that the City of San Jose and the San Jose Redevelopment Agency, as well as city officials and former officials, be required to provide access to “e-mails, text messages, and other electronic information relating to public business, regardless of whether they were created or received on the City owned computers and servers or the City Officials’ personal electronic devices.”41 In March 2013, the superior court held in favor of the San Jose Mercury-News, ruling that all

How much pressure can a government agency bring on its employees to provide records that reside entirely outside of the government’s filing systems?
of the requested records were public records of a “local agency.”42
However, in March 2014, the California Court of Appeals reversed, holding that the statute’s definition of “local agency” did not include the agency’s individual officers or employees: “It is the agency... that must prepare, own, use, or retain the writing in order for it to be a public record, [and thus] those writings that are not accessible by the City cannot be said to fall within the statutory definition.”43 The court held that the CPRA does not impose a duty on the

Access to electronic records turns on how long the government is required to maintain copies of those records in which public business is discussed.

city to produce messages stored on the personal electronic devices and accounts of its employees or officials that are inaccessible to the agency; nor is the city required to search those devices and accounts in response to a CPRA request. The court rejected the plaintiff’s (and media amici’s) argument that the city had “constructive control” over the mayor’s and councilmembers’ personal devices. Curiously, although the court acknowledged that in 2004 California’s voters had passed Proposition 59, which declared that “the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny,”44 that language was not considered in the court’s analysis.

As this article goes to press, briefing is being prepared before the California Supreme Court45 in this important case that will be closely watched by other courts throughout the nation.

“Privacy Rights” of Government Employees Should Not Bar Access to “Public Records”

As indicated above, some courts have expressed concern for public employees’ privacy rights that would supposedly be implicated by a regime requiring government entities to search individuals’ personal devices and Gmail accounts to locate writings that satisfy the definition of public records (those whose contents bear a “demonstrable connection” or “substantial nexus” to the discharge of official public duties). However, these concerns are properly limited only to the e-mails or records whose content is truly “private,” i.e., those that do not satisfy the definition of “public record.” No claim can be made by a public employee that his or her communications in his or her official capacity, discussing official public business, are subject to a reasonable expectation of personal privacy.46 Thus, only purely private information—i.e., information that does not reflect or document the public employee’s discharge of his or her official duties—is entitled to any expectation of privacy, and is outside the statutory definition of “public records.”47

One way to minimize the intrusion on a public employee’s legitimate privacy rights—by exposing his or her truly private e-mails to scrutiny by his or her government employer—is to impose upon the employee himself or herself the duty to search and provide access to public records housed in a personal account. Increasingly, states, cities, and municipalities are adopting policies requiring public employees to send public records from their personal accounts and devices to a government central repository.48 Other government leaders have issued directives requiring public employees to restrict their use of personal devices to nongovernmental communications, so that all “public records” will be exchanged and housed on government-controlled media.49

Indeed, the it is this very concern for personal privacy interests and the “burden” of having government employees sort through electronic records to extract only those whose contents address public business that provides the strongest policy argument for why government employees, as a general policy/rule, should be required to maintain a separate account and/or electronic folders in which only their governmental IMs, texts, e-mails, and other records are stored. A rule of law that condones the intermingling of private and public records—whether electronic or paper form—to shield public records from inspection under FOI laws only incentivizes the intermingling of records. If a government official chooses to intermingle his or her public and private writings in a single account, device, or file cabinet, then he or she should not be heard to complain about the “administrative burden” of sorting those records into two piles, private and public, to comply with FOI mandates.

Retention: “I’d Be Glad to Give You Those Records, Only We No Longer Have Them”

Both the federal FOIA and state public records laws provide a right of access only to those records that are in existence at the time of the request; the government is not required to generate a new record in response to a records request, nor to provide access to a record that no longer exists.50 Thus, for many records requesters, the question of access to electronic records turns on how long the government is required to maintain copies of those records in which public business is discussed. (Notably, unlike paper records, which required affirmative physical action to destroy or discard, digital records—especially text and e-mail messages—have a built-in, automatic “shelf life” as a result of standardized “auto-delete” functions).

The answer to the question “how long must a record be kept?” frequently depends on a set of laws and policies extraneous to the FOI or “right to know” law.51 The duty to retain public records generally is found in companion statutes that define “public records” for purposes of records preservation, as in a state archives.52 Unfortunately, in many instances, these statutes, and the records retention schedules promulgated by state archivists thereunder, leave a tremendous amount of discretion to individual records custodians. Worse still, those custodians are often the very employees who generated and exchanged the e-communications. Yet they are given the authority to determine whether the records are of “preliminary or short-term informational value” or “lasting value” in documenting the workings of government agencies.53
At the federal level, the recent high-profile scandal involving the destruction of hundreds of e-mails that had been on the laptop computer of former (and embattled) IRS Commissioner Lois Lerner brought to the fore the issue of what obligations executive branch agencies have to retain electronic records. During congressional hearings exploring the loss of Lerner’s e-mails, the U.S. archivist, David Ferriero, told the House Oversight and Government Reform Committee that the IRS “did not follow the law” when it failed to report that the e-mails had been lost.54

The Federal Records Act sets forth the executive branch agencies’ duties to preserve records in accordance with the general records schedules promulgated by the National Archives and Records Administration (NARA).55 It is the duty of each federal agency (270 of which are subject to the Federal Records Act) to propose disposition schedules for their records, and the vast bulk (95–97 percent) of records are eventually destroyed.56 Under the Managing Government Records Directive adopted by the Obama administration in 2011, “[b]y the end of 2016, all agencies need to manage e-mail in automated, electronic ways.”57 In August 2013, NARA issued its guidance on e-mail management,58 which sets forth what is referred to as a “capstone” approach: under this tiered system, all work-related e-mails of certain high-level department officials, who are deemed “capstone” employees, are to be maintained permanently by the agency; those of lower (mid-) level agency employees are to be preserved for seven years; and those of the more subordinate employees are to be retained for shorter periods of time, according to the agency’s needs.59

As many government entities have discovered, failure to ensure that electronic records are properly maintained and preserved can give rise to additional burdens on such agencies to conduct adequate “search and retrieval” of records.60 The consequences of intentional public records destruction can also prove quite costly. In 2012, a Colorado school district was ordered to pay $122,000 in attorneys’ fees to the parents of a student after a school official had ordered several school employees to destroy thousands of e-mails and other public records.61 In January 2014, Orange County, Florida, agreed to pay a coalition of citizen groups $90,000 to settle a lawsuit the media dubbed “textgate” after a criminal investigation concluded that the mayor and four county commissioners had violated state law when they deleted text messages that were public records.62 And in 2009, the City of Venice, Florida, was ordered to pay $750,000 in attorneys’ fees following the settlement of a lawsuit brought by a citizen’s group that accused city councilmembers of having conducted illegal meetings via e-mail and then destroying or failing to preserve public records; that was on top of the $600,000 the city paid to defend the councilmembers in the suit.63

Even though storing digitized records is generally much cheaper than warehousing paper files, massive data storage imposes significant costs and administrative burden on governments, particularly in light of the tremendous volume of data that governments generate daily. Hence, government agencies at all levels—federal, state, and local—have a legitimate need to not “keep” everything in perpetuity. Most states’ public records preservation and archives statutes dictate that the length of time for keeping records must be determined by the content of the record, not its format, medium, or title.64 But the manner in which specific records retention schedules are promulgated and implemented, and particularly when e-records “expire” automatically, will continue to pose problems for public records requesters.

The conclusion of the 2009 report on this subject by the Reporters Committee for Freedom of the Press (RCFP) is as relevant and accurate today as when it was published five years ago: “E-mail retention policies likely will generate increasing amounts of litigation—and deservedly so. In states where the issue has not been settled by statute or case law, there are effectively no bright-line legal mandates requiring officials to retain e-mail [or other digitized] records for a given period of time.”65

Production: “Of Course You Can Have Our Database; We’ll Print It Out for You”

Another issue that often arises is whether the public is entitled to access the electronic records in the same format in which the government maintains the data. FOIA case law prior to the “digital era” sheds some light on this question: federal courts recognized that a request to inspect (and listen to) an audio recording is not satisfied by obtaining access only to a written transcript of the recording, precisely because the “quantum of information” on the recording (voice fluctuations, pauses, and inflection) is lost in the transcription process.66 However, when the quantum of information remained unchanged—as when a set of data points is transferred from a computer tape to a microfiche—the courts held that there was no “right” under the FOIA to demand access to the tape itself.67 However, subsequently (and after the FOIA was amended in 1996),68 federal courts have disagreed with this analysis, and have required federal agencies, such as NOAA, to provide access to information kept in a digitized form, finding that a paper printout of the same data set does not provide access to the particular “agency record” sought.69

But how much effort must the government expend to make its records available to the public? The federal FOIA provides that an agency shall make a record available “in any form or format requested by the person if the record is readily reproducible by the agency in that form or format.”70 The Justice Department’s Office of Information Policy has stated that the onus is on the records requester to dictate the format in which he or she wishes to receive an agency record.71 Further, agencies should make “reasonable efforts” to produce a record in a requested format if it is “readily reproducible” in that form.72 Many federal courts adhere to the standard for reasonableness announced by the Ninth Circuit in TPS, Inc. v. U.S. Department of Defense: a record is readily reproducible if an agency already has the means to create and convert documents into a specific format even if it does not routinely do so for purposes of responding to FOIA requests.73 Some, but not all, states’ open records laws expressly guarantee the right to obtain records in a particular format if so requested.74 For example, Mississippi’s statute provides that “[a]
public body shall provide a copy of the record in the format requested if the public body maintains the record in that format.” Notwithstanding these legislative directives to provide access to digitized records in their native format, many government entities have refused to do so. Common excuses include concern about security of the data and the “burden” of redacting nonpublic information, such as Social Security numbers.

State and federal courts called upon to enforce these directives have not been consistent in doing so. Some courts have upheld the right of the requester to receive information in the particular medium requested, liberalizing construing the relevant FOI law, while other courts have adhered to a very narrow interpretation of what is “readily reproducible.” Several state courts have distinguished case law applying the federal FOIA because it has been interpreted to provide access only to “information,” as opposed to state statutes that guarantee the right to access the very “public records” in the hands of the government.

In 1992, Ohio’s Supreme Court provided a clear and compelling explication of why access to information—in the same form and format in which is maintained by the government—is required to fulfill the purposes of a “public records” act:

"Electronic Fingerprints": Access to Metadata

Prior to the digital age, when paper documents were stored in filing cabinets, there would sometimes be an index to the files, generated by government employees, showing the “filing scheme” that might, in appropriate circumstances, reveal how the documents were characterized and classified by government officials (e.g., "enemies" or "personas non grata"). Such government-generated catalogs or file indexes were unquestionably "public records" that reflected the "mental processes" or "inner workings" of the government.

With the advent of the digital age, however, the filing systems are automated, and the data-processing systems—whether they be spreadsheets, word processing, e-mails, or text messaging—automatically record and track various information that previously required human labor (and that more often than not was simply not recorded). Examining the "metadata" on a typical document created and edited on Microsoft Word, for example, one can determine who first generated the document, on what date and at what time, and for how long it was open and being edited, and thereafter, by whom, on which dates, and at which times; indeed, depending on the document settings, it is sometimes possible to recreate earlier drafts of a document and to show which persons made which edits.

