To Speak or Not to Speak: Developing Legal Standards for Anonymous Speech on the Internet

Tomas A. Lipinski
Center for Information Policy Research,
University of Wisconsin, Milwaukee, WI, USA

tlipinsk@csd.uwm.edu

Abstract

This paper explores recent developments in the regulation of Internet speech, in specific, injurious or defamatory speech and the impact such speech has on the rights of anonymous speakers to remain anonymous as opposed to having their identity revealed to plaintiffs or other third parties. The paper proceeds in four sections. First, a brief history of the legal attempts to regulate defamatory Internet speech in the United States is presented. As discussed below this regulation has altered the traditional legal paradigm of responsibility and as a result creates potential problems for the future of anonymous speech on the Internet. As a result plaintiffs are no longer pursuing litigation against service providers but taking their dispute directly to the anonymous speaker. Second, several cases have arisen in the United States where plaintiffs have requested that the identity of an anonymous Internet speaker be revealed. These cases are surveyed. Third, the cases are analyzed in order to determine the factors that courts require to be present before the identity of an anonymous speaker will be revealed. The release is typically accomplished by the enforcement of a discovery subpoena instigated by the party seeking the identity of the anonymous speaker. The factors courts have used are as follows: jurisdiction, good faith (both internal and external), necessity (basic and sometimes absolute), and at times proprietary interest. Finally, these factors are applied in three scenarios—e-commerce, education, and employment—to guide institutions when adopting policies that regulate when the identity of an anonymous speaker—a customer, a student or an employee—would be released as part of an internal initiative, but would nonetheless be consistent with developing legal standards.

Keywords: Anonymous Speech, Internet, Legal Standards and Compliance, Institutional Policies and Decision-Making

Introduction

The value of anonymous speech in society is regarded as a cornerstone of democratic government. This position also applies to Internet speech. However, recent legal developments in the Untied States, pressure actors harmed by such speech to seek recourse from the actual speaker, as opposed to an intermediate actor such as the technological equivalent of traditional publisher, the online service provider. This pressure means that in increasing numbers the identity of those anonymous speakers will be sought. Several courts have dealt with the factors under which a legal request in the form of a subpoena to obtain the identity of an anonymous speaker will be granted. These factors are identified and discussed. As a result several predictors can be established that indicate the circumstances under which future subpoenas will succeed. These predictors can also be used to draft organizational policies regarding anonymous speech that would conform to legal precedent thus making anonymous speakers—those specific to the organization as well as anonymous speakers in general—aware of the circumstance under which their anonymity might be breeched. The purpose of this iteration is to indicate how internal institutional policy formation or decision-making can be undertaken consistent with the principles of the developing law. This in turn serves to make the circumstances surrounding the expression of anonymous speech within the organization legally compliant.

Background: Defamation

In general, an action for defamation requires a showing that the plaintiff has been exposed to hatred, contempt or ridicule, or that it causes a person to be shunned or avoided or otherwise injures his or her standing in the community (Keeton and Prosser, 1984, 773). The four elements of a claim for defamation are: a false and defamatory statement, that is published to one or more third parties without privilege, by a publisher who is at least negligent in communicating the information, and that results in presumed or actual damage (Street and Grant, 2001, §6.02, at 6-3). Typically, those who act as a publisher or re-publisher (Restatement of Torts §578) of defamatory material are also liable with the speaker or writer of the defamation. The law imposes this burden on the intermediary as publisher for several reasons. First, as the publisher benefits economically from the publication, so it should also share in its social cost. Second the publisher

may have resources or be in the most efficient position to intercede in preventing the harm, i.e., it can halt or cease publication of the harmful material. Finally, imposing liability of publishers is a form of risk allocation; if an individual author would carry the sole burden of responsibility for defamatory harms, future speakers (authors) might be less willing to speak (write), and future speech might be chilled. In this way, publishers offset the cost of a single harm against the profits received from numerous other authors' successes.

Another category of intermediary is known as a distributor. However, distributors are not liable, unless the distributor knows or has reason to know of the defamatory nature of the publication it distributes, through sales, rentals, loans, etc. The law draws a distinction between a true publisher or re-publisher for that matter, of a defamatory statement and a mere distributor of a defamatory statement. "Examples of such distributors include libraries, bookstores, and news vendors" (Talbot, 1999, §10.4, at 10-4). Another category of intermediary is the conduit or the common carrier. Common carriers, a telecommunication service provider such as a telephone company, are generally not liable for defamatory messages sent by third parties over its systems, as a common carrier is neither a publisher nor distributor. However, in cyberspace parties acting as mere intermediaries (distributor or common carrier), traditionally secure from such actions, may be exposed to liability given the unsettled nature of the Internet legal environment. Technological advances often blur the legal distinction between the intermediary (distributor and generally not liable), and the information creator and producer (author or publisher, generally liable). This operates to compound the legal problematic. Electronic publishing is a good case in point (Counts and Martin, 1996; Talbot, 1999, §10.15). A web site operator that cuts, pastes, grafts or otherwise edits content onto its web site has arguably moved beyond the function of a mere conduit or distributor and is now acting more like a traditional publisher or editor. The ability to achieve instantaneous and prolonged distribution of a work in cyberspace may also confuse the line between distributor (no liability unless know or reason to know standard is met) and true publisher. Unlike some jurisdictions, the United States generally follows a single publication rule, i.e., publish 20,000 copies of a book containing defamatory content and courts will view the pressing of a particular copy of the book and its subsequent sale (distribution) as a single publication, not 20,000 distributions, i.e., 20,000 separate acts of defamation. The single publication rule has been extended to the Internet; while the act of making defamatory material available over the Internet might constitute a "publication," in the absence of some alteration or change in form, its continued availability on the Internet does not constitute a republication each time it is accessed, read, or even forwarded, that would start the statute of limitations running anew with each interaction. (*Firth v. State of New York*; *Van Buskirk v. The New York Times Co.*) It should also be observed that defamation in other jurisdictions, especially those inheriting from the English legal tradition, may not distinguish between the author and publisher, and distributor, or provide only limited protection to distributors. (Lipinski, Buchanan, and Britz, 2002) It is the strong protection that speech receives under the U.S. Constitution that accounts for the application of differing legal standards and often contributes to opposite outcomes in similar defamation suits in the United States, versus for example, the United Kingdom.

Even within the United States, the developing law is often inconsistent, with one infamous decision holding that an online service provider (thought to be at most a mere conduit or distributor) liable for the defamatory postings of third parties on its system (*Stratton Oakmont, Inc. v. Prodigy Services Co.)*. In *Stratton Oakmont*, the court was persuaded by evidence that suggested the online service provider Prodigy acted more like a publisher than a distributor when it appointed a board moderator, used filtering software to regulate content and held itself out as a family oriented (another indication of content control) network access provider. At the same time several legislative initiatives in the United States concerned with regulating the content of information available to children on the Internet and in other media have appeared, such as the V-Chip legislation (officially known as the Parental Choice in Television Programming Act, codified at 47 U.S.C. §303), the Children's Online Protection Act (codified at 47 U.S.C. §231), regulating access by minors to commercial pornography on the World Wide Web, and the Children's Internet Protection Act requiring filtering software in qualifying schools and libraries (adding 20 U.S.C. §3601, and amending 20 U.S.C. §9143 and 47 U.S.C. §254). In conjunction with the V-Chip initiative Congress added 47 U.S.C. §230(c) to the federal communication law offering "immunity" to online service providers (both provisions were part of the Telecommunications Act of 1996). Congress sought, in section 230(c), to ensure that online service providers, when attempting to promote the national policy of protecting children and others from obscene or indecent material online, would not be viewed as the editor of that content (at least when their efforts at protection, alteration, modification, etc. failed) and be placed into the "publisher" category of actors for purposes of liability assessment. This new section of the federal communication law overrules the decision in *Stratton Oakmont*. (Conference Report, 1996, 194)

