Tulsa Law Review

Volume 47
Number 3 *State-Tribal Relations: Past, Present, and Future*

Volume 47 | Number 3

Spring 2012

In Defense of Anonymous Online Speech in Oklahoma

Sean Kilian

IN DEFENSE OF ANONYMOUS ONLINE SPEECH IN OKLAHOMA

The Internet is a democratic institution in the fullest sense. It serves as the modern equivalent of Speakers' Corner in England's Hyde Park, where ordinary people may voice their opinions, however silly, profane, or brilliant they may be to all who choose to read them.[1]

The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously.[2]

I. INTRODUCTION

Despite the many ways the Internet impacts our lives, some would argue that its greatest value lies in strengthening democracy[3] by empowering individuals whose voice might otherwise not be heard. It has been called the "greatest innovation in speech since the invention of the printing press"[4] and a "unique democratizing medium unlike anything that has come before."[5] The democratic nature of the Internet[6] is at odds with two types of litigation that have evolved over the past forty years: the strategic lawsuit against public participation ("SLAPP") and its more recent digital offspring, the cyber SLAPP.

A cyber SLAPP is a variation of a SLAPP, which was first identified and named[7] by Professors Penelope Canan and George W. Pring in a study published in 1988.[8] They described SLAPPs as "attempts to use civil tort action to stifle political expression."[9] The goal of a SLAPP is not to win the suit, but rather to "use litigation to intimidate

1. Notice of Motion by John Doe to Proceed Under Pseudonym and to Quash Deposition Subpoena Directed to Yahoo!, Inc. and Memorandum of Points and Authorities in Support Thereof at 3, Pre-Paid Legal Servs. Inc. v. Sturtz (Super. Ct. for the Cnty. of Santa Clara 2001) (No. CV798295).

2. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

3. Michael L. Best & Keegan W. Wade, *The Internet and Democracy: Global Catalyst or Democratic Dud?* (Berkman Ctr. Research Publ'n No. 2005-12), *available at* http://cyber.law.harvard.edu/publications/2005/Internet_and_Democracy_Global_Catalyst_or_Democratic_Dud.

4. Raymond Shih Ray Ku, *Open Internet Access and Freedom of Speech: A First Amendment Catch-22*, 75 TUL. L. REV. 87, 88 (2000).

5. Doe v. Cahill, 884 A.2d 451, 455 (Del. 2005).

6. *See* Reno v. ACLU, 521 U.S. 844, 868 (1997).

7. Penelope Canan & George W. Pring, *Strategic Lawsuits Against Public Participation*, 35 SOC. PROBS. 506, 506 (1988).

8. *Id.*

9. *Id.*

opponents' exercise of rights of petitioning and speech."[10] One court has characterized SLAPPs as "generally meritless suits brought by large private interests to deter common citizens from exercising their political or legal rights or to punish them for doing so."[11] Though the suits are often meritless, they nevertheless produce the intended effect of chilling the defendant's rights to petition and to freedom of speech.[12]

The Canan and Pring study identified four categories of factual bases[13] under which a SLAPP may arise, the most common being where one party's petition to the government about a problem triggers a lawsuit by another party with an opposing interest.[14] There are many different factual bases for the countless SLAPPs filed since the study.[15] Many state legislatures have responded to the SLAPP phenomenon by passing anti-SLAPP statutes.[16] To date, twenty-seven states have passed some form of anti-SLAPP statute, including Oklahoma.[17]

The particular and recent variation of SLAPP that this comment will address is the cyber SLAPP, the name given to a SLAPP when it arises not out of the defendant's petition, but out of his anonymous online speech.[18] The distinguishing feature of a cyber SLAPP is that its goal is not only to silence the defendant but also to identify him.[19] One example of a typical cyber SLAPP might progress as follows.[20] An individual posts an

10. Duracraft Corp. v. Holmes Prods. Corp., 691 N.E.2d 935, 940 (Mass. 1998).

11. Wilcox v. Super. Ct., 33 Cal. Rptr. 2d 446, 450 (Cal. Ct. App. 1994).

12. U.S. CONST. amend. I; *see* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

13. Canan & Pring, *supra* note 7, at 508-09.

14. *Id.* at 508.

