



Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations

a.k.a. Craig R. Scott

To cite this article: a.k.a. Craig R. Scott (2004) Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations, Free Speech Yearbook, 41:1, 127-141, DOI: [10.1080/08997225.2004.10556309](https://doi.org/10.1080/08997225.2004.10556309)

To link to this article: <http://dx.doi.org/10.1080/08997225.2004.10556309>



Published online: 21 Dec 2012.



Submit your article to this journal [↗](#)



Article views: 840



Citing articles: 4 View citing articles [↗](#)

Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations

“Bronco” (a.k.a. Craig R. Scott)

The University of Texas at Austin

Anonymous communication has a relatively long and sometimes controversial history in this country. From the anonymous publishing of the *Federalist Papers* under the pseudonym “Publius” over two centuries ago to anonymous sources such as “Deep Throat” during the Watergate scandal, anonymity has played and continues to perform a unique role in American culture. The ability to communicate anonymously is viewed as part of our basic right to free speech—an interpretation historically upheld in U.S. courts (Bowman 2001) but increasingly problematized by new communication technologies (see Lipinski 2002). Indeed, concerns and debates about anonymous communication may well be at an all time high. Even though we all experience anonymity in a variety of somewhat mundane ways (e.g., anonymous letters to the editor/media, tips to law enforcement, organizational evaluations/appraisals, “leaks” and “whistleblowing,” church confessionals, suggestion boxes, “secret” admirers, letters with no return address, call-in radio show comments, anonymous gift giving, caller-id blocking, some forms of electronic mail, certain online meetings, and a range of support groups; see Anonymous 1998; Marx 1999), recent events have propelled discussions of anonymity to the national stage. The anthrax-laced letters anonymously sent to various influential individuals in our country in late 2001 and the invasive legislation prompted in part by such actions, as well as the growing use (and some would argue, *misuse*) of new communication technologies affording users at least some anonymity, point to two influential explanations for our growing interest and concern about anonymous communication.

First, in the ongoing aftermath from the events of September 11, 2001, there exists a climate of suspicion and heightened security that seems increasingly interested in establishing identity. Terrorists’ use of the Internet to communicate with one another covertly has furthered concerns by law enforcement and others (Wieland 2001). Indeed, Marx (2001) confirms that identification technologies have greatly expanded in recent years (e.g., facial/retinal/vocal recognition systems). As will be examined in more detail below, judicial and organizational officials are increasingly likely to take actions limiting one’s privacy and to provide identifying information in the name of national security—all of which erodes anonymity. However, this has led, in part, to resistance through anonymity. Samoriski (2002) suggests

“the retreat from the prying eyes of surveillance has led to the spread of technologies of anonymity . . . citizens are seeking privacy and anonymity at a time when the government and the business sector are using information technology to compile bigger databases [of information about citizens]” (161).

Diane Saco (2002), in her book *Cybering Democracy*, advises “Precisely because we live in a context wherein surveillance has become ubiquitous . . . anonymity can become a viable and even advisable form of resistance” (119).

Another driving force centers on technology. This issue is most real in the virtual, online environment(s) of the Internet (and other networked communication technologies). In many ways, communication technology makes anonymity more possible—given the obvious challenges of maintaining anonymity in unmediated situations. For example, individuals have the ability to communicate anonymously or pseudonymously using chat rooms, discussion boards, multi-user domains (MUDs), instant messaging (IM), group decision support systems, caller-id blocking as well as anonymous remailers and anonymous web surfing.¹ Of course, some experts (see Turkle 1995) describe the online experience as being largely anonymous in general also. For some, the ease with which people can now communicate anonymously is cause for concern. Not surprisingly then, these same technologies are also used to trace individuals. For example, several of the technologies mentioned here create logs indicating the message and/or computer source. The use of certain screen names or other pseudonyms may also reveal identity. I have playfully penned (keyboardeed?) this chapter under the pseudonym “Bronco”—which I regularly use as an online identity based on my fanaticism about Denver’s professional football franchise. Also, system operators and service providers are typically able to ultimately identify the source of an otherwise anonymous message.

As a result of these forces, previously protected rights to free speech via anonymous online communication are now being questioned. As one legal scholar noted: “The status of anonymous speech as a protected right is contracting, and given technological changes, the anonymous speaker faces unprecedented new challenges. Given the changing nature of anonymous speech from the eighteenth century to the twenty-first, it is likely that the anonymous writer Publius—celebrated by the Founding generation—will soon be dead” (Wieland 2001 590). Before “Anonymous” potentially suffers such a fate, and perhaps to prevent its death completely, we need to better understand the dangers and necessity of anonymous online communication. To that end, this essay begins by more thoroughly defining anonymous online communication and considering its most commonly discussed drawbacks and benefits. Next, court cases regarding anonymous online communication are reviewed to gain a clearer sense of this issue—focusing heavily on what have been termed “John Doe” and “cybersmearing” cases. Finally, based on that casework and current legal opinions, several critiques and communicative recommendations are offered to more thoroughly address the complex challenges posed by online anonymity. If the *Fast Company* magazine columnist who recently proclaimed, “we’re entering an era of anonymity” (Godin 2001 86) is correct, then it is imperative that such analysis take place to ultimately preserve anonymous online communication as an increasingly important form of free speech.