Developments: Section 230 and Recent Precedent

In passing Section 230 Congress commented that "[t]hese protections apply to all interactive computer services [ICS], as defined in new subsection 230(f)(2), including non-subscriber systems such as those operated by many businesses for employee use" (Conference Report, 1996, 194). Section 230(f)(2) defines an ICS as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." Subsequent case law interpreted the Section 230 "protections" as offering complete immunity for all harms associated with third party content creation on the Internet (*Zeran v. America Online, Inc.*: defamation; *Blumenthal v. Drudge*: defamation; *Ben Ezra, Einstein & Co. v. American Online, Inc.*: defamation and negligence; *Doe v. American Online, Inc.*: negligence, *Stoner v. eBay. Inc.*: business law; *Kathleen R. v. City of Livermore*: nuisance). Although these developments have been criticized (Wiener, 1999; Ballon, 1997; Kane, 1999; Spencer, 2000), expansion of Section 230 immunity continues, even to public libraries in contexts other than defamation. In, *Kathleen R. v. City of Livermore*, the court granted a defendant's motion for summary judgment when the library patron-plaintiff claimed that a lack of filtering software on Internet access terminals caused her child to be exposed to harmful materials. The court relied in part on Section 230 in providing tort immunity from harmful material that the library, as a conduit, made accessible through its connection to the Internet, i.e., the library did not create the content nor provide a link, nor was the mere provision of Internet access deemed a publication, thus no publisher, or intermediary liability.

Legal precedent establishes that those who act in the capacity of re-publishers of defamatory material and not as mere distributors are equally liable for the defamatory material as is the initial publisher. The question here is whether there exist circumstances whereby the online service provider, bulletin board operator, etc. would move out of its traditional role as mere distributor and be placed in the position of a re-publisher or creator of defamatory or otherwise harmful content. According to Street those information or service providers that "claim to exercise editorial control or do in fact exercise editorial control . . . are likely to be treated as publishers and held liable for defamation in the materials they publish" (Street, 2000, §6-2(b), at 625-626, see also, Zuckman, Et al., 1999, Section 5.10, at 612).

It could be argued that through its web site, through linking, cutting and pasting or uploading content the information organization or educational institution has moved beyond the mere provision of online service (conduit). Initially, Section 230 immunity was targeted at those Internet or Online Service Providers (OSP) that attempt to filter or control the access of harmful content on their systems, whether through manual editing as in *Stratton Oakmont* or through technological means such as software filters contemplated by Section 230(c)(2)(b). The new law specifically includes a library or educational institution within the definition of OSP or "Internet or other Interactive Computer Services." See, 47 U.S.C. §230(f). Section 230(c) provides "immunity" by stating that in these situations the OSP or Interactive Computer Services (to use the statutory phrasing) Provider (ICSP), should not be treated as a creator or editor of content but as a mere distributor. As long as the content comes from a third party, regardless of how it is incorporated into an institutional web site, courts have consistently concluded that the institution as service provider will be immune from liability for defamation and for other torts as well. As a result, plaintiffs seeking redress have only one alternative left: pursue remedy against the original speaker or tortfeasor. But what if the harm was committed online, and the tortfeasor acted anonymously?

Anonymous Internet Speech: Background

In United States law, the right to free speech is a cornerstone of constitutional jurisprudence. Concomitant with the right to speak is the right to speak anonymously. There is historical as well as judicial precedent to support this conclusion. (See Table 1.) In several cases, *Talley v. California*, *McIntyre. v. Ohio Election Commission* and *Buckley v. American Constitutional Law Foundation*, the right to speak anonymously has been reiterated by the Supreme Court, in specific, the right to distribute material anonymously without any personal identification. However, it must be observed that previous Supreme Court precedent involved political speech (handbills, campaign literature, petition drives). Nonetheless, the Court in *Reno v. ACLU* observed that 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." The recent 2002 Supreme Court opinion in *Watchtower Bible and Tract Society of New York v. Village of Stratton*, arguably expands that protection to an array of speech, including political and religious information that door-to-door canvassers, the target of the regulation in that case, might desire to distribute. Moreover, recent lower court precedent specifically extends this right of anonymity to the Internet (*In re Subpoena Duces Tecum to American Online, Inc.*; *Doe v. 2TheMart.com, Inc*.) The point should be made that the First Amendment, in a strict legal sense, has no application in disputes among private parties. However, the concept of free speech and all of it accoutrements permeates

American social fabric including the Internet and courts often adopt the legal nomenclature and rationale of these constitutional issues even when adjudicating non-constitutional issues.

Case	Subject of Anonymous Speech	Rationale*
N.A.A.C.P. v. Alabama, 357 U.S. 449 (1958).	The Court overturned a finding of contempt against the NAACP for its refusal to turn over its membership lists, after being ordered to do so by an Alabama state court judge.	I
Talley v. California, 362 U.S. 60 (1960).	Invalidating a California statute prohibiting the distribution of "any handbill in any place under any circumstances" that did not contain the name and address of the person who prepared it. Identification and fear of reprisal might deter "perfectly peaceful discussions of public matters of importance." 363 U.S. at 65.	I II II?
McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).	Overturning an Ohio law that prohibited the distribution of campaign literature that did not contain the name and address of the person issuing the literature. "[U]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent. Anonymity is a shield from the tyranny of the majority." 514 U.S. at 357.	I II
Buckley v. American Constitutional Law Foundation, 525 U.S. 182 (1999).	Invalidating, on First Amendment grounds, a Colorado statute that required initiative petition circulators to wear identification badges.	I II
Watchtower Bible and Tract Society of New York v. Village of Stratton, 122 S. Ct. 2080 (2002).	Ohio village ordinance requiring door-to-door canvassing unless a "Solicitation Permit" is first obtained. The canvasser must then carry and display upon request the permit containing identity and organizational affiliation data. These requirements are unconstitutional.	I II**
Reno v. A.C.L.U., 521 U.S. 844 (1997).	Internet: "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of web pages, mail exploders and newsgroups, the same individual can become a pamphleteer." 521 U.S. at 870. First Amendment protections extend to speech via the Internet.	I II? III
In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir.26 (Cir. Ct. Fairfax Cnty. 2000). 52 Va. Cir. at 32.	"It cannot be seriously questioned that those who utilize the 'chat rooms' and 'message boards' of AOL do so with an expectation that the anonymity of their postings and communications generally will be protected." "If AOL did not uphold the confidentiality of its subscribers, as it has contracted to do, absent extraordinary circumstances, [footnote omitted] one could reasonably predict that AOL subscribers would look to AOL's competitors for anonymity. As such, the subpoena duces tecum at issue potentially could have an oppressive effect on AOL." 52 Va. Cir. at 32. "To fail to recognize that the First Amendment right to speak anonymously should be extended to communications on the Internet would require this Court to ignore either United States Supreme Court precedent or the realities of speech in the twenty-first century." 52 Va. Cir. at 34. "This Court declines to do either and holds that the right to communicate anonymously on the Internet falls within the scope of the First Amendment's protections." 52 Va. Cir. at 34.	I II*** III IV III III
Doe v. 2TheMart.com, *Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001).	"A component of the First Amendment is the right to speak with anonymity." 140 F. Supp. 2d at 1092. "The right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas." 140 F. Supp 2d at 1092.	II**** II**** III

Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. Super. 2001).	"[C]ourts must decide such applications by striking a balance between the First Amendment right of an individual to speak anonymously and the right of a company to protect its proprietary interest in the pursuit of claims based on actionable conduct by the ISP message board user." 775 A.2d at 776, citing Dendrite International, Inc. v. John Doe No. 3, 775 A.2d 756 (N.J. Super. 2001).	I III? IV
Dendrite International, Inc. v. John Doe No. 3, 775 A.2d 756 (N.J. Super. 2001).	"The trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants." 774 A.2d at 760.	I III IV

Notes:

*Four rationales for the application of the right to speak anonymously on the Internet appear in the case law:

(I) applicable precedent regarding free speech,

(II) historical tradition of protecting anonymous speech,

(III) reality of speech in the 21st century and the extension of free speech and anonymous speech concepts to the Internet, and

(IV) promotion of competition in the Internet environment (anonymity, like privacy, is becoming a salable commodity).