Here, the added value is not only the organization of the data, but also the compression of the data into a form that allows greater ease of public access. Thus, in keeping with the expressed intent of the General Assembly to provide broad access to public records, we hold that a governmental agency must allow the copying of the portions of computer tapes to which the public is entitled, if the person requesting the information has presented a legitimate reason why a paper copy of the records would be insufficient or impracticable, and if such person assumes the expense of copying.

As Communications Technology Evolves, So Will the Legal Battles over Access to Public Records

Progress toward the “paperless office” continues in the halls of government as it does in the private sector. As ever more government records that shed light on the conduct of the public’s business are comprised of digital zeros and ones, and are stored “off premises” in the cloud and/or on portable electronic devices, the issues discussed in this article will increasingly be litigated. Thus far, courts have generally (and appropriately) recognized that it is the content of the record, not its physical form or location, that should determine whether the public is entitled to inspect and copy such data. It is hoped that government leaders’ lofty proclamations extolling the virtues of “transparency” and committing to “proactive access” will someday translate into concrete steps—that the government will systematically post and/or distribute public records without requiring that individual requests be submitted. Until that Elysian day arrives, however, advocates for access will continue to battle to inspect public records, wherever they reside, and constitutes an “agency record” under the federal FOIA. In 2011, Judge Shira A. Scheindlin of the Southern District of New York ruled that “metadata maintained by the agency as a part of an electronic record is presumptively producible under FOIA, unless the agency demonstrates that such metadata is not ‘readily reproducible.’” However, that opinion was short-lived. The parties subsequently settled and the opinion was withdrawn, so it holds no precedential value.

State courts, on the other hand, have been fairly uniform in concluding that metadata encompasses an “agency record” that must be produced under state open records laws. Based on the language of FOIA itself, state courts’ interpretations of similarly worded state open records laws, and executive guidance, there is a strong argument that metadata should be considered part of an agency record subject to the federal FOIA, as Judge Scheindlin had once concluded.
in whatever format. After all, such records are often the only way reliably to determine what our government is up to.

Endnotes


6. In 2012, the chief of staff to New Mexico Governor Susana Martinez was caught on tape stating that he never used his government-provided e-mail account to discuss public business, so that his communications would not be subject to that state’s open records law. See Steve Terrell, Martinez Administration Dodges Requests for Out-of-State Travel Costs, SANTA FE NEW MEXICAN, Mar. 20, 2014.


13. An excellent summary of this body of case law can be found in Peter S. Kozinet, Access to the E-Mail Records of Public Officials: Safeguarding the Public’s Right to Know, COMM. LAW., Summer 2007, at 17. See, e.g., Denver Publ’g Co. v. Bd. of Cnty. Comm’rs of Arapahoe Cnty., Colo., 121 P.3d 190 (Colo. 2005) (holding that sexually explicit text messages exchanged between two government employees on county-provided devices, while on duty, were not “public records” because the content of those messages did not bear “a demonstrable connection” to the discharge of public functions).

14. The Colorado Supreme Court has held that when a public employee makes only passing reference to his or her professional conduct in the entries of a private diary, that diary is “made, maintained, [and] kept” purely in that employee’s private capacity. Wick Commc’ns Co. v. Montrose Cnty. Bd. of Cnty. Comm’rs, 81 P.3d 360 (Colo. 2003).


16. See, e.g., City of Clearwater, 863 So.2d at 154 (concluding that “the determining factor [in deciding whether e-mails are public records] is the nature of the record, not its physical location,” and noting that “an agency cannot circumvent the Public Records Act by allowing a private entity to maintain physical custody of documents that fall within the definition of ‘public records’”).
19. Id. at 357.
20. U.S. Dep’t of Justice v. Tax Analysts, 492 U.S. 136, 142 (1989). Two requirements must be met before materials will be considered to be “agency records.” First, the agency must “either create or obtain” the documents. Id. at 144 (quoting Forsham v. Harris, 445 U.S. 169, 182 (1980)). Second, the agency “must be in control of the requested materials at the time the FOIA request is made.” Id. at 145.
21. See, e.g., Burk v. U.S. Dep’t of Health & Human Servs., 87 F.3d 508, 515 (D.C. Cir. 1996) (finding that HHS had “constructive control” of data tapes in the possession of a private research firm); Ryan v. Dep’t of Justice, 617 F.2d 781, 785 (D.C. Cir. 1980) (“A simple possession standard would permit agencies to insulate their activities from FOIA disclosure by farming out operations to outside contractors.”); Democratic Nat’l Comm. v. U.S. Dep’t of Justice, 539 F. Supp. 2d 363, 367 (D.D.C. 2008) (concluding that e-mails maintained on a political party’s server are subject to FOIA, and that “because the form of the document does not factor into the analysis under FOIA, the court cannot adopt a per se rule that any e-mails sent on the RNC servers are not covered by FOIA”).
23. Ryan, 617 F.2d at 787.
24. As the D.C. Circuit has held, “the purpose for which the document was created, the actual use of the document, and the extent to which the creator of the document and other employees acting within the scope of their employment relied upon the document to carry out the business of the agency” are “important considerations” for distinguishing between “agency records” and personal materials. Bureau of Nat’l Affairs v. U.S. Dep’t of Justice, 742 F.2d 1484, 1493 (D.C. Cir. 1984).
25. Judicial Watch, Inc. v. U.S. Dep’t of Energy, 310 F. Supp. 2d 271, 297 (D.D.C. 2004) (“The actual physical location of the documents is not dispositive; the issue is actual or constructive ‘control.’”), aff’d in part, rev’d in part, 412 F.3d 125, 133 (D.C. Cir. 2005) (recognizing that “[a]s the district court correctly observed, . . . possession is not the proper test of whether a record is within an agency’s control,” and holding that records generated by and in possession of a Department of Interior (DOI) employee “in the legitimate conduct of his official duties” were agency records of DOI); see also Landmark Legal Found. v. EPA, 959 F. Supp. 2d 175, 184 (D.D.C. 2013) (authorizing discovery into the adequacy of the EPA’s search for responsive records, including the personal e-mail accounts of individual employees, because “[t]he possibility that unsearched personal email accounts may have been used for official business raises the possibility that leaders in the EPA may have purposefully attempted to skirt disclosure under the FOIA”).
27. McLeod v. Parnell, 286 P.3d 509, 515 (Alaska 2012) (“[U]sing private email accounts is no more an obstruction of access to public records than communicating through paper letters.”); Griffis v. Pina Cnty., 156 P.3d 418, 421 (Ariz. 2007); Bradford v. Dir., Emp’t Sec. Dep’t, 128 S.W.3d 20, 27–28 (Ark. Ct. App. 2003) (“Emails transmitted between Bradford and the governor that involved the public’s business are subject to public access under the Freedom of Information Act, whether transmitted to private email addresses through private internet providers or whether sent to official government email addresses over means under the control of the State’s Division of Information Services.”); City of Champaign v. Madigan, 992 N.E.2d 629 (Ill. App. Ct. 2013) (applying state’s open meetings law); Matter of Smith v. N.Y. State Office of the Attorney Gen., No. 3670-08, NYLJ 1202555064972, at *1 (N.Y. Sup. Ct. Apr. 30, 2012) (“[T]he OAG has both the responsibility and the obligation to gain access to the private e-mail account of former Attorney General Spitzer to determine whether the documents contained therein should be disclosed to petitioner in accordance with its FOIL request.”); State ex rel. Glasgow v. Jones, 894 N.E.2d 686, 691 (Ohio 2008) (“[R]epresentative Jones conceded that e-mail messages created or received by her in her capacity as state representative . . . constitute records subject to disclosure . . . regardless of whether it was her public or her private e-mail account that received or sent the e-mail messages.”); Mollick v. Twp. of Worcester, 32 A.3d 859, 872–873 (Pa. Commw. Ct. 2011) (“[A]ny emails that meet the definition of ‘record’ under the RTKL, even if they are stored on the Supervisors’ personal computers or in their personal email accounts, would be records of the Township.”); Burton v. Mann, 74 Va. Cir. 471 (2008) (“[T]he e-mail correspondence sought in this case indicates the use of both public and private databases, the status of which is not determinative of the issue of disclosure.”).
28. D.C. CODE §§ 2-531 et seq.
31. TEX. GOV’T CODE ANN. §§ 552.001–.353.
33. Id. at *6
34. Id. at *6 n.4.
35. Id. at *8.
36. Id. at *9 (emphasis added).
37. Id. at *12.


41. Id. at 5.

42. See Cal. Gov’t Code § 6252(a).

43. City of San Jose v. Superior Court, 169 Cal. Rptr. 3d 840, 850 (Cal. App. 2014).

44. Cal. Const. art. 1, § 3(b)(1) (emphasis added).

45. City of San Jose v. Superior Court, 173 Cal. Rptr. 3d 46 (2014).


47. See, e.g., Nixon v. Adm’t of Gen. Servs., 433 U.S. 425, 457 (1977) (holding that public officials enjoy a right of privacy only with respect to government-held information concerning “matters of personal life unrelated to any acts done by them in their public capacity” (emphasis added)); Denver Publ’g Co. v. Bd. of Cnty. Comm’rs of Arapahoe Cnty., Colo., 121 P.3d 190 (Colo. 2005) (holding that any portions of text messages exchanged between two government employees that discussed governmental business were public records and were required to be disclosed; the portions of such messages that contained only graphic, sexually explicit statements did not reflect official conduct and were redacted as “private”).

48. See Kevin Duggan, Public Access to Council Email Gets Easier, Coloradoan, Jul. 26, 2014 (reporting that the City of Fort Collins, Colorado, has posted all nonprivileged e-mails of city councilors online, where they remain available for 90 days and then are deleted, consistent with city policy); Mary Ellen Klas, Judge Orders Fla. Gov. Rick Scott to Stop Fighting Request for Records, Miami Herald, Sept. 9, 2014 (reporting that Florida Governor Rick Scott’s “‘code of conduct’ states that employees should not use personal email accounts ‘unless such use is necessary upon a reasonable evaluation of the circumstances at hand’ and then must forward the public record to his or her state account”).

49. See, e.g., Steve Terrell, Governor Orders Staff to End Use of Private Email for Work Matters, New Mexican, June 18, 2012 (“After a week of taking heat following the disclosure that Gov. Susana Martinez and top officials in her administration used personal emails to conduct state business, on Monday she ordered all state employees in agencies under her authority to use official state email for state business.”).

50. See, e.g., Freedom of Info. Act Complaint against Wilmington Hou. Auth., Del. Op. Att’y Gen. No. 06-ID23, 2006 WL 3663142 (Nov. 27, 2006) (concluding that “the Authority did not violate the . . . FOIA because any of [the executive director’s] e-mails that might have been responsive to your request no longer exist”).

51. See, e.g., Edendburn v. N.M. Dep’t of Health, 299 P.3d 424, 427 (N.M. Ct. App. 2012) (noting that the state’s records preservation statute and its right to inspect public records act are distinct, and serve different purposes, so that the former does not affect decisions under the latter).

52. The Council of State Archivists’ website includes a compilation of all 50 states’ public records preservation statutes: http://www.statearchivists.org/arc/states/res_stat.htm.


59. See Nat’l Archives, NARA Bulletin 2014-06, Guidance on Managing Email (Sept. 15, 2014), available at http://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html (stating that “[c]apstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower levels of the agency”).