Background: Defining Online Anonymity

Williams’s (1988) argument, “anonymity is a notion that ought to be thought, taught and written about much more than it is at present” (765) is perhaps even more true today with the widespread use of various online communication tools that provide at least some sense of anonymity. In thinking about this construct, it is essential to define it relative to related constructs and talk about various types of anonymity. Most simply, *anonymity*—whether online or not—is the condition in which a message source is absent or largely unknown to a message recipient. Similarly, an anonymous source is one with no known name or acknowledged identity. *Confidentiality* differs in that the source of a comment is known to a few, but the identity of the source is not further revealed to the ultimate message recipients. Thus, the source is absent to all with anonymity; however, confidentiality is a condition in which the source can be connected to his or her comments by some (e.g., researchers, reporters) who agree not to reveal the source to

others (see Anonymous 1998). Furthermore, a sense of anonymity may be achieved through a fictitious alternative identity called a *pseudonym* (e.g., “Bronco”). These fictitious identities take two general forms: sources perceived as fictitious to the message receiver and sources perceived as factual to the message receiver. The former most closely fit ideas related to online anonymity. The latter (taking on another person’s actual identity, assuming an invented identity) is substantially different because receivers may have no reason to suspect that the apparent message source is not the actual message source. Although issues related to identity theft and the use of aliases are indeed fascinating and deserving of more attention from communication scholars, they are not immediately relevant to a discussion of free speech and online anonymity.

Elsewhere (Anonymous 1998) I have suggested the following definition of anonymity for communication scholars: the degree to which a communicator perceives the message source is *unknown* and *unspecified*. By *source specification* I mean the extent to which a message source is distinguished from other possible sources. Generally, this dimension ranges from being a general member of some large public grouping to recognition as a specific, singular (though not necessarily known) individual. *Source knowledge* concerns the degree of familiarity between the source and the receiver, and may range from the two being complete strangers to being close friends. In more communicative terms, knowledge level varies between instances where a receiver has had no prior interactions with or information about the source, to situations where the receiver has had numerous prior interactions and may possess a fair amount of information about the source (e.g., knowing one by name).

There are several different types of anonymity. *Physical* (i.e., visual) anonymity is when one cannot sense the physical presence of a message source (e.g., hooding subjects in research studies). *Discursive* anonymity, on the other hand, is the condition in which specific comments cannot be attributed to a specific individual source; thus, it is tied directly to verbal communication. Kling, Lee, Teich, and Frankel (1999) also distinguish between *traceable anonymous communication*, *untraceable anonymous communication*, *traceable pseudonymous communication*, and *untraceable pseudonymity*. Additionally, there are differences between *self-anonymity* (a sender’s perceived anonymity to others when he/she is the message source) and *other-anonymity* (the anonymity experienced when a user receives communication from an unidentified source). As Spears and Lea (1994) note, self- and other-anonymity are “related but conceptually distinct” (430), leading them to distinguish between what they call “identifiability” (self’s anonymity to others) and “anonymity” (others’ anonymity to self).

Perhaps most relevant here is the distinction between what Johnson (1997) labels *offline* anonymity (including face to face, telephone, and traditional media) and *online* anonymity (when using computer-based network systems, primarily the Internet). This author suggests that achieving anonymity in the former requires sender effort but that it is more the natural state of affairs in the latter. Although the types of anonymity outlined in the previous paragraph are all possible online, there are other aspects of online anonymity that make it potentially even more powerful. Most notably, because the Internet is highly accessible and relatively cheap (Crumph 2003), it provides a wide range of the population with a channel for voicing dissent. Chiger (2002) adds that “speaking in an Internet forum is tantamount to making a conference call with half the planet” (52); thus, with ability to copy, repost, and mass mail, anonymous communicators can reach far greater numbers of recipients. O’Brien (2002) adds that Internet statements may be longer lasting, lacking in editorial oversight, and more capable of finding a receptive audience.

Two other characteristics help to define how online anonymity *should* be viewed. First, anonymity must be considered to exist along a continuum from fully anonymous to fully identified. Thus, a source is not simply anonymous or identified, but may also be partially so. Second, anonymity is usefully viewed as a perception of the communicators involved. Although certain processes and technologies may claim to be anonymous (or not), usage behavior and

other effects likely depend far more on the extent to which communicators perceive anonymity. Although such views are consistent with recent theorizing about anonymity (Anonymous, 1998; Marx, 1999), much of the work in legal and other scholarly circles tends to treat online anonymity as an on/off feature of specific technologies. Legal experts often talk about the “perfect” anonymity of the Internet (see Crump 2003), though others have reminded their scholars that “the phrase ‘Internet anonymity’ is innately an oxymoron” (Chiger 2002 53). In summary, anonymous online communication may differ in several key ways from other forms of anonymity—most notably in that it can reach more people with less cost, and greater potential power. Furthermore, it has a great deal to do with the level of perceived anonymity in a communicative situation, even though it has historically been considered in more simplistic ways. Given its potential impact and social nature, a closer examination of the pros and cons of anonymous online communication is warranted.

Dangers and Benefits of Anonymous Online Communication

Perhaps any discussion of pros and cons should begin with the disclaimer that “anonymous communication online is morally neutral” (Teich et al. 1999 72), meaning any dangers or benefits concern how it is used. Without question, it has and almost certainly will continue to be used for purposes that facilitate both beneficial and detrimental outcomes. I begin with an overview of the major arguments related to the dangers of anonymity, especially online. Next, the beneficial uses of anonymity are reviewed as an important point of comparison.

Dangers

I was recently struck by a response from an organizational employee to an open-ended survey question I had sent about when anonymity might be appropriate, because it captures some of the most extreme concerns about anonymous communication: “I don’t really believe it’s appropriate. I want accountability. I answer the telephone with my full name. I put my full name on my answering machine at home and work. I feel that America’s obsession with ‘anonymity’ is a copout; it breeds irresponsibility, non-accountability and shabby work. In the extreme case it breeds a lifestyle of sinfulness and overindulgence.” Beyond the irony that this comment was made anonymously, it illustrates that accountability for one’s actions seems to underlie most concerns about the dangers of anonymity— especially online anonymity given its potential for wider access and impact. Lemley (1999) describes the lack of accountability as “both the greatest virtue and the greatest problem with anonymity” (262). Stein (2003 193) suggests that “with respect to accountability, there are two potential repercussions of anonymity that are cause for concern: first, anonymity will lead to crime; and second, anonymity will undermine free speech rather than advance it.” A speaker who feels anonymous may choose to libel, slander, and defame (even though such actions are illegal). In fact, perhaps the fastest growing issue related to online anonymity concerns issues of what is sometimes called cybersmearing, where individuals use online anonymity to promote false statements about other people or organizations. Free speech does not extend to defamation, for instance, so anonymity is inappropriate then (see Lipinski 2002); however, because some individuals are able to successfully hide behind the veil of anonymity and disparage others (e.g., current/former employers may be criticized on Internet financial forums which can drive down stock prices), many individuals view this troubling use of anonymity as an especially strong drawback.