**"It is offensive—not only to the values protected by the First Amendment, but to the very notion of a free society—that in the context of everyday public discourse a citizen must first inform the government of her desire to speak to her neighbors and them obtain a permit to do so. Even if the issuance of permits by the mayor's office is a ministerial task that is performed promptly and at no cost to the applicant, a law requiring a permit to engage in such speech constitutes a dramatic departure from our national heritage and constitutional tradition." 122 S. Ct. 2080, 2002 U.S. LEXIS 442, at *28.

***"Inherent in the panoply of protections afforded by the First Amendment is the right to speak anonymously in diverse contexts. This right arises from a long tradition of American advocates speaking anonymously through pseudonyms, such as James Madison, Alexander Hamilton, and John Jay, who authored the Federalist Papers but signed them only as 'Publius.'" 52 Va. Cir. at 33.

****"The right to speak anonymously was of fundamental importance to the establishment of our Constitution. Throughout the revolutionary and early federal period in American history, anonymous speech and the use of pseudonyms were powerful tools of political debate. The Federalist Papers (authored by Madison, Hamilton, and Jay) were written anonymously under the name 'Publius.' The anti-federalists responded with anonymous articles of their own, authored by 'Cato' and 'Brutus,' among others. See generally *McIntyre*, 514 U.S. at 341-42. Anonymous speech is a great tradition that is woven into the fabric of this nation's history." 140 F. Supp. 2d 1088, 1092.

Table 1. Development of the Right to Speak Anonymously

Anonymous Internet Speech: Recent Precedent

Several cases involving anonymous speech on the Internet have arisen. Moreover, as all intermediaries such as a school, library or commercial provider of an interactive computer service, are conceivably immune from tort liability under section 230, whether acting in the capacity of a publisher or distributor, individuals who are harmed by Internet speech or other tortfeasance have but one recourse and that recourse is to seek remedy from the actual speaker or creator of the harmful content. As a result and as discussed below, the developing precedent involves categories of harms beyond defamatory speech alone, yet all target the anonymous speaker or poster of the message.

When speakers or creators choose to speak under the veil of anonymity, those harmed have sought to compel through legal process (a subpoena) the divulgation of the identity of the anonymous speaker. The identity of the anonymous speaker is necessary before the legal action against the perpetrator (the speaker or creator) of the harm can continue. Thus courts are placed in the unenviable but inevitable position of deciding when a person's right to proper redress by the courts (i.e., exercising one's right to obtain his or her day in court) outweighs another person's right to speak anonymously. (See Tables 2a-d for a detailed summary of the issues involved in the foregoing cases.)

The following discussion reviews the circumstances of several recent and relevant cases, identifies the standards each court used when making its determination of whether or not to order the release of the anonymous speaker's identity, and finally attempts to characterize and categorize those standards into a synthesized set of common factors that can be used in successive litigation or adapted by an institution when evaluating its response to an anonymous speech issue, either as part of its own policy formation or related decision-making. The factors are as follows and are explained below as the cases are discussed: jurisdiction, good faith (both internal and external), necessity (both basic and absolute), and, at times, proprietary interest.

Tables 2a-d. ANONYMOUS INTERNET SPEECH: STANDARD OF DISCOVERY

Notes for Tables 2a-d:

*The *2TheMart.com* court made its decision after discussing both *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999); and *In re Subpoena Duces Tecum to America Online, Inc.*, 52 Va. Cir. 26 (2000). The *Dendrite International, Inc. v. John Doe No. 3* court also discussed both previous cases in determining the applicable standard or set of factors to employ.

**The language quoted is from *Dendrite International, Inc. v. John Doe No. 3*, 775 A.2d 756 (N.J. Super. Ct. 2001), issued on the same day and by the same judge from the New Jersey Superior Court that decided *Immunomedics, Inc. v. Doe.* The *Dendrite International, Inc. v. John Doe No. 3* court articulated the standard of review in anonymous Internet speech cases involving harms resulting from the release of proprietary information that the *Immunomedics, Inc. v. Doe* court reiterated in its decision, 775 A.2d at 776-777.

*** Several cases considered the formulation of factors in light of the harm to a proprietary interest, in all cases harm suffered by a corporation. In *In re Subpoena Duces Tecum to America Online, Inc.*, the economic harm was the potential loss of customers in the absence of a policy protecting the anonymity of subscribers, and in *Dendrite International, Inc. v. John Doe No. 3* and *Immunomedics, Inc. v. Doe* the harm to a proprietary interest was a direct result of the anonymous speech (the defamatory statements), in *Dendrite International, Inc. v. John Doe No. 3*, and in *Immunomedics, Inc. v. Doe*, *as* a result of breach of contract and tortious interference, among other claims.

Case	Problem	Factors	Balance
Columbia Insurance Co. v. Seescandy.Com, 185 F.R.D. 573 (N.D. Cal. 1999). Facts: Dispute over use of trademark owned by See's Candy Shops, Inc. against anonymous party who registered seescandy.com and seecandys.com. Release allowed.	"With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely online." "Parties who have been injured are likely to find themselves, chasing the tortfeasor...with little or no hope of actually discovering the identity of the tortfeasor."	Jurisdiction: (Standard of Conduct) "[I]dentify the missing party with sufficient specificity such that the court can determine that defendant is a real person or entity who could be sued in Federal court." Good Faith: Party (Internal Consistency) "[I]dentify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants." Legal "Good Faith": Claim (External Consistency) "[P]laintiffs should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." Necessity: Basic (as to party/claim) "[P]laintiff should file a request for discovery with the Court, along with reasons justifying the specific discovery requested as well as identification of a limited number of person or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible."	"In such cases the traditional reluctance for permitting filings against John Doe defendants or fictitious names and the traditional enforcement of strict compliance with service requirements should be tempered by the need to provide injured parties with an[sic] forum in which they might seek redress for grievances." Balance: right of redress with the right to speak anonymously.

Table 2-a. *Columbia Insurance Co. v. Seescandy.com*

The dispute in *Columbia Insurance Co. v. Seescandy.com* (Table 2a.) did not involve a claim of defamation or any tort for that matter; rather it arose out of a trademark dispute. The plaintiff, holder of a trademark on See's Candy Shops, sought the identity of the person, persons or entity that registered two domain names: seescandy.com and seecandys.com. The two domain names were registered anonymously with Network Solutions, Inc.

The court employed the use of four factors or safeguards to "ensure that this unusual procedure [the issuance of a subpoena ordering the release of the identity of an anonymous domain name registrant and alleged trademark infringer] will only be employed in cases where the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service, and will prevent use of this method to harass or intimidate." (*Columbia Insurance Co. v. Seescandy.com*, 578)

The first factor identified establishes that a court has the right to exert control over the questionable behavior. In law this is know as jurisdiction. As a practical matter jurisdiction is a way of saying that there is agreement on the standard of conduct (expressed in the law of the jurisdiction) by which to evaluate the claim made by the plaintiff of harm caused by the defendant. In *Columbia Insurance Co. v. Seescandy.com* the court required that "the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court." (578)

The court was also concerned that such requests by plaintiffs do not turn in routine "hunting" exercises and chill speech on the Internet. This requires plaintiffs demonstrate good faith. In *Columbia Insurance Co. v. Seescandy.com* the court looked to two types of good faith. One good faith factor is derived from the plaintiff's actions and might be viewed as accomplishing an internal consistency of sorts as it looks at factors internal to the litigation, i.e., the plaintiff's actions ("the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants," 579). The other good faith factor is derived from the legal merits of the case or the claim the plaintiff is making ("plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss," 579). This might be called "legal" good faith; it is an assessment made by the court to the facts at hand and thus is external in character. The good faith of the plaintiff whereas is an internal factor and is dependant upon how the plaintiff has conducted him or herself. Both factors relate to the consistency of legal process as meeting these two factors ensures that there is merit to both the plaintiff's actions and his or her legal claim.