60. See, e.g., Valencia-Lucena v. U.S. Coast Guard, 180 F.3d 321, 328 (D.C. Cir. 1999) (finding agency’s search inadequate where a particular responsive record was missing and agency failed to contact other personnel where “there is a close nexus . . . between the person and the particular record”); FLP Grp., Inc. v. IRS, 698 F. Supp. 2d 66, 78–80 (D.D.C. 2010) (applying FOIA and holding that if known responsive documents have been destroyed, the agency is obligated to search the electronic and paper files of other personnel who are “likely to have copies of the destroyed materials,” including former employees (emphasis added)); State ex rel. Toledo Blade Co. v. Seneca Cnty. Bd. of Comm’rs, 899 N.E.2d 961, 970 (Ohio 2008) (ordering government entity to bear the cost of forensic data recovery to attempt to restore e-mails that had been deleted in violation of published records retention schedule).

§ 25-61-10(2); 5(d); tent' is available in statistical tables."

example, merely because the same 'con-

agency's FOIA duty is to disclose records,


105(d)(2)(B); 

§ 16.11(b)(3) ("Components shall honor a

foia-amendments; 28 C.F.R.

available at 4

Policy, foia uPdate, vol. xvii, no.

reproducing data in the ordi-

"In evaluating reproducibility, the agency

("In evaluating reproducibility, the agency


73. 330 F.3d 1191, 1197 (9th Cir. 2003)

("In evaluating reproducibility, the agency


75. Miss. Code Ann. § 25-61-10(2); see

also Ark. Code Ann. § 25-19-105(d)(2)

(B) (providing that a citizen “may request a

copy of a public record in any medium

in which the record is readily available or

in any format to which it is readily convert-

able with the custodian’s existing software"

(emphasis added)); 5 ILL. COMP. Stat.

140/6(a) ("When a person requests a copy of

a record maintained in an electronic

format, the public body shall furnish it

in the electronic format specified by the

requester, if feasible. If it is not feasible to

furnish the public records in the specified

electronic format, then the public body

shall furnish it in the format in which it

is maintained by the public body . . . ."

(emphasis added)).

76. See, e.g., Prall v. N.Y. City Dep’t of

Corrections, 971 N.Y.S.2d 821 (Sup. Ct.

2013) (holding that NYC DOC did not

violate FOIL when it provided inmate

arrest records in PDF format rather than

in native format as requested because dis-

closing original format would also have

required disclosure of metadata contain-

ing confidential information).

77. See, e.g., Menge v. City of Man-

chester, 311 A.2d 116 (N.H. 1973)

(holding that expense and labor involved

in abstracting information from other

sources far outweighed ease and minimal

cost of tape production).

78. See, e.g., Sample v. Bureau of

Prisons, 466 F.3d 1086 (D.C. Cir. 2006)

(holding that under FOIA, Bureau of

Prisons was obligated to provide record in

electronic form to inmate, as requested);

Minn. Med. Ass’n v. State, 274 N.W.2d 84

(Minn. 1978) (holding that state data pri-

vacy act placed no restriction on the form

in which records could be made available

other than that they be easily accessible for

convenient use); Brownstone Publish-

ers, Inc. v. N.Y. City Dep’t of Bdgs., 560


It is clear that both the statute and its un-

derlying policy require that the DOB comply

with Brownstone’s reasonable request to

have the information, presently main-

tained in computer language, transferred

onto computer tapes."); see also Blay-

lock v. Staley, 732 S.W.2d 152 (Ark. 1987);

Szikszy v. Buelow, 436 N.Y.S.2d 558


79. See, e.g., Laroche v. SEC, No. C

05-4760 CW, 2006 WL 2868972, at *3

(N.D. Cal. Oct. 6, 2006) (finding that SEC

could not readily reproduce in electronic

format data not available electronically

when “the only other way to create a

searchable electronic file [besides scanning

paper copies] would be for an SEC staff

member to cut and paste each cell of data

from the individual electronic records into

another document for Plaintiff.”).

aff’d, 289 F. App’x 231 (9th Cir. 2008); Citizens

for Responsibility & Ethics in Wash. v.

U.S. Dep’t of Educ., 905 F. Supp. 2d 161,

171 (D.D.C. 2012) (holding that agency

had no responsibility to provide electronic

format of responsive e-mails because

“DoEd’s email records are not ‘readily

reproducible’ in electronic format, and the

DoEd email retention system ‘will not
display or print’ the BCC field ‘for any

retrieved email.’”).

80. See, e.g., AFSCME v. Cook Cnty.,

555 N.E.2d 361 (Ill. 1990); Farrell v.

City of Detroit, 530 N.W.2d 105, 108–09


Michigan’s statute “gives a person the

right to ‘inspect, copy, or receive copies of

a public record,’ not merely to obtain the

‘information’ contained in a public record

in any form in which the public body sees

fit to release it”); Brownstone Publishers,


v. Cnty. of Essex, 660 A.2d 1163, 1170

(N.J. 1995) (requiring disclosure of tax list

records in computerized form under com-

mon-law balancing test). But see Wells

v. Wharton, No. W2005-00695-COA-

R3-CV, 2005 WL 3309651, at *9 (Tenn.

Ct. App. 2005) (rejecting these cases, and

concluding that “[a]llowing a custodian of

records to choose the manner in which he

or she presents public records to citizens

is unreasonable in the long run because

it does not distort the record or inhibit

access to that record.”).

81. State ex rel. Margolius v. City of

Cleveland, 584 N.E.2d 665, 669 (Ohio

1992) (emphasis added) (citation omitted).

82. A helpful description of various

programs’ available metadata, and how

to access it, is available at http://canons.
sog.unc.edu/wp-content/uploads/2010/03/
document_metadata-2.pdf.

83. REPORTERS COMMITTEE FOR FREEDOM

OF THE PRESS. Access to File “Metadata,”

in FEDERAL FOIA APPEALS GUIDE, supra

note 73. “Metadata is quite simply data

about data, or hidden statistical informa-

tion about a document that is generated

by a software program.” O’Neill v. City

of Shoreline, 240 P.3d 1149, 1152 (Wash.

2010) (quoting Jembaa Cole, When

Published in Communications Lawyer, Volume 31, Number 1, Winter 2015. © 2015 American Bar Association. Reproduced with permission. All rights reserved. This information or any portion
thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
Invisible Electronic Ink Leaves Red Faces: Tactical, Legal and Ethical Consequences of the Failure to Remove Metadata, 1 SHIDLER J.L. COM. & TECH. 8, ¶ 7 (Feb. 2, 2005).

84. See Kozinets, supra note 13.

85. Id.

86. Under the Electronic FOIA Amendments of 1996, a record is defined as “any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.” 5 U.S.C. § 552(f)(2)(A).


89. See, e.g., Lake v. City of Phoenix, 218 P.3d 1004, 1007–08 (Ariz. 2009) (“The metadata in an electronic document is part of the underlying document; it does not stand on its own. When a public officer uses a computer to make a public record, the metadata forms part of the document as much as the words on the page. . . . We accordingly hold that when a public entity maintains a public record in an electronic format, the electronic version of the record, including any embedded metadata, is subject to disclosure under our public records law.”); O’Neill v. City of Shoreline, 240 P.3d 1149, 1153–54 (Wash. 2010) (“Metadata may contain information that relates to the conduct of government and is important for the public to know. . . . An electronic version of a record, including its embedded metadata, is a public record subject to disclosure.”); see also Irwin v. Onondaga Cnty. Res. Recovery Agency, 895 N.Y.S.2d 262 (App. Div. 2010); Hearst Corp. v. State, 882 N.Y.S.2d 862 (Sup. Ct. 2009).


THE PROGENY: JUSTICE WILLIAM J. BRENNAN’S FIGHT TO PRESERVE THE LEGACY OF NEW YORK TIMES V. SULLIVAN

BY LEE LEVINE AND STEPHEN WERMIEL

Celebrate the 50th anniversary of Justice William J. Brennan's landmark opinion in New York Times Co. v. Sullivan with this fascinating and insightful book!

New York Times Co. v. Sullivan, credited with defining the "central meaning" of the First Amendment, has protected the freedom of expression for the past 50 years. This book focuses on "the progeny" of that decision—examining how Justice Brennan nurtured and developed the constitutional law of defamation and related claims from this important milestone.

Told largely from Brennan's perspective, and based on his previously unreported papers and interviews with his biographer, the authors deconstruct the internal machinations that resulted in the historic line of cases that now govern the law of defamation as well as closely related claims such as invasion of privacy and intentional infliction of emotional distress.

Given Sullivan's enormous impact on the development of our rights to freedom of speech and press, this book is a must read for Supreme Court watchers, journalists, fans of legal history, constitutional scholars, and, of course, First Amendment enthusiasts.

To order, call the ABA Service Center at 800-285-2221 or visit our website at www.ShopABA.org.
Jurisdictional Issues in Anonymous Speech Cases

MARC FULLER

For more than a decade, courts have grappled with constitutional issues relating to the protection of anonymous online speech. These courts have focused primarily on the First Amendment requirements that plaintiffs must satisfy in order to unmask bloggers, commenters, and others whose speech is alleged to be defamatory. On this issue, the case law has generally coalesced around the basic principle that plaintiffs must make a prima facie evidentiary showing to support their claims, rather than merely plead a possible claim.1

Courts have paid less attention to the jurisdictional issues relating to the unmasking of anonymous speakers. But two cases—one recently decided by the Texas Supreme Court and another currently pending before the Virginia Supreme Court—highlight the importance of jurisdictional considerations in the protection of anonymous speech.

**Trooper: The Role of Personal Jurisdiction**

On August 29, 2014, the Texas Supreme Court decided *In re Doe a/k/a “Trooper”*, a case that many expected to set the substantive standards in Texas for unmasking anonymous Internet posters in defamation cases.2 *Trooper* involved a presuit discovery petition by a company and its CEO under Rule 202 of the Texas Rules of Civil Procedure. The petitioners sought the deposition of Google in an effort to discover the identity of an anonymous blogger, “the Trooper,” who had derided the company’s software products as “crap” and had compared its CEO to Bernie Madoff and Bobo the Clown. According to their Rule 202 petition, the company and CEO anticipated filing defamation and business disparagement claims against the Trooper.3

This use of Rule 202 has become common in Texas. For decades, the state has had the country’s broadest presuit discovery practice. Rule 202 has its origin in the courts of equity, and equitable principles frequently prevail over formal legal requirements in the Texas trial courts’ application of the rule.4 As a result, Rule 202 courts often do not scrutinize the petitioner’s anticipated claim to ensure that it is legally viable or that it will satisfy jurisdiction and venue requirements. If petitioners can articulate a good faith interest in the requested information, they stand a very good chance of obtaining it. Accordingly, when businesses and individuals feeling aggrieved by online speech seek to unmask anonymous bloggers and commenters, they frequently turn to Rule 202.

In *Trooper*, the company and CEO’s Rule 202 petition was served on Google, which hosted the Trooper’s blog. Google notified the Trooper of the petition by e-mail. The Trooper then entered an anonymous special appearance, challenging the petition on the grounds that it violated the procedural requirements of Rule 202 and the substantive protections for anonymous speakers under the First Amendment. Procedurally, the Trooper argued that the Texas court was not a “proper court” under Rule 202 because it would not be able to exercise personal jurisdiction over him in the anticipated defamation case. Substantively, the Trooper argued that the company and CEO were required, and had failed, to satisfy the *Dendrite/Cahill* standards.5 He lost on both issues at the trial court and the intermediate appellate court.