Another concern about anonymity directly related to free speech concerns flaming. Defined as the exchange of rude or hostile messages between online participants (Barnes 2003), flaming may be facilitated by the sense of anonymity and the reduced accountability the participants

feel online. Although it is probably the most publicized form of online misbehavior (Barnes), recent work has questioned just how widespread this is and has pointed to the need to entirely reconceptualize the construct (O'Sullivan & Flanagin 2003).

Although they are less directly related to free speech concerns, accountability is also at issue regarding the use of the Internet to conduct terrorist activities and other threats to national security. Dystopian rhetoric about the use of anonymity for high tech pedophilia, virtual pornography, destructive computer viruses, and other forms of cybercrime all point to potential negatives associated with the lack of online accountability.

Another set of concerns centers not so much around accountability, but the possibility that anonymity actually "undermines rather than improves public debate on important issues" (Stein 2003 193). Audiences have a harder time evaluating credibility, and there is more room for deception and frivolousness. "Knowing a speaker's identity is necessary to better evaluate the truthfulness of the assertions" (Barnes 1999 386). People communicating anonymously may believe they have to do so because it would be unsafe to do otherwise—further undermining the value we may perceive as individuals in speaking openly and in an identified fashion. Anonymous speech may seem like less sincere and less involved participation for many. Related to this are concerns about trust. Nissenbaum (2003) contends that online anonymity decreases trust, because we know relatively little about personal character and even the nature of the relationships in which we are involved. To the extent that one lacks a history with a communication partner online (which can be overcome in pseudonymous exchanges), it is difficult to either establish a reputation or to build trust.

Several other more general drawbacks can briefly be mentioned. When interacting anonymously (online or otherwise), individuals may not get credit for their input/ideas, which runs counter to other values in our society. People may also be less influential and less identified with their organizations and work teams when exchanging messages anonymously (see Scott 1999; Scott & Easton 1996), both of which may limit effective decision-making. As another example, scholars have argued about the dangers of anonymous sources and leaks to the media by top government officials (Erickson & Fleuriet 1991).

In a broader sense, some legal experts have suggested that even though anonymity was necessary at earlier times in this country when people might not otherwise have voiced their views, this is no longer true in the information rich society of today (Wieland, 2001). This author further contends that the vast quantities of information online today demand that citizens better know who is speaking. All this represents just one more way in which the possible dangers of anonymous online communication are weighed against the potential benefits. We turn to those next.

Advantages

"The value of anonymous speech in society is regarded as a cornerstone of democratic government" (Lipinski 2002 95). Indeed, the right to communicate anonymously has generally been considered part of our first amendment right of free speech in the U.S.; i.e., the right to free speech includes the right to speak anonymously. Anonymity encourages free expression and the ability to voice opinions on unpopular ideas. This right is associated with a variety of benefits outlined below.

Marx (2001) offers several reasons as to why we need anonymous communication in general, though they apply to online anonymity as well. These include (a) facilitating the flow of communication on public issues without killing the messenger (e.g., tiplines, whistleblowing, unsigned political communication, etc.); (b) obtaining sensitive information (such as in research); (c) focusing attention on message content rather than status of source; (d) encouraging reporting,

sharing, etc. for stigmatized situations; (e) protecting one from subsequent contact (e.g., anonymous donors); (f) avoiding persecution and retaliation for one’s beliefs; (g) encouraging risk-taking, innovation, and experimentation; and (h) enhancing play/recreational interaction. I have also argued, anonymously of course (Anonymous 1998), that reasons we anonymize include having less relational status than the message receiver, needing to convey sensitive or suspect information, having low concerns about credibility and low need for credit, and when it is easy to do so (and one believes they will not be detected). Shedletsky and Aitken (2004) note that users may desire online anonymity in situations where they have been harassed/stalked, experienced previous embarrassment, wish to avoid recognition by others on multiple lists, want to voice controversial statements, or need to discuss personal/intimate topics. In all these instances, individuals are able to speak more freely (or even do so at all) because of the anonymity provided. As Barnes (1999) notes, “members of marginalized social groups can use anonymity to express their point of view without fear of social ostracism” (385).

To some extent, even the philosophical writing of Habermas (1989) seems to support the advantages of anonymity. Diane Saco (2002) asserts that “A defense of anonymity can be read out of Habermas’s theory of the public sphere, particularly with respect to the construction of a universalized public voice” (206). Additionally, Habermas also expresses a concern as to how anonymity can facilitate individual safety. Even more powerful is the relevance of Habermas when it comes to his writing about the ideal speech situation. For Habermas, truth is rational consensus, which depends on communicative freedom and responsibility being shared and asserted by relevant parties. Anonymous communication would be advantageous in helping to reach this ideal speech situation because anonymity (a) allows all parties must have an equal opportunity to speak, and (b) makes them more free to advance any kind of claim and free to question or challenge claims made by others.

Another set of advantages associated with anonymous speech center on democratic participation. Samoriski (2002) contends that “anonymous speech and free speech have become closely related and continue to play an important part in democratic movements” (p. 161). This happens by providing a means/role in informing and shaping opinion (with many experts agreeing that efforts to identify individuals may serve to chill expression (Samoriski 2002). Additionally, “anonymity makes political dissension safer” (Saco,2002 119) and advances democracy through secret assemblies (p. 193). She notes that the secret ballot box was to protect voters and that anonymity, rather than visibility, can be a stronger form of resistance.