Finally, there is a sense, expressed more definitely in latter cases discussed below, of necessity in granting the plaintiff's subpoena request, i.e., that redress (begun by "service of process") due the plaintiff by the defendant is not otherwise possible without the divulgation of the identity of the anonymous speaker or speakers ("the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible" 580). Can the identity be determined without the service provider or other intermediary revealing the identity of the anonymous speaker? If so, then the necessity requirement has not been met and the court will not exercise its subpoena power to compel divulgation of the identifying information from the service provider or other party holding the information.

The facts of *In re Subpoena Duces Tecum to American Online, Inc*. (Table 2b.) are somewhat different; here the plaintiffs or party requesting disclosure (itself proceeding under the pseudonym "Anonymous Publicly Traded Company) alleged that comments posted to chat rooms by five John Doe participants were defamatory, misrepresentative and if made by certain knowledgeable persons such as employees constituted a breach of fiduciary duties and contractual obligations of those individuals owed to the company." The Virginia court began with a discussion of the precedent protecting anonymous speech. Since the granting of the order would have involved a governmental function, i.e., the court ordered release of John Doe identities, the court placed its continued analysis within a constitutional (free speech) context. In addition to the historical and judicial precedent and the application of those concepts to the Internet speech, the court also pointed out that piercing the veil of Internet anonymity might also harm in an economic sense, an online service provider such as American Online, by driving customers away from America Online, to other service providers that are more vigilant in protecting their customer's privacy. (*In re Subpoena Duces Tecum to American Online, Inc*., 32)

The court pointed to three criteria that must be satisfied: "a court should only order a non-party, Internet service provider to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim." (*In re Subpoena Duces Tecum to American Online, Inc*., 37)

Case	Problem	Factors	Balance
In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26 (2000). Facts: Plaintiffs claim that five John Does in chat rooms published defamatory material, misrepresentations, and confidential material in breach of fiduciary duties and contractual obligations owed to plaintiffs. Release allowed.	Whether the "subpoena duces tecum issued by the Clerk of this Court unreasonably impairs the First Amendment rights of the John Does to speak anonymously on the Internet and therefore should be quashed..." "[W]hether a state's interest in protecting its citizens against potentially actionable communications on the Internet is sufficient to outweigh the right to anonymously speak on this ever-expanding medium."	Legal "Good Faith": Claim (External Consistency) "[W]hen the court is satisfied by the pleadings or evidence supplied to that court..." Good Faith: Party (Internal Consistency) Jurisdiction:(Standard of Conduct) "...that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and..." Necessity: Basic (as to party/claim) "...the subpoenaed identity information is centrally needed to advance that claim."	Potential chilling impact of subpoena: "It cannot be seriously questioned that those who utilize the 'chat room' and 'message boards' of AOL do so with an expectation that the anonymity of their postings and communications generally will be protected." "If AOL did not uphold the confidentiality of its subscribers, as it has contracted to do, absent extraordinary circumstances, one could reasonably predict that AOL subscribers would look to AOL's competitors for anonymity." "Those who suffer damages as a result of tortuous or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrong-doers from hiding behind an illusory shield of purported First Amendment rights." Balance: right to speak with the right of redress, the duty owed customers and the prevention of the loss of the ability to compete. ***

Table 2b. *In re Subpoena Duces Tecum to American Online, Inc.*

Analyzing the two cases, there is consistency between the criteria used in *Columbia Insurance Co. v. Seescandy.com* and the criteria used in *In re Subpoena Duces Tecum to American Online, Inc*. (See Table 2 and Table 3.) For example, the "satisfied by the pleadings or evidence" of *In re Subpoena Duces Tecum to American Online, Inc*. is similar to the "withstand a motion to dismiss" of *Columbia Insurance Co. v. Seescandy.com*. This prong represents a "legal" good faith requirement, imposed upon the court, that the allegations meet the legal requirements of a basic and viable claim.

The second *In re Subpoena Duces Tecum to American Online, Inc*. factor contains two elements also present in the earlier *Columbia Insurance Co. v. Seescandy.com* formulation: the "good faith basis to contend" is viewed as a good faith requirement as to the moving party (internal consistency) and the "conduct actionable in the jurisdiction," the more general jurisdictional requirement, i.e., that this is the proper court before which to bring the action.

Finally, the "identity information is centrally needed to advance the claim" language is taken from American Online's own anonymous speaker divulgation policy ("AOL acknowledged on brief that it has complied with hundreds of similar subpoenas issued by Virginia courts when it has been satisfied (1) that the party seeking the information has pleaded with specificity a prima facie claim that it is the victim of particular, specified tortious conduct and (2) that the subpoenaed identity information was centrally needed to advance the claim. AOL's Supplemental Memorandum In Support of Motion To Quash at 4-5." *In re Subpoena Duces Tecum to American Online, Inc*., 27, note 2). This is the necessity factor also present in *Columbia Insurance Co. v. Seescandy.com* ("reasonable likelihood...would make service of process possible").

Another case for review (Table 2c) presents a different posture between the plaintiff, the party moving for disclosure and the anonymous speakers. In *Doe v. 2TheMart.com, Inc.*, the anonymous speakers were not alleged to have caused harm to the plaintiffs. Rather the shareholders of 2TheMart.com alleged that the company's

Case	Problem	Factors	Balance
Doe v. 2TheMart.com, Inc., 140 F. Supp.2d 1088 (W.D. Wash. 2001).* Facts: Defendant, (Party B), sought the identity of 23 speakers (Party C) who participated anonymously on an online board, in order to ascertain whether the 23 speakers could provide a defense for Party B in its dispute with 2TheMart.com shareholders (Party A), in Party A's derivative class action against 2TM.com officers and directors (Party B). Released denied.	"[W]hat is the scope of an individual's First Amendment right to speak anonymously on the Internet" and "what showing must be made by a private party seeking to discover the identity of anonymous Internet users through the enforcement of a civil subpoena?"	Good Faith: Party (Internal Consistency) Whether "the subpoena seeking the information was issued in good faith and not for any improper purpose." Legal "Good Faith": Claim (External Consistency) Whether the "information is needed to advance core claims or defenses?" "The information sought by TMRT [2TheMart.com] does not relate to a core defense. Here, the information relates to only one of twenty-seven affirmative defenses raised by the defendant..." The information "relates only to a secondary claim or to one of numerous affirmative defenses." Necessity: Basic (as to party/claim) Whether the "identifying information [is] directly and materially relevant to a core claim or defense?" "Unlike in *Seescandy.com* and *American Online, Inc*. their identity is not needed to allow the litigation to proceed." Necessity: Absolute (as to claim) "TMRT [2TheMart.com] has failed to demonstrate that the information it needs to establish its defense is unavailable from any other source. The chat room messages are archived and are available to anyone to read and print."	"The subpoena would have required the disclosure of...information that has no relevance to the issues raised in the lawsuit. This apparent disregard for the privacy and the First Amendment rights of the online users, while not demonstrating bad faith per se, weighs against TMRT [2TheMart.com] in balancing the interests here." "[F]ree exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously." "If Internet users could be stripped of that anonymity...this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights." Balance: of litigant's right of redress ("necessity": basic and absolute) in third party matters with First Amendment rights, including the right to speak anonymously.

Table 2c. *Doe v. 2The Mart.com, Inc.*

directors and officers engaged in wrongdoing that harmed the shareholders and so brought what is known in corporate law as a "derivative action" or lawsuit against those directors and officers in a separate but thus related litigation. The directors and officers (the defendants in the related lawsuit but the party moving for disclosure in this case) believed that the true perpetrators of the harm were the anonymous posters of the messages on boards operated by InfoSpace, an online service provider, in specific, on its Silicon Investor website.

This action was brought by those directors and officers to compel release of the identity of the anonymous speakers in order to question them and gain evidence that might exculpate them as defendants in the separate but related shareholder derivative action. This is a critical distinction between the *Doe v. 2TheMart.com,* and the previous *Inc In re Subpoena Duces Tecum to American Online, Inc*., and *Columbia Insurance Co. v. Seescandy.com* cases. In the latter two cases, discussed earlier, the perpetrator of the harm and the anonymous speaker, thus the target of the plaintiff's motion for identity disclosure were one and the same person or persons. Whereas in *Doe v. 2TheMart.com*, the anonymous speakers were not the objects of the plaintiffs claim (the shareholders as plaintiffs against the directors and officers as defendants). Rather it was the defendant directors and officers, as the moving party, who sought the identity of anonymous posters in order to secure their defense in the related (derivative) shareholder litigation.