The Texas Supreme Court saw things differently. In a 5–4 split decision, the court reversed and vacated the order requiring Google to identify the Trooper. But instead of using the case to address the First Amendment right to speak anonymously, the court decided the case on procedural grounds. Noting that only a “proper court” could issue a Rule 202 order, the Texas Supreme Court held that a “proper court” must have personal jurisdiction over the anonymous potential defendant. The court further held that it is the plaintiff’s burden to make this jurisdictional showing, just as it would be in a pending suit.6

Trooper’s impact on presuit discovery in Texas is obvious. With the new personal jurisdiction requirement, Rule 202 is now decidedly less attractive to plaintiffs seeking to target anonymous speech and commerce.7 But beyond the presuit context, and outside Texas, the potential impact of the decision is less clear. While some parts of the court’s opinion focus narrowly on Texas law, the most compelling section embraces a due process analysis that could have wide application—outside Texas and beyond the context of presuit discovery.

The court’s opinion begins with an extended discussion of the history of Rule 202.8 Yet this discussion merely sets the stage for the precise legal question to be answered: Must a “proper court” under Rule 202 have personal jurisdiction over the potential defendant?9 The court’s answer to this question owes almost nothing to its discussion of Rule 202’s history, or to any analysis of the text of Rule 202, which is silent on the issue of personal jurisdiction.

Rather, the court bases its decision to engraft a personal jurisdiction requirement onto Rule 202 in large part on its belief that presuit discovery in Texas has become too broad and needs to be reined in, so that Texas does not become “the world’s inspector general.”10 In addition, the court argues that principles of “fairness” mandate a personal jurisdiction requirement.

There are two dimensions to this “fairness” argument. The narrower—and less persuasive—argument is based on Texas procedure. Specifically, the court compares the procedural protections available to an anonymous defendant in the presuit context with those available in the pending-suit context.11 According to the court, under Texas civil procedure, a “Doe”
the absence of a personal jurisdiction requirement under Rule 202 would “eviscerate the protections” afforded anonymous defendants in pending suits. In fact, one could argue that there is no clear difference between the procedural protections available to anonymous potential defendants in the presuit context and those available to anonymous actual defendants in the pending-suit context.

Which brings us to the broader—and more compelling—part of the Trooper court’s “fairness” argument: the court’s recognition that the absence of a personal jurisdiction requirement poses serious due process concerns under the Fourteenth Amendment.21 On this point, the court is careful to clarify that its holding is based on Rule 202, not the Fourteenth Amendment. But the court’s interpretation of Rule 202 is thoroughly infused with due process considerations.22 For example, the court quotes extensively from the “prescient words” of Hanson v. Denckla,23 explaining that the Fourteenth Amendment protects against even “minimal” burdens being imposed on a defendant who lacks a sufficient connection with the forum state.24

In cases like Trooper, the “burden” imposed on the defendant is the adjudication of his or her First Amendment right to anonymity. Trooper’s real significance, therefore, lies in the court’s recognition that the adjudication of a speaker’s right to anonymity implicates Fourteenth Amendment, as well as First Amendment, concerns. Whereas the First Amendment requires that certain questions be asked about the substance of the plaintiff’s claim prior to the unmasking of an anonymous speaker, the Fourteenth Amendment requires that a proper court undertake that inquiry. And a court lacking personal jurisdiction over the speaker is not a proper court.25

In essence, Trooper is not just a Rule 202 case; it is a due process case. As such, its potential impact may be felt beyond the context of presuit discovery, and outside Texas. Although the court bases its holding on the “proper court” language of Rule 202, that concept is not unique to this Texas presuit discovery rule. The requirement that discovery be authorized by a proper court is implicit in civil procedure rules across jurisdictions, including in the pending-suit context. If Trooper is correct that due process—and, specifically, personal jurisdiction concepts—affects the determination of whether a court is a “proper court” to issue a discovery order, then the decision has broad and deep significance.

This potentially wide application raises important and difficult questions of logistics: Is a personal jurisdiction requirement in such circumstances workable? And is it fair to plaintiffs, some of whom have legitimate claims and therefore a right to pursue those claims?

The majority and the dissent in Trooper could not agree on the answers to these questions. The majority acknowledged that the plaintiff’s burden to show a prima facie case of personal jurisdiction over an anonymous defendant was a heavy burden—maybe even “impossible” in some cases.26 The dissent predicted much more drastic consequences:

[T]he Court’s holding does not reduce or circumscribe pre-suit discovery of anonymous parties in Texas. Instead, it is the end of such discovery. . . . [W]hen a party chooses to conceal his identity, he prevents the trial court from conducting a minimum-contacts analysis to determine whether it may exercise personal jurisdiction over him.27

The dissent’s concern—that “a court cannot conduct a minimum-contacts analysis while wearing a blindfold”28—has been expressed by several courts.29 As the dissent recognized, however, many of these cases involved copyright infringement claims based on the illegal downloading of copyrighted videos.30

The Trooper dissent’s reliance on these types of copyright cases is misplaced for two important reasons. First, the defendant’s right to anonymity in illegal downloading cases is negligible, which makes a court’s adjudication of that right much less consequential than when core First Amendment speech is at issue. Second, the conduct in question—illegal downloading and file sharing—provides no clear indicia of the defendant’s contacts with the
The issue is not one of personal jurisdiction but of the territorial limits of subpoena power.

Online publication will contain sufficient indicia of the defendant’s forum contacts to allow a plaintiff to satisfy its prima facie burden. In short, it is premature to accept the Trooper dissent’s conclusion that a personal jurisdiction requirement in an anonymous speech case is inherently unworkable. Just as they have with the First Amendment right to anonymity, courts must now grapple with the Fourteenth Amendment concerns highlighted by the Trooper majority, hopefully arriving at a standard that adequately protects the anonymous defendant’s due process interests while allowing the plaintiff a reasonable chance of satisfying its burden.

Hadeed: The Limits of Subpoena Power

Just as Trooper gives anonymous speakers another arrow in their quiver, the pending Virginia Supreme Court case, Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., reminds third-party online service providers seeking to protect their users’ anonymity that they, too, have a “jurisdictional” argument. However, for these third parties, the issue is not one of personal jurisdiction but of the territorial limits of subpoena power. Properly applied, these limits can help shift battles over the discoverability of identifying information to jurisdictions with strong protections for anonymous speech.

In Hadeed, a carpet-cleaning business filed suit in Virginia state court against the authors of seven scathing reviews posted on Yelp. Hadeed alleged that the reviewers had falsely represented themselves to be customers and that their allegations of shoddy service were defamatory. The day after Hadeed filed suit against the Doe defendants, it issued a subpoena to Yelp, seeking documents that would identify the authors of each of the challenged reviews.

Yelp objected to the subpoena on substantive and on procedural grounds, but the district court overruled its objections and held the company in contempt. On appeal, Yelp argued that Hadeed had failed to satisfy its burden under the First Amendment and Virginia law to unmask these anonymous reviewers. The court of appeals rejected this substantive argument, holding that Virginia law governed the inquiry and that Hadeed has satisfied all of the relevant statutory requirements. Procedurally, Yelp argued that Virginia courts did not have subpoena power over it, based on the company’s residence in San Francisco, California. The court of appeals also rejected this argument, holding that Hadeed’s service of the subpoena on Yelp’s registered agent in Virginia subjected it to the subpoena powers of Virginia courts.

In its appeal to the Virginia Supreme Court, Yelp has again raised both arguments. Its briefs, and the briefs of supporting amici, have focused primarily on the First Amendment issue. But to reach this issue, the Virginia Supreme Court will have to consider first whether the district court erred in asserting subpoena power over a nonresident service provider. There is a very good argument that it did.

The court of appeals summarized its holding on this procedural issue as follows: “[W]e agree with the [district] court’s holding that ‘service of a subpoena duces tecum on Yelp’s registered agent in Virginia provides jurisdiction for the Court to adjudge the motion to compel.’” This holding improperly conflates three distinct concepts: service, personal jurisdiction, and subpoena power. Contrary to the court of appeals’ assumption, proper service of process alone does not confer personal jurisdiction. The exercise of personal jurisdiction still must be consistent with the state’s long-arm statute and constitutional due process. Moreover, a company’s designation of a registered agent for service of process in the state is generally insufficient, on its own, to establish personal jurisdiction.

The court of appeals also failed to distinguish between personal jurisdiction and subpoena power. These are fundamentally different concepts, subject to different limitations. Personal jurisdiction is primarily concerned with a state’s ability to subject a defendant to the judgment of its courts. Since International Shoe, the U.S. Supreme Court has recognized that this power may be exercised outside the territorial borders of the forum state, provided there are “minimum contacts” between the defendant and the forum state. But subpoena power is governed by the “strict territorial approach” of Pennoyer v. Neff. Courts and commentators have consistently recognized that subpoena power ends at the state borders. There is no such thing as “long-arm” subpoena power, and a court’s ability to exercise personal jurisdiction over a nonresident company does not mean that it has subpoena power to compel that company to produce documents located outside the state. These territorial limits on a court’s subpoena power cannot be avoided by serving the subpoena on the registered agent of a nonresident witness.

In short, the court of appeals’ holding on Yelp’s procedural argument is doubly wrong. First, Hadeed’s service of the subpoena on Yelp’s registered agent in Virginia does not provide Virginia courts with jurisdiction. And even if Hadeed could show that Yelp has sufficient contacts with Virginia to justify personal jurisdiction, there is no legal basis for a Virginia court to exercise extraterritorial subpoena jurisdiction over Yelp by requiring it...
to produce documents located outside the state. Accordingly, Hadeed must involve the California courts if it seeks documents from Yelp, a California resident.45

There are sound policy reasons for requiring plaintiffs like Hadeed to follow well-established subpoena procedures when attempting to secure documents from a nonresident online service provider. Unless and until the U.S. Supreme Court weighs in on the First Amendment requirements for unmasking anonymous online speakers, different courts will continue to have different tests. Even among the majority of courts that have embraced the Dendrite/Cahill approach, variations remain. Indeed, even Dendrite and Cahill differ in some respects. Plaintiffs with dubious claims should not be able to forum shop their way to a jurisdiction with weak protections for anonymous speech, and online service providers ought to know the circumstances under which they will be forced to disclose their users’ identifying information.

In addition, the exercise of universal subpoena power over online service providers raises serious due process concerns. Even though nonparty witnesses are not at risk of being subjected to the judgment of a court, their compliance with discovery orders obviously imposes a burden on them. A deposition subpoena may require the witness to travel to the forum state, and even a document subpoena may necessitate the hiring of local counsel. In addition, as Hadeed demonstrates, nonparties who do not comply with a court’s discovery orders are at risk of being held in contempt, which could include a fine or other sanction.46

Yet it is not clear that the exercise of extraterritorial subpoena power over service providers like Yelp would satisfy a “minimum contacts” test. It is well established that minimum contacts come in two forms: specific and general jurisdiction.47 Specific jurisdiction requires a connection between the forum, the party, and the claims being adjudicated.48 But nonparty witnesses are not facing any claims; they are merely repositories of information relating to the claims being adjudicated by the parties to the case. And the U.S. Supreme Court has recently limited general jurisdiction such that, absent extreme circumstances, a company is not subject to general jurisdiction outside the state of its principal place of business, or “home.”49 Indeed, the concept of universal “subpoena jurisdiction” based on a service provider’s virtual omnipresence harkens back to the long-discredited line of early Internet cases that found personal jurisdiction in any forum in which the defendant’s website was accessible.50 In short, a Virginia court’s direct exercise of subpoena power over Yelp would extend that power well beyond the territorial limits of the state, as well as the limits of due process.