Anonymous communication, especially as it may occur online, can provide several advantages in the workplace as well because it facilitates desired practices. Marx (1999), for example, suggests anonymity is a key element associated with whistleblowing, informational audits, anonymous gift giving, caller-id blocking, and review of applications without pictures and gender known. Anonymous (1998) discusses the level of anonymity in organizational flyers, upward appraisals, some forms of electronic mail, and some types of online workplace meetings. Scott and Rains (2002) specifically explore anonymous organizational communication, where they review existing work related to the function of anonymity in whistleblowing, feedback/appraisal, and use of electronic meeting tools. Without this anonymity, which often occurs through online tools, people will not blow the whistle as readily, give less honest feedback, feel more scared to report crime, have their input’s merit considered less, and perhaps not be evaluated or considered fairly in hiring and promotion decisions. Scott and Rains also report several findings regarding anonymity use and appropriateness. Specific to online anonymity, they note that anonymity is viewed as generally appropriate for organizational surveys/assessment and formal evaluation (either of which may be done electronically), but anonymous communication is only moderately appropriate for informal evaluations and use of certain technologies for anonymous messages. In other ways, because so many legal protections do not extend to most

workplaces, anonymity may provide a critical means for the expression of dissent, both internally through tools such as electronic suggestion boxes and externally through the variety of “suck” sites on the web (e.g., www.starbucked.com and www.gapsucks.org). As organizations are increasingly surveilled, monitored, and controlled (Botan 1996), the need for and benefits of anonymity are likely to increase.

As a more specific example, consider the workplace for many reading this essay. Institutions of higher learning are often considered both intellectually enlightened organizations and professional bureaucracies; yet, we use anonymity (online and offline) because we believe a variety of benefits accrue from such practices. In the classroom, anonymity may allow for freer expression about certain topics (especially when done online), focus teams on content rather than people, and promote generally more truthful communication in the students’ anonymous evaluations of instructors. In our research, we may guarantee research participants anonymity as a condition of participation, provide organizations and individuals with pseudonyms to protect their identity, and willingly submit our written work to what we often consider to be an anonymous review process. In academia we tend to value anonymity because of the objectivity, fairness, and legitimacy we attribute to it and the opportunities it provides for truthful communication about scholarship. There are other ways of doing reviews, for example, that are not blind or double blind—but there has been little interest in the communication field to adopt other procedures that remove the anonymity. In most of these cases, the anonymity in the process is accomplished largely through the use of online interactions.

Balance

The challenge then is how to provide for the benefits of online anonymity (which center largely on rights to free speech) without its drawbacks (which tend to focus heavily on issues of accountability). For some, the issue is perhaps better phrased as one of how to eliminate the dangers of online anonymity without completely removing those instances where anonymity serves a vital purpose. Balancing these competing interests, especially in an online environment, has fallen largely to the courts.

Online Anonymity on Trial

Given the array of arguments for and against the use of anonymity, especially in online contexts, it is perhaps not surprising that “courts across the country are grappling with the degree of protection to be accorded anonymous Internet speech” (Steinmeyer 2001 B8). Even though courts in the U.S. have historically recognized the importance and legality of anonymous speech as part of our basic first amendment rights to free speech (see Bowman 2001; Lipinski, 2002), some legal scholars now contend anonymous speech faces unprecedented challenges and attention (Wieland 2001).

The basis for law guiding anonymity online comes from legal opinions regarding offline anonymous speech. Although there is early evidence of court opinions (Lewis Publishing Co. v. Moran) upholding disclosure requirements in the early 1900s (Wieland 2001), almost any review of legal opinions in this area will reveal a clear shift in opinion for much of the 20th century. Most notably, a set of key cases (e.g., *Talley v. California*, *McIntyre v. Ohio Election Commission*, *Buckley v. American Constitutional Law Foundation*) heard by the Supreme Court reiterated the right to speak anonymously, primarily in terms of the right to distribute material anonymously. A very recent 2002 case (*Watchtower Bible v. Village of Stratton*) extended this right to door-to-door canvassers.

These and other rights were extended to the Internet in a series of cases, beginning with *Reno v. ACLU*. The court noted “the principles of free speech apply to the Internet and extend

to protect those who use the Internet as a ‘soapbox,’ an updated version of the eighteenth or nineteenth century ‘pamphleteer’” (see Lipinski 2002 77). However, the major free speech debate today concerning anonymity online centers on alleged cases of defamation and libel. These are better known as “cybersmearing” or “John Doe” cases. In almost every instance, a critic has anonymously sent a message (e.g., through a remailer, to a discussion board forum, in a chat room) that others have reacted to by bringing forth legal action that involves the desire to know the identity of the message source. Although courts have addressed defamation claims in a variety of contexts over many years, “the rise of the Internet has forced judges to grapple with novel legal arguments and design innovative remedies suited to this new medium” (O’Brien 2002 2745). Thus, the direction of court rulings in this area remains unclear, which continues to concern free speech advocates.