As a result, the *Doe v. 2TheMart.com* court adapted a slightly different but no less consistent configuration in its analysis. Like the *Inc In re Subpoena Duces Tecum to American Online, Inc.* court, the federal district court reviewed the existing Supreme Court precedent on anonymous speech. The district court also undertook its discussion cognizant of both the *Columbia Insurance Co. v. Seescandy.com* and *Inc In re Subpoena Duces Tecum to American Online, Inc.* decisions.

The *Doe v. 2TheMart.com* court adopted the following four-part test: "(1) the subpoena seeking the information was issued in good faith and not for any improper purpose,

(2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source." (*Doe v. 2The Mart.com* 1095, 1097) While there is no clear factor relating to jurisdiction, the *Doe v. 2TheMart.com* configuration is still consistent with the previous cases as to the requirement of a jurisdictional standard. This is so for one of two reasons. Jurisdiction might to some extent be either implied, or in the alternative, it is not required because this case unlike the others involves the actions of third parties. In other words, the jurisdiction or standard of conduct under which the actions of the anonymous speaker-perpetrators is to be judged is not relevant to this immediate issue of divulgation because the initial dispute (shareholders versus directors) is not before the court at this time.

Of the four factors (less jurisdiction) the *Doe v. 2TheMart.com* did develop, three are consistent with both the remaining factors of the *Columbia Insurance Co. v. Seescandy.com* and *Inc In re Subpoena Duces Tecum to American Online, Inc.* courts. In *Doe v. 2TheMart.com* there is both internal (as to party) and external (as to claim) consistency that are labeled good faith and "legal" good faith, respectively. The subpoena, in order to be granted must be "issued in good faith and not for any improper purpose" and it must relate to the advancement of "core claims or defenses." Unfortunately, the identity information related to only one of twenty-seven defenses and so the court concluded that its standards were not met. This is significant because unlike the *Columbia Insurance Co. v. Seescandy.com* and *In re Subpoena Duces Tecum to American Online, Inc.* courts, the court here did not grant the request of the directors and officers and refused to order the release of the identity of the anonymous posters.

Factors three and four both relate to necessity, but as this case involves the divulgation of a third party actor. The moving party, the "defendant" directors and officers were not requesting the information before proceeds against the anonymous speaker as perpetrator of some harm, but rather will ultimately use the information to proceed or defend against a different party (the shareholders) in another case (the derivative by shareholders against them). Here, the directors and officers needed the identity of the anonymous speakers in order to prepare a defense in the related case. As a result of the "once removed" relationship or third party nature of the anonymous speaker to the litigant (not needed in order to seek redress but in order to defend itself against another plaintiff seeking redress), the court expanded the necessity factor to include a requirement of what might best be labeled absolute necessity: "that the information it needs to establish its defense is unavailable from any other source." Unfortunately for the directors and officers this information was indeed available from other sources, including the message board where the postings were originally made, thus the court denied their request to issue an order to release the identity of the anonymous speakers.

In this way the three cases discussed herein are consistent with each other considering the different juxtaposition of parties in the third case, *Doe v. 2TheMart.com*. The requirement that the identity information be "directly and materially relevant to a core claim or defense" represents the necessity (basic) requirement of the *Columbia Insurance Co. v. Seescandy.com* ("requirements of service of process") and *Inc In re Subpoena Duces Tecum to American Online, Inc.* ("centrally needed to advance that claim") courts. However, here, because the *Doe v. 2TheMart.com* anonymous speaker is a third party there appears a slightly ascending standard among the three courts' basic necessity factor (see Table 3). Moreover, the court in *Doe v. 2TheMart.com* imposed an additional necessity criterion. This is called absolute necessity: "information it needs to establish its defense is unavailable from any other source." Not only must the identity of the anonymous speaker be materially relevant (basic necessity) to the dispute between the parties, it must be unavailable elsewhere (absolute necessity). As observed earlier, the court found the plaintiff's reasoning flawed, as the information was readily available from various chat room archives.

Two final cases, *Dendrite International, Inc. v. John Doe No.* 3 and *Immunomedics, Inc. v. Doe*, (Table 2d) are companion decisions released on the same day by the same court. While decided after *Doe v. 2TheMart.com*, neither of these two refers to the *Doe v. 2TheMart.com* decision. However, both *Columbia Insurance Co. v. Seescandy.com* and *In re Subpoena Duces Tecum to American Online, Inc.* are referred to by the lead decision in *Dendrite International, Inc. v. John Doe No. 3*. The internal consistency factor used by in *Dendrite International, Inc. v. John Doe No. 3*, good faith as to party ("identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitute actionable speech") is present. However, the court suggests that the plaintiffs must "undertake efforts to notify the anonymous posters" and "afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application." Yet, the court does not also intend a situation where the entire proceedings be conducted with the defendant incognito: "To allow a potential tortfeasor to disprove a plaintiff's case before the plaintiff is even provide the opportunity to learn the defendant's identity, let alone gather any discovery, has no foundation in New Jersey law." 775 A.2d at 778.

Case	Problem**	Factors**	Balance
Dendrite International Inc. v. John Doe No. 3., 775 A.2d 756 (N.J. Super. Ct. 2001).* Facts: Identity of anonymous speaker sought by company claiming he/she defamed company by posting several comments regarding corporate accounting practices regarding its corporate earnings. Release denied. *Immun-omedics, Inc. v. Doe*, 775 A.2d 773 (N.J. Super.Ct. 2001). Facts: Identity of anonymous poster of messages sought by company suspecting speaker was an employee, claims include breach of contract, legal duty of loyalty, negligence, tortious interference. Release allowed.	"We offer the following guidelines to trial courts when faced with an application by a plaintiff for expedited discovery seeking an order compelling an ISP to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals or businesses."**	Good Faith: Party (Internal Consistency) "[F]irst require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford to the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application."** "The court shall also require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitute actionable speech."** "Legal" Good Faith: Claim (External Consistency) "The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to R. 4:6-2(f), the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant."** Necessity: Basic (as to party or claim) "Finally, assuming the court concludes that the plaintiff has presented a prima facie cause of action, 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."**	"The trial court must consider and decide those applications by striking a balance between the well- established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the fictitiously-named defendants."** "In balancing Moonshine's right of anonymous free speech against the strength of the prima facie case presented and the necessity for disclosure, it is clear that the motion judge struck [sic] the proper balance in favor of identity disclosure." ** *** Balance: right to speak anonymously with the right of redress and the right to protect proprietary interests.

Table 2d. ***Dendrite International Inc. v. John Doe No. 3*. and *Immun-omedics, Inc. v. Doe***

While there is no specific mention of jurisdiction, it may be implied here as well from the "subject of a subpoena or application" requirement. An external consistency ("legal" good faith) is also present: "The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants...establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted...the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant." Passing a prima facie test in essence requires the court to apply the law of the jurisdiction to the alleged facts in a light most favorable to the plaintiff thus ensuring consistency in its proceedings. Finally a factor relating the basic necessity is included, i.e., that the "necessity for the disclosure of the anonymous defendant's identity [is needed] to allow the plaintiff to properly proceed." However in applying the same criteria the *Dendrite International, Inc. v. John Doe No.* 3 and *Immunomedics, Inc. v. Doe* courts respectively reached different results, in the former case the court maintained the anonymity of the speakers while in the latter case the court supported release of the identity of the anonymous posters.