Conclusion
It remains to be seen whether the Virginia Supreme Court will adhere to the traditional limits of subpoena power or wade into a due process dilemma. Similarly, it remains to be seen whether Trooper’s personal jurisdiction requirement will catch on in other courts, where the reasoning will need to be based explicitly on the demands of due process instead of the “proper court” requirement of Rule 202. But both cases serve as a helpful reminder that, as attention remains focused on the substantive protections of the First Amendment, potentially powerful procedural arguments remain available for online speakers and the service providers that would seek to protect their anonymity.51

Endnotes
3. Id. at *1.

4. Prior to 1999, two separate rules governed presuit discovery in different contexts. Rule 187 permitted prospective litigants to require the production of documents outside a state’s general jurisdiction. Rule 737 permitted the service of “discovery” requests to an out-of-state service provider. In 1999, Rule 187 was suppressed; Rule 737 was expanded to allow “subpoena power over online service providers raises serious due process concerns.”

5. See Dendrite, 775 A.2d at 760; Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005); see also In re Does 1–10, 242 S.W.3d 805, 820–21 (Tex. App. 2007) (endorsing the Cahill test).

7. Id. at *5.
8. Id. at *1–2.
9. Id. at *3.
10. Id. at *4–5.
11. Id. at *3.
12. Id. (footnote omitted).
13. Id. (“To allow discovery of a potential claim against a defendant over which the court would not have personal jurisdiction denies him the protection Texas procedure would otherwise afford.”).

14. Tex. R. Civ. P. 120a (providing that a personal jurisdiction challenge must be filed and decided before any other motion).

15. Tex. R. Civ. P. 120a(2).

21. Id. at *3–4.
22. Id. at *4 (“Whether due process affords protection in these circumstances...
is an issue that has not previously arisen because, as we explain below, no other American jurisdiction allows pre-suit discovery as broadly as Texas does.


33. Id. at 558.

34. Id. Unlike most jurisdictions, in which the right to anonymous speech is a matter of constitutional common law, Virginia has a statutory test for identifying anonymous online speakers. See Va. Code Ann. § 8.01-407.1.

35. Hadeed, 752 S.E.2d at 566–69.

36. Id. at 569.


38. During, 973 N.E.2d at 845.

39. See Moni Pulo Ltd. v. Trucet Oil & Gas, Inc., 130 S.W.3d 170, 175 n.7 (Tex. App. 2003) (“Although Texas law requires nonresident corporations to appoint a registered agent with a Texas address, they remain nonresidents.”).


41. See Daimler AG v. Bauman, 134 S. Ct. 746, 753–54 (2014) (citing Pennoyer v. Neff, 95 U.S. 714, 720 (1877)) (“The authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established.”).

42. See, e.g., Sygenta Crop Prot., Inc. v. Monsanto Co., 908 So. 2d 121, 127 (Miss. 2005) (finding no statutory authority that would allow court to compel nonresident nonparty to produce documents in forum state); Ryan W. Scott, Minimum Contacts, No Dog: Evaluating Personal Jurisdiction for Nonparty Discovery, 88 MINN. L. REV. 968, 984 (2004) (“Most states retain strict limits on the reach of the subpoena power, holding that subpoena service cannot reach nonparties found outside the state.”); Rhonda Wassermann, The Subpoena Power: Pennoyer’s Last Vestige, 74 MINN. L. REV. 37, 39 (1989) (“Regardless of the distance between the witness and the courthouse, the amount of contact the witness has with the state, or the need for live testimony, the states uniformly and steadfastly have refrained from exercising extraterritorial subpoena power.”).

43. See, e.g., Colo. Mills, LLC v. SunOpta Grains & Foods Inc., 269 P.3d 731, 733 n.3, 734 (Colo. 2012) (“Nor have we found any authority applying our long-arm statute, or the long-arm statute of any other state for that matter, to enforce a civil subpoena against an out-of-state nonparty.”); Ulloa v. CMI, Inc., 133 So. 3d 914, 920 (Fla. 2013) (“Even if [the corporate witness] is subject to the personal jurisdiction of Florida courts under the long-arm statute, this does not mean that [it] is required to respond to a subpoena to appear and/or to produce documents in a Florida court in a criminal case in which it is not a party.”); Phillips Petroleum Co. v. OKC Ltd., P’ship, 634 So. 2d 1186, 1188 (La. 1994) (“Whereas the long-arm statute extends Louisiana’s personal jurisdiction over persons or legal entities beyond Louisiana’s borders, there is no similar authority for extending the subpoena power of a Louisiana court beyond state lines to command in-state attendance of [out-of-state] nonparty witnesses.”).

44. See, e.g., Ulloa, 133 So. 3d at 920 (“The registered agent has a limited role, and is not a corporate employee or custodian of corporate records.”); Phillips, 634 So. 2d at 1188 & n.6 (rejecting argument that nonparty, “having qualified to do business in this state and having designated an agent for service of process, is the equivalent of a ‘resident’ of Louisiana, thus subjecting the corporation to the subpoena power of a Louisiana court”); Sygenta, 908 So. 2d at 128 (finding service of subpoena on nonresident company’s registered agent ineffective to require company to produce documents located outside the state); Reader’s Digest Ass’n v. Dauphinot, 794 S.W.2d 608, 609–10 (Tex. App. 1990) (same).

45. See, e.g., CAL. CIV. PROC. CODE §§ 2029.100 et seq.


48. Id. at 2851.


20th Annual Conference

February 5-7, 2015
Fairmont Scottsdale Princess
Scottsdale, AZ

Plenaries:

• Press Sources & Government Secrets—Striking the Proper Balance
• Native Advertising & the Illusive Line Between Commercial and Core Speech
• Cox Broadcasting Corp. v. Cohn—a Retrospective and its Impact on the “Right to be Forgotten”

Keynote Speaker:
Mary Beth Tinker
(Ms. Tinker was one of the plaintiffs in Tinker v. Des Moines Independent School District, recognizing public school students’ freedom of speech)

PLUS: 15 “Hot Topics” Sessions; Tennis & Fun in the Sun!
$5 million in presumed damages, $1 million in emotional distress, and $1 million in "future economic losses" by the jury).8

In theory, presumed damages are designed to help a plaintiff recover damages without proof of reputa-
tional harm because it is difficult to prove a negative—that a publication of a horrible lie accusing the plaintiff of criminal, professional, or sexual conduct (categorized as slander or libel per se)9 has caused clients and friends to stop calling.10 But court-
blessed windfalls are hardly necessary for a state supreme court chief justice or well-connected casino billionaire to vindicate their names, when they have plenty of other public venues and resources to create posi-
tive public opinion about themselves.

This article argues that presumed damages for public officials and public figures violate the First Amendment. These multimillion-dollar presumed damages awards chill speech and punish unpopular speakers who dare criticize government officials and public figures—something the First Amendment is supposed to guard against. In addition, presumed damages in defamation per se11 cases violate the due process clause of the Fourteenth Amendment. Punitive damages are now subject to a due process analysis; presumed damages should be as well. Indeed, presumed damages are much more arbitrary than punitive damages. Presumed damages are not tied to any evidence, give jurors unbridled power, and leave trial and appellate courts unable to conduct any meaningful review. Moreover, they are speculative, arbitrary, grossly excessive, and compulsory. Presumed dam-
ages, therefore, violate fundamental notions of fairness.

Arkansas, Kansas, Maryland, Missouri, New Mexico, and Tennessee already have eliminated presumed dam-
ages in defamation per se cases based on the First Amendment, due process, and public policy grounds, as discussed below. Iowa has barred presumed dam-
ages against media defendants, and New Jersey has restricted presumed damages. Media defense attorneys should urge more state and federal courts to follow their example.

Supreme Court Constitutionalizes Presumed Damages in Gertz

Plaintiffs love to cite Gertz v. Robert Welch, Inc.12 as their ticket to presumed damages. But Gertz contains hidden gems for defense counsel. The Supreme Court made clear in Gertz that presumed damages are subject to review under the First Amend-
ment, and are per se unconstitutional in some circumstances.13 Some juris-
dictions and legal commentators have interpreted Gertz as abolishing presumed damages altogether or when brought against media defendants involving speech of public concern, as discussed below. The door remains open for these First Amendment arguments.

The issue of presumed damages was not raised by the parties when plain-
tiff Elmer Gertz, a civil rights attorney, sought review by the Supreme Court. Remarkably, the Court decided sua sponte to constitutionalize presumed damages without "the benefit of briefs and argument" on the presumed damages issue.14 The Court delivered an unexpected broadside to the centuries-old common-law doctrine of presumed damages. It described presumed dam-
ages as "an oddity of tort law" that instructs jurors that "injury is presumed from the fact of publication," giving juries the power to "award substan-
tial sums as compensation for supposed damage to reputation without any proof that such harm actually occurred."15

The Court cautioned that presumed damages threaten First Amendment protections for free speech and press in two ways: First, the "largely uncon-
trolled discretion of juries to award damages where there is no loss" car-
ries the "potential . . . to inhibit the vigorous exercise of First Amendment freedoms."16 Second, the rule of pre-
sumed damages "invites juries to punish unpopular opinion rather than to com-
pense individuals for injury sustained by the publication of a false fact."17 The Court expressly found that "the States have no substantial interest in securing

for plaintiffs such as this petitioner gra-
tuitous awards of money damages far in excess of any actual injury."18

The Court’s 5–4 decision in Gertz held that private figure plaintiffs who establish mere negligence are precluded from recovering presumed damages.19 The Court opined that the states’ inter-
est in compensating “private individuals for injury to reputation . . . extends no further than compensation for actual injury.”20 Based on the First Amend-
ment, “[s]tates may not permit recovery of presumed . . . damages . . . when liability is not based on a showing of knowledge of falsity or reckless disre-
gard for the truth.”21

Nearly a decade after Gertz, the Supreme Court issued its confusing plurality opinion in Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.22 The Court interpreted Gertz as allowing private individuals to recover presumed damages against nonmedia defendants based on a showing of simple negli-
gence when the speech relates to private matters as opposed to speech about a matter of public concern.23 Legal scholars and courts have debated about the limits on presumed damages created by Gertz and Dun & Bradstreet. Second Circuit Judge Rob-
ert A. Sack states in his treatise that “Gertz eliminated the recoverability of presumed damages, at least, at the time, in media cases about matters of public concern.”24 Judge Sack has observed that “the Supreme Court has never stated . . . affirmative[y] . . . that presumed damages may be recovered” under the First Amendment “if actual malice is proven.”25 Thus, Gertz and Dun & Bradstreet leave the door open to arguing that the First Amendment does bar presumed damages in media cases involving public official/public figure plaintiffs, even if they prove actual malice.