A number of individual cases seem to have recently resulted in victories for anonymous free speech online. As part of a larger securities fraud case against 2TheMart.com, that organization subpoenaed bulletin board operator InfoSpace Inc. requesting the identity of 23 anonymous Internet users who posted messages to their bulletin board—messages that 2TheMart.com claimed lowered their stock prices. InfoSpace emailed the users about the request, and one user known pseudonymously as “NoGuano” moved to quash the subpoena on grounds that this would “violate his First Amendment right to speak anonymously over the Internet” (Steinmeyer 2001,B8). For a variety of reasons (see Steinmeyer for detailed review), the court concluded that the disclosure of the anonymous speakers’ identities was unwarranted. Another case (In Re Subpoena Duces Tecum to America Online) involved a publicly traded company wanting to remain anonymous who subpoenaed AOL to reveal the names of several subscribers who had anonymously posted unflattering messages about the company—with the intent of then suing those individuals for libel and other claims. Eventually, the subscribers’ names were protected in an appeal under first amendment rights, but the courts did acknowledge that this right was not absolute and identity could be revealed if a plaintiff could show that the identity of the posters was central to the claim. Even as recently as September, 2004, New York District Judge Victor Marrero ruled against the FBI and in favor of an anonymous Internet service provider (Doe v. Ashcroft), stating “Every court that has addressed the issue has held that individual Internet subscribers have a right to engage in anonymous Internet speech, though anonymity may be trumped in a given case by other concerns” (cited in Hamblett 2004 1).

However, the most central case protecting the right to anonymous online communication was a 2001 case involving Dendrite International, Inc. v. Doe, No. 3. Under the screen name “xxpirr,” nine comments were posted to a Yahoo! bulletin board concerning alleged changes in accounting practices and efforts by the CEO to sell the company (see O’Brien 2002 for detailed analysis). Dendrite subpoenaed Yahoo! as the Internet service provider to reveal the identity of the poster. The courts denied the request, at least in part on the grounds that the plaintiff had not established a case of defamation based on the messages made and their impact. Furthermore, part of the ruling was a guideline that Internet service providers notify the anonymous posters about the subpoena and thus provide them with an opportunity to present opposition to the legal efforts underway. In his decision Judge Robert Fall wrote that the court must “balance the defendant’s First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant’s identity to allow the plaintiff to properly proceed” (cited in Bischof 2001a 18).

Despite these victories for anonymous online communication, legal scholars and free speech advocates remain cautious. As Ekstrand (2003) recently notes, these precedents are new and a handful of state court decisions “hardly guarantee the trend will continue, particularly with more cases pending” (425). Others have noted that the result of the 2TheMart.com case was driven more by legal miscues than principles of law (Steinmeyer 2001). In the AOL case cited

above, the initial trial court determined a compelling state interest in protecting companies “. . . from the potentially severe consequences that could easily flow from actionable communications on the information superhighway significantly outweigh [sic] the limited intrusion on the First Amendment rights of any innocent subscribers” (cited in Steinmeyer 2001 B8).

Additionally, Bischof (2001b) cites numerous instances where courts have forced Internet service providers, who may often prefer to cooperate rather than engage in a long legal battle with deep-pocketed corporate interests (see France & Carney 2000; O'Brien 2002), to reveal identities of posters before the underlying merit of the defamation case has been established. This has resulted in individuals having their identity released before they even knew legal actions were being taken against them. Apparently, this is still happening even after the guidelines in *Dendrite*. In a rather disturbing 2003 case (*Freedman v. AOL and others*) just ruled on in February 2004 (Dorsey 2004), AOL provided complete subscriber information to police detectives (made all the more curious since this was done on the basis of a faxed warrant that did not even contain a judge's signature). The once-anonymous poster had broken no laws but had engaged in political speech against the police commissioner, prompting efforts to uncover his identity. Most relevant to this essay, the claims against AOL were actually dismissed because of a forum selection clause in the plaintiff's AOL subscription information that essentially allowed them to release this data (however, the judge did rule against the police detectives). In another case, a message poster using the pseudonym “Aquacool_2000” sued Yahoo! for revealing his name to a company about whom Aquacool_2000 had made derogatory remarks. The complaint alleged that the company's claim was meritless and that Yahoo! had failed to notify him before releasing this information. This case was settled out of court—ironically with a confidentiality agreement that protected terms.

Indeed, the John Does Foundation, a nonprofit organization supporting anonymous online users who are sued, notes that of the hundreds of suits filed to unmask John Does, very few have gone to court (Ekstrand 2003). While that may seem beneficial to free speech advocates, it also makes it difficult to establish any sort of uniform standard when the merits of anonymous speech have not been fully litigated. When these cases do reach trial, there is a sense that the courts are treading very lightly because of the constitutional implications involved (Bischof 2001b). As to why some of these cases never reach trial, Law Professor Lyrissa Lidsky notes in some instances the plaintiff in these cases may not really be seeking damages—they simply want to know the identity of the message posters “solely for the purpose of intimidating their critics into silence and that's what makes them so dangerous” (cited in Bischof 2001b 35). Others have noted that the true identity of the individual is sought in order for persons or organizations to enact their own extra-judicial punishments. According to Ekstrand (2003), only about half the U.S. states have laws prohibiting these sorts of lawsuits, known as SLAPP (strategic lawsuits against public participation) suits.

The events of September 11, 2001, may well have contributed to a shift away from online anonymity protections as well. Wieland (2001) contends that Internet service providers are now readily working with government in the interest of national security and several anonymous remailer sites have been shut down since that time. Furthermore, the courts have broadened what they may accept as compelling state reasons in cases seeking to identify anonymous communicators, which further limits protections for anonymous online communication. Even considering the recent *Doe v. Ashcroft* case mentioned previously, an examination of existing cases seems to confirm what legal experts and free speech proponents have concluded: it is difficult to determine the direction of the courts when it comes to the protection of anonymous online speech. It does not appear that a landmark decision in this area is yet in place, and when this topic has actually been litigated in courtrooms across this country, the results have been

rather mixed. As communication scholars, we can offer some critiques of this situation and guidelines that reach beyond legal views in an effort to address this complicated topic.