Case	*Columbia Insurance Co. Seescandy.com,* 185 F.R.D. 573 (N.D. (Cal. 1999).	*In re Subpoena Duces Tecum to America Online, Inc*., 52 Va. Cir.26 (2000).****	*Doe v. 2TheMartcom, Inc*, 140 F. Supp. 2d (W.D. Wash. 2001). ***	*Dendrite International, Inc*., 775 A.2d 756 N.J. Super. Ct. 2001). *Immuno-medics, Inc*., 775 A.2d 773 (N.J. Super. Ct. 2001).****
Factor:				
Jurisdiction Standard of Conduct	person or entity who could be sued in federal court	victim of conduct actionable in the jurisdiction where suit filed	implied or not necessary????	implied???? subject of a subpoena or application
Good Faith: Party (Internal Consistency)	comply with requirements of service of process	legitimate, good faith basis to contend that it may be the victim...	issued in good faith and not for any improper purpose	efforts to notify,***** actionable speech
"Legal" Good Faith: Claim (External Consistency)*	withstand a motion to dismiss	pleadings or evidence supplied	core claims or defenses	prima facie, withstand a motion to dismiss, sufficient evidence
Necessity: Basic (party/claim)**	limited number of persons and make service of process possible	identity information centrally needed to advance that claim	identity information [is] directly and materially relevant to advance a core claim or defense	necessity for the disclosure...to allow the plaintiff to properly proceed
Necessity: Absolute (claim)	not applicable	not applicable	information it needs to establish its defense is unavailable from any other source	

Notes:

*The information in a third party action (*Doe v. 2TheMart.com, Inc.*) must relate to a "core claim or defense," not merely relate to the pleadings as a whole, i.e., withstanding a "motion to dismiss" as in *Seescandy.com* or found in the "pleadings or evidence" of the *America Online* dispute.

**Regarding the necessity factor, there is a subtle but increasing standard in the three cases progressing from "make service of process possible" (*Seescandy.com*) to "centrally needed to advance the claim" (*America Online*) to "directly and materially relevant" (*2TheMart.com*). The 2TheMart.com court cited favorably both previous cases.

***When the dispute involves third party action—the person seeking to discover the identity does not seek remedy from the anonymous speaker—there is less need for the identity to be revealed. In these circumstances the "jurisdiction" factor is implied or not relevant as the actual dispute between the plaintiff and defendant may take place in other jurisdiction altogether. In order for the identity of a third party defamer to be revealed it must be "directly and materially relevant to a core defense" and supplemented or replaced entirely by a higher standard of necessity: the litigation of the plaintiff against the third party cannot proceed unless the veil of anonymity is pierced. This higher, additional standard of necessity is labeled "absolute" as the "information it [the moving party, i.e., 2TheMart.com] needs to establish its defense is unavailable from any other source." This higher standard in third party actions was observed in *Doe v. 2TheMart.com*: "The standard for disclosing the identity of a non-party witness must be higher than that articulated in *Seescandy.com* and *America Online, Inc*. When the anonymous Internet user is not a party to the case, the litigation can go forward without the disclosure of their identity." (140 F. Supp 2d at 1095.)

****Though not included as a specific factor, both the *America Online, Inc.* and *Immunomedics, Inc. v. Doe* cases phrased the ultimate use of the factors as offering assistance to courts in balancing the right to speak anonymously with potential impact that speech might have upon the proprietary interest of the plaintiff, either in the loss of future Internet speakers as customers to America Online in *America Online* or in harms perpetrated against the plaintiff itself in *Immunomedics, Inc. v. Doe*.

***** The standard articulated by the New Jersey court in the *Dendrite International, Inc. v. John Doe No. 3* and *Immunomedics, Inc. v. Doe* cases suggest a factor that anticipates the anonymous speaker be given notice of the impending divulgation: "We hold that when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board." 775 A.2d at 761, and repeated again at 775 A.2d 773.

Table 3. Summary

The *Dendrite International, Inc. v. John Doe No.* 3 involved a claim of defamation resulting from statements posted on an online bulletin board dedicated to Dendrite investors that adversely affected the value of the stock of the plaintiff corporation. In *Immunomedics, Inc. v. Doe*, breach of contract and tortuous interference with economic

interest were among numerous claims made by a corporation that suspected an employee was behind the anonymous postings of proprietary information. The decision of the *Immunomedics, Inc. v. Doe* court to support divulgation of the identity of the speakers is contrasted with *Dendrite International, Inc. v. John Doe No.* 3 where the reviewing court agreed with the trial court and concluded that the insufficient evidence presented did not warrant release of the identity information: "The record does not support the conclusion that John Doe's postings negatively affected the value of Dendrite's stock, nor does Dendrite offer evidence or information that these postings have actually inhibited its hiring practices, as it alleged they would." Whereas in *Immunomedics, Inc. v. Doe*, the court felt that the plaintiffs had demonstrated that "Moonshine [the pseudonym of the anonymous poster] is an employee of Immunomedics, that employees execute confidentiality agreements, and the content of Moonshine's posted messages providing evidence of the breach thereof, the disclosure of Moonshine's identity, which can be reasonably calculated to be achieved by information obtained from the subpoena, was fully warranted." The circumstances of these two cases suggest that courts may consider whether the anonymous posting might harm the proprietary interest of the aggrieved party.

Finally, the resulting difference in the outcomes between two cases from the same court with similar facts is also important because it suggests that the criteria used to determine whether or not a court will support the release of identity information of anonymous speakers is not reduced to a bright line test or a sole factor of the whether the identity is related to a primary party as speaker (released in *Columbia Insurance Co. v. Seescandy.com* and *Inc In re Subpoena Duces Tecum to American Online, Inc.*) versus a third party as speaker (release denied in *Doe v. 2The Mart.com*), but may vary between two first party cases.

The New Jersey cases, both involving actions claimed to harm the proprietary interest of a corporation, are thus consistent with the developing formulation of other courts requiring two aspects of good faith, one as to party the other as to claim, another factor involving jurisdiction and a fourth concept of necessity, which is at least basic (needed to proceed) and may be absolute in third party actions (unavailable from any other source). (See Table 3)

Incorporating Developing Legal Standards into Institutional Decision-Making

Courts have been consistent in the analysis of the factors that must be present before a court will either order enforcement of a discovery subpoena or a issue a subpoena of its own accord, and in either case pierce the veil of anonymous Internet speech. For example, America Online contended that it was unwilling to comply with the subpoena and release the names of the anonymous speakers because the company requesting the release refused to reveal is own identity, as a result the court issued a subpoena for release of the identity information. It should be observed that none of the criteria require in specific that the anonymous speaker be given notice that his or her identity is about to be revealed. Only the *Dendrite International, Inc. v. John Doe No. 3* and *Immunomedics, Inc. v. Doe* court believed that notice should be first given in order to offer the anonymous a speaker an opportunity to respond to an impending divulgation of his or her identity. This suggests that a service provider or other entity could at least notify the anonymous poster of the impending release of his or her identity, consistent with the *Dendrite International, Inc. v. John Doe No.* 3 and *Immunomedics, Inc. v. Doe* decisions.

In most cases the intermediary will either release the information on their own accord, or deny the request for release by the plaintiff in which instance several of the resulting cases have arisen. These factors can be used to construct institutional disclosure policies that indicate to the speaker—the customer, student or employee—when the veil of his or her anonymity will be pierced.

It is obvious that the standards courts employ will influence both the policies that institutions adopt and the decision-making it undertakes. Moreover, the standards articulated by courts may influence in specific those entities such as online service providers that field requests from third parties for release of customer identity information. This was evident in the *Inc In re Subpoena Duces Tecum to American Online, Inc.* (AOL policy reprinted in footnote 2 and discussed at pages 27-28 of the decision). Consider the Yahoo! Policy at issue in *Dendrite International, Inc. v. John Doe No.* 3 and *Immunomedics, Inc. v. Doe*. The policy allowed release of identity information in one of three circumstances: 1) with the permission of the speaker, 2) in "special circumstances," when Yahoo! "believes in good faith that the law requires it," or 3) when it is necessary to identify, contact or bring legal action against someone who may be violating Yahoo!'s Terms of Service or may be causing injury to...anyone...that could be harmed by such activities," as quoted in *Dendrite International, Inc. v. John Doe No.* 3 (775 A.2d at 762). While adopting policy language linking institutional responses to developing legal standards or the reality of third party harms (ultimately determined by existing legal standards) might appear to provide the institution with somewhat of a legal or moral imperative to release the identity information it also requires cognizance of the developing law.