The Restatement (Second) of Torts broadly defines Gertz’s First Amend-
ment safeguards against presumed damages: “The Supreme Court held that the common law rule of presumed damages is incompatible with the First Amendment freedoms and therefore unconstitutional.”26 The Restatement’s

Presumed Damages Gone Wild

continued from page 1
“general damages” rule states that “[o]ne who is liable for a defamatory communication is liable for the proved, actual harm caused to the reputation of the person defamed.” However, the Restatement refuses to take a stand on whether the First Amendment allows a plaintiff to recover presumed damages even with proof of actual malice, and posits that “there is little reason to conclude that the constitutional limitation on recoverable damages will be confined” to the circumstances of \textit{Gertz}.\textsuperscript{27}

Notwithstanding the Supreme Court’s failure to state affirmatively that presumed damages might be permitted with a showing of actual malice, lower “courts have generally assumed that proof of ‘actual malice’ permits an award of presumed damages.”\textsuperscript{28}

It is time to start challenging the assumption that presumed damages by public figures and public officials would withstand First Amendment scrutiny. \textit{Gertz} made clear that presumed damages must be tested against the First Amendment protections for free speech and press, and that “the States have no substantial interest in securing for plaintiffs ... gratuitous awards of money damages far in excess of any actual injury.”\textsuperscript{29} Surely that must be the case for public official and public figure plaintiffs who suffer no actual reputational or economic harm and still recoup millions.

\textbf{A Minority of States Have Abolished or Limited Presumed Damages}

Eight states have already eliminated or restricted presumed damages as unconstitutional or unworkable “relics” of the past. Tennessee, Maryland, Kansas, and Missouri have interpreted \textit{Gertz} as barring presumed damages in all defamation cases. In these jurisdictions, the defamation and slander plaintiff must plead and prove injury from the allegedly defamatory words. Tennessee held that “presumed damages are no longer permissible” under any circumstance, and that \textit{Gertz} had created a “uniform requirement for proof of actual damages” that “obliterate[d]” the “illogical distinctions” of libel per se and per quod, which were mostly “relics from centuries past.”\textsuperscript{30} Maryland also interpreted \textit{Gertz} as completely “forbid[ding] presumed damages.”\textsuperscript{31} Not only has Kansas abolished presumed damages entirely under \textit{Gertz} and the First Amendment, but the state also requires a defamation plaintiff to prove actual reputation harm as a prerequisite to “parasitic” emotional distress damages.\textsuperscript{32}

Missouri and New Mexico have both concluded that \textit{Gertz} abolished presumed damages under all circumstances, and rejected the view that \textit{Dun & Bradstreet} permitted presumed damages in some cases. The Missouri Supreme Court concluded that a total ban was necessary to avoid “unjustifiable iniquities for plaintiffs and defendants alike” and that all defamation plaintiffs “must prove actual damages in all cases.”\textsuperscript{33} The New Mexico Supreme Court held that the libel per se/ per quod distinction was “outmoded” and barred under \textit{Gertz}, and declined to resurrect presumed damages after \textit{Dun & Bradstreet}.\textsuperscript{34}

In contrast, when the Arkansas Supreme Court “abolished” presumed damages entirely, it relied on an implicit due process analysis.\textsuperscript{35} The court relied heavily on an article by media law Professor David A. Anderson.\textsuperscript{36} Professor Anderson, who is now a professor at the University of Texas, is highly critical of the First Amendment protections for public officials and public figures to recover presumed damages in media cases if actual malice is proven,\textsuperscript{41} the court has made clear that the First Amendment creates additional burdens for public officials and public figures suing reporters over speech of public concern, even if those constitutional burdens curb the plaintiffs’ rights under centuries-old common-law rules.

\textbf{Presumed Damages Violate the First Amendment}

Although the Supreme Court has never stated “affirmative[ly]” that the First Amendment allows public officials and public figures to recover presumed damages in media cases if actual malice is proven,\textsuperscript{41} the Court has made clear that the First Amendment creates additional burdens for public officials and public figures suing reporters over speech of public concern.

It is time to start challenging the assumption that presumed damages by public figures and public officials would withstand First Amendment scrutiny.
common-law defamation rules by prohibiting recovery without proof of fault and restricted the recovery of presumed damages.43

In Philadelphia Newspapers, Inc. v. Hepps, the Supreme Court cited New York Times and Gertz when it decided, once again, that the First Amendment required “the common-law rule [to be] superseded by a constitutional rule.”44 In Hepps, the Court held that the First Amendment required the Court to toss out the old common-law burden requiring defamation defendants to prove truth in cases involving media defendants and speech of public concern, and switched the burden to plaintiffs: “We believe that the common law’s rule on falsity—that the defendant must bear the burden of proving truth—must similarly fall here to a constitutional requirement that the plaintiff bear the burden of showing falsity, as well as fault, before recovering damages.”45

Under New York Times and its progeny, the First Amendment should be read as requiring public official and public figure plaintiffs suing over speech of public concern to prove reputational harm and as barring them from recovering any presumed damages awards. Without such a burden, plaintiffs like Justice Thomas win a promotion to chief justice of the Illinois Supreme Court and a $7 million jury award comprised of $5 million in presumed damages, $1 million for “embarrassment, mental suffering, and humiliation,” and $1 million in “future economic loss.”46 Both Justice Thomas’s $7 million jury award and his reduced award of $4 million violate the First Amendment because multimillion-dollar court awards are per se chilling to news reports about powerful public officials. Indeed, most news reports about public officials focus on their fitness in their “business, trade, profession, or office,” which opens the news organization to a claim for libel per se. Multimillion-dollar presumed damages verdicts awarded to public officials encourage other public officials to follow suit, literally.47

It is also chilling to the media when a jury awards a powerful public figure such as Wynn $17 million in presumed damages, plus $3 million in “mental anguish” or actual damages, without requiring him to prove actual reputational harm. Reporters will think twice about reporting news about Wynn and other public figures. Wynn’s only evidence of harm was his own self-serving testimony concerning his “mental anguish” about the harm that might befall his employees if his casinos suffered harm, and testimony by a gaming commission expert about all the possible investigations that gaming authorities might have taken in response to Francis’s statement.48

Because Wynn was not required to present any evidence of any harm to his reputation, there was no way for the jury to measure whether Wynn was actually shunned by friends, business associates, or potential clients. It is also possible that the Los Angeles jury punished Francis because he was an unpopular defendant, which would violate the First Amendment. Indeed, the California Court of Appeal noted that Francis “gained notoriety for creating an adult entertainment enterprise which included ‘Girls Gone Wild’ videos and DVD’s which featured ‘young, and sometimes underage, women in states of partial or total nudity, and sometimes performing more explicit sex acts.’”49

If the jury used presumed damages to punish Francis for his volatile personality or sexually oriented business, it would be an impermissible use of presumed damages to punish “unpopular opinion rather than to compensate individuals for injury sustained by the publication of a false fact,” as the Supreme Court warned in Gertz.50

The Court correctly held in Gertz that the “state interest in compensating private individuals for injury to reputation . . . extends no further than compensation for actual injury.”51

The Court also acknowledged that presumed damages in defamation cases provide “largely uncontrolled discretion of juries to award damages where there is no loss,” create the danger that the “system of liability for defamatory falsehood [will] inhibit the vigorous exercise of First Amendment freedoms,” and “invite[] juries to punish unpopular opinion.”52

These multimillion-dollar presumed damages awards are indeed “an oddity of tort law,” are outdated, and violate the First Amendment. Jury awards for presumed damages of $5 million or $17 million are “largely uncontrolled,” are not narrowly tailored to protect a substantial state interest, invite frivolous litigation, “punish unpopular opinion rather than compensate individuals for injury sustained,” chill First Amendment free speech and free press rights, and unnecessarily exacerbate “the danger of media self-censorship,” as described in Gertz.53 It is time for courts to conclude once and for all that presumed damages present a severe unconstitutional burden on defendants when sought by public official or public figure plaintiffs claiming libel per se over speech of public concern, especially against media defendants. The First Amendment and New York Times, Gertz, and Hepps require the imposition of a burden on public official/public figure plaintiffs to prove actual reputational harm to recover compensatory damages when suing over speech of a public concern, and only after reputational harm is proved can the plaintiff seek “parasitic” emotional distress damages, as the Kansas Supreme Court held in Gobin.54

Presumed Damages Violate Due Process

The Supreme Court has held that punitive damages must be subjected to constitutional scrutiny to ensure that punitive jury awards do not violate the due process clause of the Fourteenth Amendment. “One must concede,” Justice Blackmun wrote for the majority in Pacific Mutual Life Insurance Co. v. Haslip, “that unlimited jury discretion—or unlimited judicial discretion for that matter—in the fixing of punitive damages may invite extreme results that jar one’s constitutional sensibilities.”55 Justice Blackmun cautioned that just because punitive damages have been recognized for so long, “they are not immune from constitutional review.56 “[N]either the antiquity of a practice nor the fact of steadfast legislative
and judicial adherence to it through the centuries insulates it from constitutional attack.”

Perhaps in a foreshadowing of the Joe Francis empire, Justice Blackmun said that the Supreme Court was “once again . . . concerned about punitive damages that ‘run wild.’” The same due process scrutiny should be applied to the common-law doctrine of presumed damages, even if the doctrine is deeply entrenched in our judicial and legislative branches. In Haslip, the Court found that Alabama jury instructions satisfied due process because they did not give jurors “unlimited discretion” and “explained that their imposition was not compulsory.” The Court also found that Alabama met due process requirements by adopting posttrial procedures requiring courts to examine jury awards to ensure “punitive damages awards are not grossly out of proportion to the severity of the offense and have some understandable relationship to compensatory damages,” which created “meaningful and adequate review by the trial court.”

In BMW of North America, Inc. v. Gore, Justice Breyer opined in his concurrence that this due process scrutiny, “itself harkening back to the Magna Carta, arises out of the basic unfairness of depriving citizens of life, liberty, or property, through the application, not of law and legal processes, but of arbitrary coercion.” He explained that due process scrutiny is necessary to ensure that damages are fairly and uniformly applied to “similarly situated persons” and not the result of a jury’s “caprice,” and that the civil court rules governing damages must provide “some kind of constraint upon a jury or court’s discretion, and thus protection against purely arbitrary behavior” by jurors and courts alike. The due process clause, therefore, “prohibits a State from imposing a ‘grossly excessive’ punishment on a tortfeasor.”

In Gore, the Supreme Court held that a $2 million punitive damages award (reduced from $4 million) violated due process because it was “grossly excessive” compared to the $4,000 in actual harm awarded to the plaintiff. The Court concluded that the reduced award was still “grossly excessive” because it was 500 times the actual harm—a more extreme ratio than the 1:4 or 1:10 ratio between compensatory and punitive damages it had discussed in previous cases—and remanded the case back to Alabama.

In Exxon Shipping Co. v. Baker, the Supreme Court again decreed the increasing size and unpredictable nature of punitive damages and the lack of relationship to the plaintiff’s actual harm. The Court held that the ratio of compensatory to punitive damages should be 1:1 in maritime cases. The Court majority signaled that it probably would apply that same 1:1 ratio to tort cases as well.

The Court justified its drastic limitation on punitive damages as necessary “to protect against the possibility (and the disruptive cost to the legal system) of awards that are unpredictable and unnecessary.”