Critiques and Communicative Recommendations

Rather than wait and hope for better laws and clearer legal standards that provide adequate protection for online anonymous communication, several critiques and recommendations are offered for work in this area. No one, including myself, is proposing anything that would allow for slander or defamation via anonymous online communication; free speech rights do not extend to such abuses and not having substantial checks on online libel might render online speech meaningless in many ways. But, the solution cannot be to ban online speech because of the potential harms or in the interest of national security. The balance that is sought is one that clearly protects free speech, including anonymous speech online as a first amendment right, unless compelling and substantiated evidence clearly suggests the need to reveal one's identity.

A very useful starting point emerges from the Dendrite guidelines. Relying on earlier guidelines from a case on anonymous cybersquatting, the court suggested the following four-part test to be employed in cases involving subpoenas requesting the identity of anonymous communicators (see O'Brien 2002 for details): (a) the plaintiff should make efforts to notify the anonymous posters that they are subject to subpoena, and withhold action until the defendants have reasonable opportunity to respond; (b) the plaintiff should identify the exact statements made by the anonymous poster that constitute actionable speech; (c) the plaintiff must present a *prima facie* case; and (d) the court must balance the necessity of disclosing the defendant's identity with regard to his/her first amendment rights relative to allowing the plaintiff to proceed with the case. Existing analyses from legal scholars and free speech proponents generally support such guidelines (see Chiger 2002; O'Brien 2002). In extending these guidelines, both Chiger and O'Brien note that the online context in which these comments take place must be considered—because the informal and uninhibited nature of the chat room or message board area really should be considered separately from the newspaper editorial page or a television broadcast on a major news network.

The discussion of differences between channel/technology also demands that efforts to consider anonymous online communication consider the array of tools that may permit such interaction. The focus of current attention has been heavily geared toward online discussion/message boards, with some additional attention to online websites, chatrooms, and remailers. Though an obvious starting point, it does not even begin to address the range of technologies that could be used for anonymous online speech. Simply forwarding emails and stripping off identifying information from previous senders begins to make for anonymous speech. Even in synchronous chat rooms, instant messaging sessions, or during text-messaging, individuals have (and will increasingly have) the ability to copy, cut, paste, and forward messages to environments that reach more and more people. Voice files or Internet telephony raise a whole additional set of issues—and may still constitute anonymous communication when the identity of the sender is unknown (and the voice unrecognized or disguised). It is unclear if existing laws and guidelines cover other forms of mediated communication when it comes to free speech rights, especially when other forms do not share some of the same characteristics of the text-based asynchronous message boards. In possibly parallel legal work related to online privacy, fundamentally different laws are generally applied to recorded (asynchronous) vs. live (synchronous) interactions (see Martucci & Place 1998). And, even though technology is increasingly available to gather Internet traffic data and implement sophisticated data retention programs (which may themselves violate first amendment rights (see Crump 2003), individuals have technological solutions as well to

preserve their anonymity—including the use of public computers, identity-masking programs, and anonymizing services (though these can vary vastly in the degree of anonymity they ultimately provide). In short, the Internet is not a singular environment—and the types of anonymity made possible and the degree of protections provided may well vary depending on the specific application/tool used.

Existing models/frameworks for anonymity may also be instructive. Marx (1999), for example, suggests that there are seven different types of identity knowledge that vary in degree of identifiability. These range from legal name, through various forms of pseudonyms, to broader social categories. Legal efforts seem focused entirely on legal name, though issues related to locatability and reachability (his second category) are often part of the identity-uncovering and identity-protecting efforts as well. Since much of the anonymous communication on the Internet is actually pseudonymous, there is a great deal of identifiability in place already. Is it possible that a pseudonym (as an extension of an offline self) can be sued or criminally charged in ways that meet others' needs but still protect the identity of the communicator? Little serious attention has been given to such issues to date. Anonymous's (1998) model of communicator anonymity may also be relevant in several ways. First, a determination of the motivations/reasons one has to communicate online anonymously may be informative when courts are evaluating the importance of free speech relative to someone else's rights. If lowered status or concerns about credibility and retribution are the motivation, that may carry more weight than motivations done simply because it was easy to do so or fun. Relatedly, the motivations of the party trying to overcome the anonymity of the message sender should be considered, as certain motivations may again carry more weight than others. Finally, the model suggests the importance of anonymity or identification efforts over time. If one's identity is revealed even once, we should understand that action may deter future uses of anonymous communication—effectively chilling speech well beyond any intended frame.

Another critique and focus for future work centers on reading/hearing anonymous communication. Although first amendment rights generally include rights to receive and read communication also, rarely has this been considered in terms of its extension to freely reading/hearing anonymous online speech. Froomkin (1999) notes that even though logic would suggest such an extension, there is "no directly relevant decision of the Supreme Court to support this assertion" (122). Yet, as Crump (2003) notes, since so much online activity centers on reading web pages (and people generally spend more time reading online versus sending anyway), this is a vital issue to consider. Furthermore, the advantages of anonymous speech depend almost entirely on others' ability to view such material—and doing so anonymously may be essential at times. In an age of increased Internet monitoring, the same tools that identify anonymous message senders can also tell us who has received (anonymously or otherwise) such messages. In the dialogue and exchange of ideas that depends heavily on sending/speaking, reading/hearing and responding, legislation and legal interpretations that cover the entire anonymous communication process are needed.

An extremely important set of players in this anonymity-accountability debate are the intermediaries involved. For the most part, this has meant the Internet service provider organizations that maintain information on their otherwise pseudonymous posters; however, intermediaries could include organizations providing other tools (e.g., anonymizer.com), neutral third-party organizations, or even private individuals operating certain anonymizing services. Even though laws have reduced the extent to which these intermediaries are liable for users' messages, most Internet service providers still do little to protect user anonymity. Ironically perhaps, the growth of suits requesting user identity information from these providers has moved them toward "a critical new role as potential defenders of anonymous speech" (Ekstrand 2003 426). Ekstrand argues that the time may be appropriate for these service providers to step forward in defense

of those subscribers who wish to criticize anonymously. Yet, as the recent case involving *Freedman vs. AOL* (and others) illustrates, even these service providers moving toward such roles are clearly still not there on a consistent basis. This suggests that other types of intermediaries—as long as they are not government based—may be a more viable means of protecting user identities until compelling reasons are provided otherwise. Whoever the intermediaries are, they must make very clear and communicate regularly their institutional policies on disclosure of identifying information.