Consider Internet scenarios where the words of anonymous speakers may arguably cause harm and where the aggrieved party or some other party at interest might desire to know the source of the anonymous speech. It is obvious that an outside party might seek the disclosure of a customer, student or employee, in conjunction with a legal dispute if that individual has perpetrated some malfeasance against the outside party. In those cases the factors articulated in the previous discussion would apply. See, Table 2 and Table 3. However, these factors can also be adapted and used to guide "disputes" that might arise internally within an institution as well. Here it is contemplated that no actual legal action would be taken, but an Intranet web master or other institutional online administrator or one acting in a similar capacity as a "watchdog" might receive internal requests for the release of identity information. In response the institution might look to the developing precedent and adapt the criteria for use in its own internal unique decision-making setting.

There are several benefits to this approach. The modeling of institutional policies for internal use consistent with developing precedent can help preserve a spirit of free speech, yet allow for the continued functioning of the organization. Such policies can also be easily adapted to apply in situations where the request is from an external source and would then mirror the case law more precisely. In the latter external-request scenario, a legally consistent policy could save the institution time and legal entanglement, as it would have the determinative factors already incorporated into its operating policies. In the former internal-request scenario, there may result a positive impact upon morale, as members of the organization base decisions on articulated standards, which in the present discussion attempt to incorporate common values such as free speech, privacy, anonymity, etc. As a result, this offers consistency between external (request from a third party) and internal (request coming from within the organization) decision-making.

Institutions such as commercial entities, schools or employers may wish to apply or adapt these evolving standards to situations likely to occur in their respective internal settings. Consider the following three scenarios: one from e-commerce, one from an educational environment and another in an employer-employee context. Suppose a web site proprietor would like to share customer information with another product or service department within the organization or with a related entity such as a subsidiary, or a school administrator would like to identify the student who posted a malicious message suggesting that the student-poster is the one behind recent acts of vandalism at the school, or an employer would like to identify an anonymous employee who may be engaging in a pattern of harassment of other employees or customers, or making improper (but not otherwise unlawful) comments about the employee or customer. (See Table 4) (It should be noted that this discussion does not incorporate the relevance of other laws that may forbid release of information to third parties, such as federal privacy legislation governing the release of customer information or student records. If this is a concern to the institution, then the custodian of the information should obtain the consent of the speaker as a condition of service, access or employment, as most laws contain a consent exception. The incorporation of these principles into the institutional structure demonstrates how legal precedent may impact the development of fair information practices even though, in light of the consent of the speaker, there would be no legal obligation to maintain the confidentiality of the information.)

How can the four factors be applied to institutional settings and guide decision-making in determining when it might be prudent to release the identity of anonymous posters either internally or externally to third parties? As with the application of these factors in the subpoena or court order scenarios, all four factors must be present or the release of identity cannot be made. In addition, the examples of the factors might be applied in the scenarios presented serve as mere suggestions, as particular institutions might derive their own "interpretations" of a how factor such as necessity might be applied.

Applying the jurisdiction factor would suggest that the anonymous speech occurred using the institution's technology or somehow relates to subject or context of the institution. For an e-educational setting this might mean that the harmful posting was made by students using the school's computer network and related to a school sponsored activity. For an e-commerce or employer-employee scenario this might mean that only the identity of current employees or customers could be released as opposed to former or future employees or customers. Different institutions could define the limits of this "jurisdiction" differently, but the concept remains the same, approximating the logical limits of subjects over which the institution has control.

The second, internal good faith factor might require that an employer not pierce that veil of anonymity for the sole purpose of snooping on what employees are saying to each other or about customers. Instead the identity of an employee could be released as part of an internal network "audit" in response to some perceived harm, i.e., in order to curb misuse of its system or to investigate the posting of harassing messages by employees, or to perform routine (as opposed to extraordinary, i.e., repeated and invasive) "business" or performance monitoring of employees. This concept of "ordinary course of business" or "legitimate business purpose" is often used in other contexts such as the regulation of privacy and electronic communications

under federal law (18 U.S.C. §2510 et seq.) and could be adopted here as well.

The third factor, of "legal" good faith might require compliance with various disclosure requirements. In the same way courts made an assessment based upon the existing law so too does the organization use some measure by which to assess of conforming behavior, such as association standards, industry best practices, etc. As observed earlier, this might mean conformance to other information laws such as those protecting the privacy of student school or school library records. (See, Lipinski, 2001; Lipinski, 1999) In e-commerce settings it might suggest that the institution conform to developing industry standards of privacy/anonymity, or in employee performance monitoring for example, to align practices with the developing law.

Setting:	e-Commerce*	Educational** Environment	Employment***
Anonymous Speaker:	Customer	Student	Employee
Factor:			
Jurisdiction Standard of Conduct	current customer or "minimum contacts" of both parties via web established****	use of premise or property and related to school sponsored activity	same standard: premise or property or current customer or contacts
Good Faith: Party (Internal Consistency)	notice to customer prior to release: consent or expresses initial interest	promote school safety or increase effectiveness of educational process	curb harassment or create a positive work environment
"Legal" Good Faith: Claim (External Consistency)	industry or developing regulatory standards	compliance with federal, state laws district policy or other standards of conduct	compliance with federal, state laws or company policy articulating standards of conduct
Necessity: Basic (party/claim)	needed to process customer order or request	needed in order to identify perpetrators of harm or abuse	needed in order to promote corporate "civility code"
Necessity: Absolute (claim)	Not Applicable?: independent compilation of customer information is cost prohibitive	Not Applicable?: identity necessary in order to curb vandalism, enforce tolerance or behavior policy	Not Applicable?: unable to determine breech agreement without information from third party
Proprietary Interest	Not Applicable?: loss of customers to competitors regarding new product or service development	Not Applicable?: damage to physical environs or potential liability of school district	Not applicable?: economic reputation of company or good standing of customers affected

Notes:

*In the e-Commerce setting assume the customer interacts with the organization through the vendor web site anonymously, another service or product unit within the organization or a related entity such as a subsidiary desires to know the identity of an anonymous customer. (Note: this scenario presupposes that the e-commerce vendor is in compliance with other applicable privacy laws regarding the release of consumer information to third parties or has nonetheless obtained the consent of the customer as a condition of the initial service or product interaction.)

**In the educational environment assume the school administration desires to know the source of anonymous student postings as the messages posted suggest the speakers are responsible for harms related to the school environment such as recent vandalism, might have information regarding the lack of compliance with a zero tolerance policy by other students or attempts to trace the source of recent derogatory postings about teachers or administrators or other unacceptable communications made through school computing facillites, i.e., in violation of a "school acceptable use" policy.

***In the employment setting assume the employer would like to obtain the identity of anonymous posters (employees) who may be the perpetrators of harassing messages made with respect to other employees or disparaging comments about customers or the company itself.

****"Minimum contacts" refers to a legal standard that is met when web site purveyors have conducted business through their web site sufficient to establish that there is enough interaction (minimum contacts) with web site visitors to subject the web site owner to legal jurisdiction in the home state of the web site visitor even though it may be different than the home state of the web site owner. The practical result is that the web site visitor-customer need not commence litigation in a different state than his or her own, such as the home state or jurisdiction of the web site owner, but can seek recourse from the court system in his or her own state. See, *International Shoe Co. v. Washington*, 326 U.S. 310 (1945). See also, David S. Godkin and Marc E. Betinsky, Personal Jurisdiction: If the [International] Shoe Fits, Wear It – But Does it Fit the Net?, JOURNAL OF INTERNET LAW, July, 1999, at 17, and the cases discussed therein.