The due process guideposts required under Haslip and Gore are utterly lacking for presumed damages. There is no meaningful guide in jury instructions. Some jurisdictions, such as California, instruct jurors that the plaintiff is “entitled” to a presumed damages award and that they “must” award at least nominal presumed damages. These instructions for presumed damages create a category of “compulsory damages” that the Supreme Court cautioned would create due process problems.

There is also little guidance for trial courts and appellate courts. When the size of the presumed damages award is left to the unbridled discretion of the jury, it is difficult for a court to determine if the jury’s award is “grossly excessive.” If there are no actual damages awarded for out-of-pocket losses or actual reputational harm, the court is unable to conduct an analysis to measure proportionality of the presumed damages. There can be no ratio of 1:10 or 1:4 or 1:1 described in Haslip, Gore, and Exxon Shipping. As scholars have explained:

Judges cannot give meaningful instructions when the substantive law concedes that “there is no legal measure of damages in actions for these wrongs. The amount which the injured party ought to recover is referred to the sound discretion of the judge.” As a result, “the process of fixing the amount of presumed damages is inherently irrational.”

Juries also may be tempted to consider factors, such as the defendant’s unpopularity, that have nothing to do with any harm caused to the plaintiff. The huge size of some presumed damages awards—even when there is a complete lack of evidence of actual harm—suggests that they function as de facto punitive damages.

New Jersey is one jurisdiction that has implicitly recognized large presumed damages awards violate due process. The New Jersey Supreme Court recently held that presumed damages must be limited to nominal damages and compensatory damages must be established with actual harm to reputation, pecuniary or otherwise.

Yale University argued in a libel per se case in a U.S. district court in North Carolina that presumed damages are unconstitutional under the due process clause because they are “inherently speculative and irrational,” invite jury awards “based on emotion and prejudice,” and “offend our fundamental notions of fairness.” Calling Yale’s due process argument “novel,” the court “conceded[d] that, as a policy matter, reasons exist to disfavor presumed damages” and that “there may be room for debate concerning the wisdom of presumed damages.” But the district court rejected the due process challenge, observing that the Supreme Court “has had ample opportunity to strike down presumed damages and has not done so,” while admitting that the Court has not considered a due process challenge to presumed damages.

Perhaps the Supreme Court will one day decide to find presumed damages unconstitutional but obviously that has not yet occurred.” However, the district court did not address Haslip, and the Supreme Court had not yet decided Gore or Exxon Shipping at the time of the district court’s 1993 decision.
Given the inherent “unlimited jury discretion” and “unlimited judicial discretion” in fixing presumed damages, the “extreme” multimillion-dollar awards despite the utter lack of reputational or economic harm, and the “compulsory” jury instructions, there is no question that presumed damages “jar one’s constitutional sensibilities” and have “run wild.”

**Presumed Damages Create Evidentiary Barriers that Violate Due Process**

In some jurisdictions, plaintiffs argue that presumed damages are not arbitrary or unfair because the defendant can present rebuttal evidence showing the plaintiff suffered no injury at all. In practice, however, the rebuttal evidence doctrine does not work.

The problem is that courts allow plaintiffs to introduce purely speculative evidence that is difficult to rebut, while barring defendants from obtaining discovery on the plaintiff’s finances and other records that would rebut the presumption of reputational harm. In *Wynn*, the Los Angeles County Superior Court allowed casino mogul Wynn to introduce expert testimony that casino licensing authorities “could” have opened an investigation into Wynn based on the statements by Francis.** Wynn also testified that he suffered “mental anguish” over worries that his employees might suffer if his casinos suffered future potential harm caused by Francis’s statements. Cross-examination may not be strong enough to rebut such speculative evidence.

In *Thomas*, the state court trial judge allowed Justice Thomas to introduce speculative testimony by experts that if Justice Thomas ever followed up on his vague plan to apply for a federal judgeship or equity partnership in a Chicago firm at some point in the future, his application would be hurt by the newspaper report. The highly speculative testimony won Justice Thomas $1 million from the jury in “future economic losses.” The trial court later vacated the future economic losses award as “purely speculative,” but not before the defendants incurred significant expense on economic damages experts at trial and Justice Thomas scored sympathy points with the jury.**

Justice Thomas also won a $5 million jury award for presumed reputational damages despite the fact that every third-party witness testified that the plaintiff did not suffer any loss in reputation caused by the article, “still enjoys a good reputation, and earned a promotion on the high court. The jury seemed to ignore this rebuttal evidence. The trial court held that Justice Thomas did “not need evidence” for a presumed “loss of reputation, thereby making the determination of such damages purely a jury function.”** The trial court did, however, reduce Justice Thomas’s presumed reputational harm award to $3 million. The court held that given the “paucity of evidence” of actual reputational harm, the jury’s $5 million presumed reputational award “falls outside the range of fair and reasonable compensation, was the result of passion and prejudice, and shocks this judicial conscience.”** Despite the lack of evidence of reputational harm, the court refused to vacate Justice Thomas’s $1 million emotional distress award.**

The reliance on speculative evidence is nothing new. In *Gertz*, after remand from the Supreme Court, Gertz established actual malice and was permitted to introduce similarly speculative presumed reputation testimony at his second trial. Gertz was permitted to call a witness who testified “that calling a lawyer a Communist would be highly injurious to professional reputation”—not that it actually caused reputational harm to Gertz.**

Sometimes, even rebuttal evidence establishing a plaintiff’s unharmed reputation will not dissuade a jury from awarding presumed damages or persuade a court to vacate them. For example, in *Liberty National Life Insurance Co. v. Daugherty*, the Alabama Supreme Court refused to vacate the jury’s $300,000 presumed damages award, despite rebuttal evidence of the plaintiff’s “excellent” reputation.** The court held that “the law recognizes a right to recover for mental anguish” for presumed damages—even if the defendant’s rebuttal evidence “negated any injury to his reputation.”**

Courts also may block a defendant entirely from discovery of powerful impeachment evidence to rebut presumed damages. This happened in a libel per se case in Kansas state court. The plaintiff said he was not seeking any damages against the newspaper for actual reputational harm or economic loss, only for emotional distress/presumed reputational damages. The trial court agreed to block discovery and trial testimony about the plaintiff’s lengthy criminal record, civil litigation, and economic status. The jury awarded the plaintiff $100,000 “for claimed harm to his innermost feelings” about presumed reputational harm, without learning about his criminal past and or “hearing and determining what his true reputation was in the community.”** Stung by the realization that a criminal plaintiff could use presumed damages to whitewash his reputation and win a $100,000 jury award, the Kansas Supreme Court issued a new rule barring all presumed damages and requiring all defamation plaintiffs to present evidence of reputational harm, because “[d]efamation actions in Kansas are primarily concerned with injury to reputation, not injury to one’s personal sensitivities” and “[i]njuries to the latter alone cannot support a claim for defamation.”**

**Conclusion**

As these cases illustrate, trial courts tend to allow purely speculative presumed damages that would normally be excluded under well-established discovery rules for future economic losses in other tort and contract cases. Courts sometimes bar discovery or testimony on the plaintiff’s actual reputation. The idea that defendants will be able to challenge “presumed” damages with rebuttal evidence is largely an illusion when discovery of the plaintiff’s finances and other records is blocked by the court as “irrelevant” to presumed reputational harm. These
discovery issues provide another basis to challenge presumed damages on due process grounds.

The use of presumed damages by all plaintiffs—but especially public official and public figure plaintiffs—is an abuse of our judicial system and a violation of due process. Our public courts are supposed to mete out justice and follow the rule of law, not rubber-stamp huge monetary awards to uninjured plaintiffs when the awards are, by definition, compulsory, speculative, arbitrary, unreviewable—and unconstitutional.

Endnotes

2. Wynn v. Francis, No. B245401, 2014 WL 2811692, at *3–4 (Cal. Ct. App. June 23, 2014) (unpublished decision). The trial court reduced the mental anguish/actual damages award to $2 million. The jury also awarded Wynn $20 million in punitive damages, which were vacated by the trial court due to the lack of evidence of Francis’s current financial worth. Id. at *4–5. Francis’s first “shovel death threat” statement was made during a judgment debtor proceeding convened by Wynn, but the appellate court held that Francis’s statement was not sufficiently related to that proceeding to qualify for the litigation privilege. Id. at *2–3, *5–6. Francis’s other two statements repeating what he said in court were made immediately outside the courtroom to a staff member of the celebrity news organization TMZ, and during Francis’s appearance on ABC television’s Good Morning America program to talk about the Wynn v. Francis slander case. The TMZ staffer said he did not “really believe” the statement because of “the way [Francis] was acting and given his past.” Id. at *3. Wynn did not sue TMZ for publishing Francis’s “shovel death threat” statement.
3. Memorandum Opinion at 17–20, Thomas v. Page, No. 04-LK 013 (Ill. Cir. Ct. Kane Cnty. Mar. 30, 2007). The only testimony about Justice Thomas’s supposed loss of reputation “came from Justice Thomas himself,” which the trial court later held “hardly supports an award of $5 million.” Id. at 18. The trial court reduced Thomas’s presumed damages award from $5 million to $3 million, vacated his $1 million “future economic losses” award, and left intact his $1 million in emotional distress award, but the total award of $4 million is hardly a nominal award for a judge who provided no evidence of any reputational or economic harm.
4. Wynn, 2014 WL 2811692, at *4. Francis challenged the evidentiary basis for $10 million of the $17 million presumed damages award. The Los Angeles County Superior Court rejected the challenge, leaving the $17 million presumed damages award intact. The California Court of Appeal noted—perhaps with regret—that Francis’s appeal made no challenge to the evidentiary basis for Wynn’s $17 presumed damages award or his $2 million mental anguish/actual damages award. Id. at *4–5.
6. See Wynn, 2014 WL 2811692; Memorandum Opinion, supra note 3.
7. Complaint for Slander, Wynn v. Chamos, No. 3:14-cv-04329-MEJ (N.D. Cal. Sept. 25, 2014), ECF No. 1. Wynn sued on behalf of himself and his corporation, Wynn Resorts Limited. His complaint alleges that Chamos told a group of attendees at an “invitation only” event in Berkeley, California, in April 2014 that Wynn and his company had violated the Foreign Corrupt Practices Act. The complaint alleges a claim for slander per se, so defamation per se is a “defamation per se” tort, but most jurisdictions have combined libel and slander per se, so defamation per se is a reasonably accurate label.
8. First Amended Complaint, Ryan v. Fox Television Stations, Inc., No. 10-L-6258 (Ill. Cir. Ct. Cook Cnty. May 19, 2011). Judge James Ryan alleged claims for defamation per se, false light, intentional infliction of emotional distress, and intrusion against several media defendants over several news reports about his work hours, and sought $7 million in compensatory damages for each claim and unspecified punitive damages, for a total of $28 million. Id.; see also Transcript of Oral Argument, Ryan v. Fox Television Stations, Inc., Nos. 1-12-0005, – 0007 (Ill. App. Ct. Sept. 25, 2012) (on file with author) (explaining Ryan’s $7 million per-claim demand was based on Thomas’s $7 million jury award).
9. “One who publishes matter defamatory to another in such a manner as to make the publication a slander [or libel] is subject to liability to the other although no special harm results if the publication imputes to the other (a) a criminal offense[,] (b) a loathsome disease[,] (c) matter incompatible with his business, trade, profession, or office[,] or (d) serious sexual misconduct.” Restatement (Second) of Torts § 570.
10. Restatement (First) of Torts § 621 & cmt. a. The rationale for permitting a defamed person to recover for presumed reputational harm without a showing of “any specific harm to his reputation or any other loss caused thereby” is that “in many cases the effect of defamatory statements is so subtle and indirect that it is impossible directly to trace the effects thereof to the person defamed. . . . If . . . the defamatory publication is of such kind and was published under such circumstances as to justify the inference of some general impairment of his reputation or, through loss of reputation, to his other interests, he is entitled to recover general damages therefor.” Id.; see also Weller v. Am. Broad. Cos., 283 Cal. Rptr. 644, 659 (Ct. App. 1991); DiGiorgio Fruit Corp. v. AFL-CIO, 30 Cal. Rptr. 350, 359–60 (Dist. Ct. App. 1963).
11. I recognize that there is technically no “defamation per se” tort, but most jurisdictions have combined libel and slander per se, so defamation per se is a reasonably accurate label.