A discussion of institutional policy brings us to consideration of the organizations in which most of us work as another site for anonymous organizational communication. My own formal and informal efforts to examine anonymity in this area suggest that most organizations do not think much about anonymity—and if they do, it typically goes against desired cultural norms favoring openness and directness. Yet, Lipinski (2002) suggests that institutional policies that reflect legal precedents “can help preserve a spirit of free speech, yet allow for the continued functioning of the organization” (p. 108). Thus, policies should be established and communicated in the workplace. Tools that provide for anonymous input should be made available for those situations where people may need them to speak openly. If organizations adopt an attitude of valuing members’ rights to anonymous communication and viewing anonymous input as an important form of feedback—often times more honest feedback—there are almost certainly more rewards than potential problems to be gained. Such considerations are especially important to the extent that so many individual protections from the government do not extend to the nongovernmental workplace. One final area relevant to organizations concerns the external message boards or “suck sites” that exist. As opposed to constant legal efforts to shut down such sites, many organizations would be well advised to monitor them to gain feedback about how they might improve operations. Another option is to use these and other interactive media to post an organization’s perspective or to provide an alternative viewpoint on the subject.

Perhaps the most important observation and need from all this concerns education of users. Even with the rapid growth of technology, the legal process takes time and it is already clear that there are rather mixed views and competing forces at work here that will likely prohibit an immediate solution to the issues surrounding anonymous online communication. In the meantime, users should be educated in two broad areas. First, “people have a false sense of security about technology and place more trust in it than is warranted. In this way, they are blind to the fact that there exists no such thing as guaranteed anonymity or guaranteed security. Almost anything one does to conceal one’s identity can be defeated” (*Teich et al* 1999 75). Education in our classrooms, in our workplaces, in various online communities, and by some of the nonprofit groups that deal with this and related issues (e.g., Electronic Privacy Information Center, John Does Foundation) are key first steps. People need to understand how they are only partially anonymous, and that decisions to communicate this way must be informed of that fact. But at the same time, people should be informed about the technological tools that do provide even this partial anonymity so that those in need are aware that such options exist. Relatedly, these same sources of information can help better educate users about current laws, about when others might be forced to reveal their identities, and when their identities will be protected. Second, we need to be educated as consumers of anonymous information. Again, understanding the motivations as to why something may have been communicated anonymously or pseudonymously may help us to evaluate the credibility of such messages even in the absence of a known source. Relatedly, users in anonymous environments can sometimes manipulate the message so as to make it seem widely supported among a community of users (e.g., having multiple pseudonyms belonging to a single person support an idea) or to play with people’s minds by posting frivolous ideas. Although similar behaviors occur offline, they may be even harder to

detect in anonymous online communication. Teaching people to be skeptical without rejecting all anonymous messages provides a starting point.

Of course, numerous other challenges and directions emerge here as well. In one sense, the U.S. can pass all sorts of laws on this issue—but the international access to the Internet and the variety of legal standards and norms that exist globally may make such laws increasingly less forceful over time. Additionally, in one of the more ironic cases involving anonymous speech (*Wasson v. Agrella*; see Hereford 2000), a dismissed employee accused of sending anonymous letters to a college president was not granted first amendment protections because she denied ever sending the messages—meaning that this government employee had to own up to the anonymous speech before such speech could be protected (under the idea that you can't be protected for something you did not say; for related discussion about rights of attribution (see Lemley 1999). These two examples, and many others, point to the numerous challenges still ahead for anonymous online communication.

In closing, even as communication and speech scholars, some of us are hesitant about the use of anonymity. Somehow, it seems secretive and indirect, and a substitute for how communication should really take place. And, ideally perhaps, there would be no need for anonymous communication because we would live in a world where people really could freely express their ideas without any fear of attack or ridicule (or worse). But, at the turn of the 21st century, we are perhaps no more living in that ideal world than was Publius over 200 years ago. In many ways, the growth of various new communication technologies facilitating both the appropriate and inappropriate use of anonymous speech makes today's world even more complicated in this regard. As a result, it is important that we not bemoan the anonymous speaker's rapidly approaching death, but instead celebrate the potential for its resurrection in the online chatrooms, bulletin boards, and other virtual environments we use for communication today.

Endnotes

1. Anonymous remailers, which may be unfamiliar to many, remove all the information in the address header to make the message sender anonymous to message receivers. By sending messages through numerous remailers (across various networks and servers), the messages can become largely untraceable (see Barnes 1999). Anonymous web surfing allows one to go online without websites, governments, or others being able to track one's activities while in cyberspace. The most sophisticated systems are based on onion routing, where messages are relayed via a distributed network of random servers; furthermore, messages in this network are unwrapped by an encryption key at each server that peels off one layer to obtain further instructions (Harrison 2004).

Works Cited

- Anonymous (1998). "To reveal or not to reveal: A theoretical model of anonymous communication." *Communication Theory*, 8, 381-407.
- Barnes, S. B. (1999). "Ethical issues for a virtual self." In S. J. Drucker & G. Gumpert (Eds.), *Real law @ virtual space*. Cresskill, NJ: Hampton. 371-398
- Barnes, S. B. (2003). *Computer-mediated communication: Human-to-human communication across the Internet*. Boston: Allyn & Bacon.
- Bischof, D. (2001a). "Appeals court affirms right to anonymity online." *News Media & The Law*, 25(3), 18.
- Bischof, D. (2001b). "Through accusations of defamation, companies are starting to unmask anonymous online critics." *News Media & The Law*, 25(1), 35-35.
- Botan, C. (1996). "Communication work and electronic surveillance: A model for predicting panoptic effects." *Communication Monographs*, 63, 293-313.
- Bowman, L. M. (2001, August 13). "Online anonymity wins again." Retrieved August 16, 2001, from <http://news.cnet.com>.
- Chiger, S. J. (2002). "Cybersmear: Telecommunication's 200-year-old riddle." *Communications and the Law*, 24(2), 49-67.