Table 4. Applying Developing Legal Standard of Anonymous Speech: Three Case Studies

Finally, the necessity factor might suggest that divulgation of a student's identity would be released by school A (applying the factors) in response from a request from School B order to assist B in enforcing its zero tolerance policy. The request is made to school A by B for the identity of several of A's students who might have witnessed a potential infraction of school B's policy. Another example of necessity might exist in the investigation of a possible breach of a non-compete or non-disclosure agreement in an e-commerce or employment context where employer A suspects that former employee C is engaging in conduct in violation of the agreement. The request for information is made to employer B for customer information that A believes will help it determine whether or not C has violated the non-compete or non-disclosure agreement in force between A and C. Both examples mirror the third party scenario of the *Doe v. 2The Mart.com* case. In either case, the zero tolerance policy or the non-compete or non-disclosure agreement could not be enforced unless the institution—the school or employer—knows the identity of a anonymous posters who can help it identify the deviation from the agreed upon behavior (tolerance policy or agreement).

As commented earlier, the release of the customer, student or employee identity could not be made unless some aspect of each of the four factors was present in a given situation. Incorporating such standards into internal institutional decision-making would impart a spirit of free speech and the right to speak anonymously that courts have attempted to preserve in legal proceedings. Furthermore, conforming institutional releases of identity to third parties according to the four articulated standards would also align institutional policies with the developing legal precedent should a request for disclosure be made by an external third party in conjunction with related legal proceedings.

Conclusion

This paper discussed the developing precedent concerning anonymous speech on the Internet. In specific, under what conditions will courts indorse the release of identity information relating to the anonymous speaker? Having an understanding of these cases will help institutions articulate appropriate responses when faced with similar requests for information from third parties or when the institution is itself the target of perceived harmful and anonymous speech, and it seeks to obtain the identity of the anonymous speaker. While courts have adopted various standards, this paper synthesized these into four factors: jurisdiction, good faith as to party, good faith as to legal claim, and necessity (basic or absolute). These standards can drive institutional decision-making, making it legally compliant (external requests for information), but factors can also be adopted to design internal policies and decision-making as well, and as a result contribute to an overall climate of compliance and consistency.

Please Note: This paper is designed to provide accurate and authoritative information in regard to the subject matter covered. However, this information is NOT provided as a substitute for legal advice. If legal advice or expert assistance is required, the services of a competent legal professional should be sought.

References

Ballon, Ian C. (July/August, 1997). Defamation and Preemption under the Telecommunications Act of 1996: Why the Rule in *Zeran v. America Online* is Wrong, *Cyberspace Lawyer* 2: 6-10.

Conference Report, House Report 104-458. (104th Congress, 2nd Session (1996)). (Conference Report on the Telecommunications Act of 1996). Washington, D.C.: United States Government Printing Office.

Counts, Cynthia L. and C. Amanda Martin. (1996). Libel in Cyberspace: A Framework for Addressing Liability and Jurisdictional Issues in this New Frontier, *Albany Law Review*, 59, 1083-1133.

Godkin, David S. and Marc E. Betinsky. (1999, July). Personal Jurisdiction: If the [International] Shoe Fits, Wear It – But Does it Fit the Net? *Journal Of Internet Law*, 17-.

Kane, Michelle J. (2000). Business law: 1. Electronic Commerce: b) Internet Service Provider Liability: *Blumenthal v. Drudge*, *Berkeley Technology Law Journal.* 14: 483-501.

Keeton, W. Page, et al. (5th ed. 1984). *Prosser And Keeton On The Law Of Torts*. St. Paul, Minnesota: West Group.

Lipinski, Tomas A. (1999). Designing and Using Web-Based Materials in Education: A Web Page Legal Audit--Part II, Information Liability Issues, *Education Law Reporter* 137: [21] (October 14, 1999).

Lipinski, Tomas A. (2001). Legal Issues Involved in the Privacy Rights of Patrons in "Public" Libraries and Archives, in *Libraries, Museums And Archives: Legal Issues And Challenges In The New Information Era* 95-111 (Tomas A. Lipinski editor). Lanham, Maryland: Scarecrow Press, Inc.

Lipinski, Tomas A., Elizabeth A. Buchanan, and Johannes J. Britz. (2002). Sticks and Stones and Words that Harm: Liability vs. Responsibility, Section 230 and Defamatory Speech in Cyberspace, *Ethics and Information Technology* (forthcoming).

Restatement of Torts, Restatements of the Law, Second, Torts. (1977). Philadelphia, Pennsylvania: American Law Institute.

Spencer, Michael H. (2000). Defamatory E-Mail and Employer Liability: Why Razing *Zeran v. America Online* Is a Good Thing, *Richmond Journal of Law and Technology* 6: 25-.

Street, F. Lawrence and Mark P. Grant. (2001). *Law of the Internet*. Newark: New Jersey: LexisNexis.

Talbot, James M. (1999). *New Media: Intellectual Property, Entertainment And Technology Law*. St. Paul, Minnesota: West Group.

Wiener, David. (1999). Negligent Publication of Statements Posted on Electronic Bulletin Boards: Is There Any Liability Left After Zeran?, *Santa Clara Law Review* 39: 905-939.

Zuckman, Harvey L., et al. (2001). *Modern Communications Law*. St. Paul, Minnesota: West Group.

Legal References

Ben Ezra, Einstein & Co. v. American Online, Inc., 206 F. 3d 980 (10th Cir. 2000).

Blumenthal v. Drudge, 992 F. Supp 2d 44 (D.D.C. 1998).

Buckley v. American Constitutional Law Foundation, 525 U.S. 182 (1999).

Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

Dendrite International, Inc. v. John Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. 2001),

Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 140 1088 (W.D. Wash. F. Supp. 2d at 1092. 2001).

Doe v. American Online, Inc., 783 So. 2d 1010 (Florida 2001).

Firth v. State of New York, 184 Misc.2d 105 (N.Y. Ct. Cl. 2000).

Immunomedics, Inc. v. Doe., 775 A.2d 773 (N.J. Super. Ct. 2001).

In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26 (2000).

International Shoe Co. v. Washington, 326 U.S. 310 (1945).

Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772 (Cal. App. 2001).

Lunney v. Prodigy Services Co., 701 N.Y.S.2d 684 (1999); cert. denied 120 S. Ct. 1832 (1999);

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

Reno v. A.C.L.U., 521 U.S. 844 (1997).

Stoner v. eBay. Inc., No. 305666 (Cal. Super. Ct., San Francisco County, Nov. 7, 2000).

Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 N.Y. Misc. LEXIS 229, 23 Media L. Reporter (BNA) (N.Y. Sup. Ct. May 24, 1995).

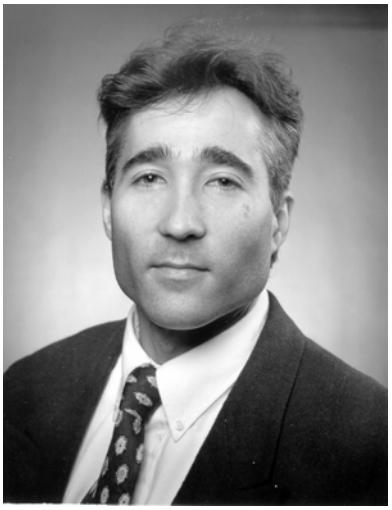
Talley v. California, 362 U.S. 60 (1960).

Van Buskirk v. The New York Times Co., 2000 WL 1206732 (S.D.N.Y. Aug. 24, 2000).

Watchtower Bible and Tract Society of New York v. Village of Stratton, 122 S. Ct. 2080 (2002).

Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).

Biography



Tomas A. Lipinski is Co-Director and Assistant Professor of the Center for Information Policy Research at the School of Information Studies at the University or Wisconsin—Milwaukee. In summers he is a visiting faculty member of the University of Illinois at Urbana-Champaign and the University of Pretoria, Pretoria, South Africa. He researches, teaches and lectures in the areas of information and Internet law and policy, including copyright. Recent titles of interest to educators include, as editor and contributor, a monograph entitled Libraries, Museums and Archives: Legal Issues and Challenges in the New Information Era (2001), a chapter entitled Legal Issues in Web-Based Distance Education, in Handbook of American Distance Education, to be published by Pennsylvania State University Press (Michael G. Moore, editor) (forthcoming 2002), and the following article entitled Legal Reform in an Electronic Age: Analysis and Critique of the Construction and Operation of S. 487, the Technology, Education and Copyright Harmonization (TEACH) Act of 2001, under review by the Brigham Young University Education and Law Journal.