31. Metromedia, Inc. v. Hillman, 400 A.2d 1117, 1123 (Md. 1979) (holding that Gertz and the First Amendment require a libel plaintiff to plead “a basis for believing that the plaintiff has sustained actual injury”).

32. Gobin v. Globe Publ’g Co., 649 P.2d 1239, 1244–44 (Kan. 1982) (adopting the “rule that the plaintiff in an action for defamation must first offer proof of harm to reputation; any claim for mental anguish is ‘parasitic,’ and compensable only after damage to reputation has been established”).

33. Nazeri v. Mo. Valley Coll., 860 S.W.2d 303, 313 (Mo. 1993) (en banc (interpreting Gertz as holding that all claims for libel per se and presumed damages violate the First Amendment).

34. Smith v. Durden, 276 P.3d 943, 948 (N.M. 2012) (requiring that defamation plaintiffs must “prove actual injury to reputation and actual resulting damages” in media and nonmedia cases alike).

35. United Ins. Co. of Am. v. Murphy, 961 S.W.2d 752, 754, 756 (Ark. 1998) (holding that all defamation plaintiffs “must prove reputational injury in order to recover damages”).


37. Murphy, 961 S.W.2d at 756 (citing Anderson, supra note 36, at 749–52).

38. Bierman v. Weier, 826 N.W.2d 436, 447 (Iowa 2013) (declining to abolish presumed damages for nonmedia defendants and holding that defamation plaintiffs suing media clients can recover damages only if they establish “actual reputational harm” and “parasitic damages,” i.e., “personal humiliation or mental anguish” are permitted against media defendants only if reputational harm is proved first).


40. See, e.g., Delta Health Grp., Inc. v. Stafford, 887 So. 2d 887, 896 (Ala. 2004) (“Damage is implied by law when spoken words are found to be slander per se.”); MacDonald v. Riggs, 166 P.3d 12, 15 (Alaska 2007) (noting that libel and slander per se do not require proof of special damages); Denver Publ’g Co. v. Bueno, 54 P.3d 893, 900 (Colo. 2002) (“[I]f the plaintiff is a private person, and the claim is for libel per se, the plaintiff need not prove actual damages.”); Gaudio v. Griffin Health Servs. Corp., 733 A.2d 197, 215 (Conn. 1999) (finding that reputational injury could be conclusively presumed in a defamation action by an employee against an employer for claims made in a termination letter); Tuite v. Corbitt, 866 N.E.2d 114, 121 (Ill. 2006) (“A statement is defamatory per se if its defamatory character is obvious and apparent on its face and injury to the plaintiff’s reputation may be presumed.”); Baker v. Tremco Inc., 917 N.E.2d 650, 657 (Ind. 2009) (stating that in a defamation per se action, no proof of injury is required); Stringer v. Walmart Stores, Inc., 151 S.W.3d 781, 793–94 (Ky. 2004) (indicating that Kentucky follows a traditional common-law approach to defamation per se in private plaintiff/private concern cases and that damages and malice are presumed); Costello v. Hardy, 864 So. 2d 129, 140 (La. 2004) (stating that “[w]hen a plaintiff proves publication of words that are defamatory per se, the elements of falsity and malice (or fault) are presumed, but may be rebutted by the defendant” and “[t]he element of injury may also be presumed”);

41. Morgan v. Kooistra, 941 A.2d 447, 455 (Me. 2008) (indicating that defamation action requires “either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication”); Mitau v. Campbell, 706 N.W.2d 420, 421 (Mich. 2005) (indicating that defamation per se renders a statement actionable “irrespective of special harm”); State v. Crawley, 819 N.W.2d 94, 104 (Minn. 2012) (stating that Minnesota recognizes defamation per se, which is “actionable without any proof of actual damages”); Speed v. Scott, 787 So. 2d 626, 632 (Miss. 2001) (explaining that no proof of special harm is required for slander per se); Blue Ridge Homes, Inc. v. Thein, 191 P.3d 374, 382 (Mont. 2008) (“Defamation per se requires no proof of special damages.”); McCune v. Neitzel, 457 N.W.2d 803, 810 (Neb. 1990) (“In a suit for slander per se, no proof of any actual harm to reputation or any other damage is required for the recovery of either nominal or substantial damages.”); Bongiovanni v. Sullivan, 138 P.3d 433, 448 (Nev. 2006) (finding a doctor’s statement that another doctor had poor surgical skills was slander per se and the plaintiff was entitled to presumed damages); Lassonde v. Stanton, 956 A.2d 332, 342 (N.H. 2008) (upholding a damages award to a home contractor in a defamation per se case despite the absence of proof of damages); Geraci v. Probst, 938 N.E.2d 917, 922 (N.Y. 2010) (stating that damages will be presumed “for statements that charge a person with committing a serious crime or that would tend to cause injury to a person’s profession or business”); Ellis v. N. Star Co., 388 S.E.2d 127, 129 (N.C. 1990) (noting that the court has previously held that in libel per se actions, damages may be presumed without a finding of malice); Brown v. Gatti, 145 P.3d 130, 133 (Or. 2006) (explaining that certain defamation is actionable without proof of specific harm); Nassa v. Hook-SuperRx, Inc., 790 A.2d 368, 374 (R.I. 2002) (“For slander per se, a plaintiff can establish liability without a showing of special or pecuniary damages because those damages are presumed.”); Fontaine v. First Reliance Bank, 730 S.E.2d 305, 309 (S.C. 2012) (indicating that when a statement is defamatory per se, the defendant “is presumed to have acted with common law malice and the plaintiff is presumed to have suffered general damages”); Salinas v. Salinas, 365 S.W.3d 318, 320 (Tex. 2012) (“Our law presumes that statements that are defamatory per se injure the victim’s reputation and entitle him to recover general damages, including damages for loss of reputation and mental anguish.”); Larson v. SYSCO Corp., 767 P.2d 557, 560 (Utah 1989) (indicating that with defamation per se, malice and damages are presumed); Askew v. Collins, 722 S.E.2d 249, 251 (Va. 2012) (concluding as a matter of law that “the jury needed no proof of damages suffered by Collins on which to predicate its compensatory award based upon the per se defamation”); In re Judicial Disciplinary Proceedings against Gableman, 784 N.W.2d 605, 624 (Wis. 2010) (“A plaintiff in a traditional defamation action, unless proceeding on a theory of defamation per se, proves damages or a harm to reputation.”); Hoblyn v. Johnson, 55 P.3d 1219, 1233 (Wyo. 2002) (“Defamation per se means a statement which is defamatory
on its face and, therefore, actionable without proof of special damages.” (internal quotation marks omitted)).

41. Sack, supra note 23, § 10:3.3, at 10-12 n.50.
44. 475 U.S. 767, 776 (1986).
45. Id.
47. See supra note 8 and accompanying text.
51. Id. at 348–49.
52. Id. at 349.
53. Id. at 349–50.
56. Id.
57. Id. (quoting Williams v. Illinois, 399 U.S. 235, 239 (1970)).
58. Id.
59. Id. at 19.
60. Id. at 19–22.
62. Id. at 587–88.
63. Id. at 562 (majority opinion).
64. Id. at 582, 585–86.
66. Id. at 493, 513.
67. Id. at 513.
68. See id.
70. Anderson, supra note 36, at 750.
73. Id. (citing Anderson, supra note 36, at 749–56; Francis D. Murnaghan, From Figment to Fiction to Philosophy—The Requirement of Proof of Damages in Libel Actions, 22 Cath. U. L. Rev. 1 (1972)).
74. Id.
75. Id. at 67.
77. Powers, supra note 48.
79. Id. at 17.
80. Id. at 18–19.
81. Id. at 18.
82. Gertz v. Robert Welch, Inc., 680 F.2d 527, 540 (7th Cir. 1982) (emphasis added). In his second trial after remand, Gertz won $100,000 in “compensatory” damages based solely on his own self-serving testimony about his “severe mental distress, anxiety and embarrassment which he suffered as a result of the article”: he presented no evidence of actual reputational harm or economic harm. Id. Gertz’s mental anguish award would be worth approximately $300,000 in 2014 dollars. 83. 840 So. 2d 152, 163 (Ala. 2002). 84. Id. at 162.
86. Id.

**INTERNET PUBLISHING PERILS AND PRACTICES**

STEVEN D. ZANSBERG AND JOHN P. BORGER, EDITORS

The ever-changing digital landscape is a tricky place for legal practitioners. The rules and laws governing electronic communications have grown out of legal concepts imported from more traditional fields, adapted from prior law, and created to address the unique features of the constantly evolving digital landscape. Charting a course through the digital domain has grown easier, but remains fraught with potential hazards. This volume offers a compass and some landmarks for that journey.

Providing analysis of relevant case law, this volume is an accessible tool for those with general legal knowledge who do not encounter this area regularly. It explores, in detail, questions and concepts related to liability, defamation, privacy, copyright infringement, website terms of use, and employer’s rights and risks in relation to employees’ off-duty online conduct. This thorough treatise was written by an impressive panel of attorneys from across the country with expertise in First Amendment issues, media law, intellectual property, advertising, e-commerce, data privacy, and other relevant practice areas.

Your clients count on you to chart the correct path. This book is your guide to successfully navigate the wilds of electronic communications in the digital frontier.

Product Code: 5550030   List Price: $54.95   Member Price: $46.95

To order, call the ABA Service Center at 800-285-2221 or visit our website at www.ShopABA.org.
Dear Fellow ABA Member,

In the spirit of the season, please support your colleagues’ commitment to the rule of law and to the practice of law by giving a free trial ABA and Section membership.

Share what ABA membership has meant to you and how the ABA’s resources will help attorneys you know become better lawyers:

- 32 Sections, Divisions and Forums
- Free CLE Series
- Free Career Advice Series
- Nationwide network of colleagues
- Specialized committees and task forces

Give the gift of a free trial ABA and Section membership by sharing the enclosed cards.

Sincerely,

William C. Hubbard

William C. Hubbard
President, American Bar Association
P.S. To learn about more ways to share, visit ambar.org/gift.
ACCEPT THIS GIFT BY JANUARY 31, 2015

Visit ambar.org/abagift, or call 800-285-2221 and use code ABAGIFT

For new members only. Offer ends 1/31/15. Visit ambar.org/abagift for full offer details and rules.