- Crump, C. (2003). “Data retention: Privacy, anonymity, and accountability online.” *Stanford Law Review*, 56, 191-229.
- Dorsey, P. C. (2004, February 7). “*Ruling on plaintiff’s motion for partial summary judgment.*” Retrieved February 15, 2004, from http://www.ctd.uscourts.gov/Opinions/020403.PCD.Freedman_partialSJ.pdf.
- Ekstrand, V. S. (2003). “Unmasking Jane and John Doe: Online anonymity and the first amendment.” *Communication Law & Policy*, 8, 405-427.
- Erickson, K. V., & Fleuriot, C. A. (1991). “Presidential anonymity: Rhetorical identity management and the mystification of political reality.” *Communication Quarterly*, 39, 272-289.
- France, M., & Carney, D. (2000, February 28). “Free speech on the net? Not quite.” *Business Week*, 93-94.
- Froomkin, A. M. (1999). “Legal issues in anonymity and pseudonymity.” *Information, Computers, & Technology*, 14, 79-88.
- Godin, S. (2001, October). “In my humble opinion.” *Fast Company*, 51, 86-88.
- Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* (Trans. T. Burger). Cambridge, MA: MIT Press.
- Hamblett, M. (2004, September 30). “Judge disallows secret FBI demand for customer data.” *New York Law Journal*, p. 1.
- Harrison, A. (2004, August 5). “Onion routing averts prying eyes.” Retrieved February 5, 2005, from <http://www.wired.com/news/privacy/0,1848,64464,00.html>.
- Hereford, L. (2000). “California court rejects professor’s ‘anonymous’ free speech.” *Community College Week*, 12(17), 8-9.
- Johnson, D. G. (1997). Ethics online. *Communications of the ACM*, 40(1), 60-65.
- Kling, R., Lee Y., Teich, A., & Frankel, M. S. (1999). “Assessing anonymous communication on the Internet: Policy deliberations.” *Information Society*, 15, 79-90.
- Lemley, M. A. (1999). “Rights of attribution and integrity in online communication.” In S. J. Drucker & G. Gumpert (Eds.), *Real law @ virtual space* (pp. 251-266). Cresskill, NJ: Hampton.
- Lipinski, T. A. (2002). “To speak or not to speak: Developing legal standards for anonymous speech on the Internet.” *Informing Science*, 5, 95-111.
- Martucci, W. C., & Place, J. M. (1998). “Privacy rights and employee communication in the workplace.” *Employment Relations Today*, 25, 109-120.
- Marx, G. T. (1999). “What’s in a name? Some reflections on the sociology of anonymity.” *Information Society*, 15, 99-112.
- Marx, G. T. (2001). “Identity and anonymity: Some conceptual distinctions and issues for research.” In J. Caplan & J. Torpey (Eds.), *Documenting individual identity: The development of state practices in the modern world*. Princeton, NJ: Princeton University. 311-327
- Nissenbaum, H. (2003). “Securing trust online: Wisdom or oxymoron?” In B. E. Kolko (Ed.), *Virtual publics: Policy and community in an electronic age* (pp. 134-171). New York: Columbia University.
- O’Brien, J. (2002). “Putting a face to a (screen)name: The first amendment implications of compelling ISPs to reveal the identities of anonymous Internet speakers in online defamation cases.” *Fordham Law Review*, 70, 2745-2776.
- O’Sullivan, P. B., & Flanagan, A. J. (2003). “Reconceptualizing ‘flaming’ and other problematic messages.” *New Media & Society*, 5, 69-94.
- Saco, D. (2002). “*Cybering democracy: Public space and the Internet.*” Minneapolis, MN: University of Minnesota.
- Samoriski, J. (2002). *Issues in cyberspace: Communication, technology, law, and society on the Internet frontier*. Boston: Allyn & Bacon.
- Scott, C. R. (1999). “The impact of physical and discursive anonymity on group members’ multiple identifications during computer-supported decision making.” *Western Journal of Communication*, 63, 456-487.
- Scott, C. R., & Easton, A. (1996). “Examining equality of influence in group decision support system interaction.” *Small Group Research*, 27, 360-382.
- Scott, C. R., & Rains, S. A. (2002, November). *Anonymous communication in organizations: Assessing appropriateness, use, and adequacy*. Paper presented to the annual convention of the National Communication Association, New Orleans, LA.
- Shedletsky, L. J., & Aitken, J. E. (2004). *Human communication on the Internet*. Boston: Pearson.
- Spears, R., & Lea, M. (1994). Panacea or panopticon? The hidden power in computer-mediated communication.” *Communication Research*, 21, 427-459.
- Stein, E. (2003). “eers anonymous: Lesbians, gay men, free speech, and cyberspace.” *Harvard Civil Rights-Civil Liberties Law Review*, 38, 159-203.
- Steinmeyer, P. A. (2001). “Anonymous speech.” *The National Law Journal*, 23, B8.
- Teich, A., Frankel, M. S., Kling, R., & Lee Y. (1999). “Anonymous communication policies for the Internet: Results and recommendations of the AAAS conference.” *Information Society*, 15, 71-77.

- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.
- Wieland, J. B. (2001). "Death of Publius: Toward a world without anonymous speech." *Journal of Law & Politics*, 17, 589-629.
- Williams, R. (1988). "Reflections on anonymity." *Perceptual and Motor Skills*, 67, 763-766.