15. *See* Equilon Enter. v. Consumer Cause, Inc., 52 P.3d 685 (Cal. 2002) (where an oil company sued a consumer group over its notice of intent to sue the company, and the court granted a consumer group's anti-SLAPP motion to dismiss); Damon v. Ocean Hills Journalism Club, 102 Cal. Rptr. 2d 205 (Cal. Ct. App. 2000) (where a former manager of a homeowner's association brought a defamation action against residents who wrote an article critical of him, and the court granted the residents' motion to strike); Berryhill v. Ga. Cmty. Support & Solutions, Inc., 638 S.E.2d 278 (Ga. 2006) (where a non-profit organization brought a tort action against a mother who complained about services rendered by the organization to her son, and the court granted her anti-SLAPP motion to dismiss); Melius v. Keiffer, 980 So. 2d 167 (La. Ct. App. 2008) (where a bar owner filed suit against individuals who spoke out in opposition of a plan to construct a new bar, and the court granted the individuals' motion to strike the petition); Baker v. Parsons, 750 N.E.2d 953 (Mass. 2001) (where a property owner sued an individual who commented to state officials about the property owner's application to construct a pier, and the court granted the individual's anti-SLAPP motion to dismiss); Maietta Const., Inc. v. Wainwright, 847 A.2d 1169 (Me. 2004) (where a court dismissed a defamation action filed in response to a resident's letters to city council under an anti-SLAPP statute).

16. ARIZ. REV. STAT. ANN. §§ 12-751 – 12-752 (2009); ARK. CODE ANN. §§16-63-501 to 16-63-508 (2009); CAL. CIV. PROC. CODE § 425.16 (West 2006); DEL. CODE ANN. tit. 10, §§ 8136 – 8138 (2009); FLA. STAT. ANN. § 768.295 (2005); FLA. STAT. § 720.304(4) (2010); GA. CODE ANN. § 9-11-11.1 (2008); HAW. REV. STAT. §§ 634F-1 to 634F-4 (2002); 735 ILL. COMP. STAT. 110/1 to 110/99 (2008); IND. CODE §§ 34-7-7-1 to 34-7-7-10 (2008); LA. CODE CIV. PROC. ANN. art. 971 (2008); ME. REV. STAT. ANN. tit. 14 § 556 (2008); MD. CODE ANN. § 5-807 (2008); MASS. GEN. LAWS ANN. ch. 231 § 59H (West 2008); MINN. STAT. §§ 554.01 – 554.05 (2008); MO. REV. STAT. § 537.528 (2008); NEB. REV. STAT. §§ 25-21,241 to 25-21,246 (2008); NEV. REV. STAT. §§ 41.635 – 41.670 (2008); N.M. STAT. ANN. §§38-2-9.1 to 38-2-9.2 (2008); N.Y. C.P.L.R. 3211(g) & 3212(h) (2009); OKLA. STAT. tit. 12, § 1443.1 (2008); OR. REV. STAT. §§ 31.150 – 31.155 (2008); 27 PA. CONS. STAT. §§ 8301 – 8305 (2008); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (2008); R.I. GEN. LAWS § 45-24-67 (2008); TENN. CODE ANN. §§ 4-21-1001 to 4-21-1004 (2009); UTAH CODE ANN. §§ 78B-6-1401 to 78B-6-1405 (2008); WASH. REV. CODE § 4.24.520 (2008).

17. OKLA. STAT. tit. 12, § 1443.1 (2008).

18. Press Release, cyberSLAPP.org, Privacy Groups Demand Protection of Users' Anonymity Online (July 11, 2002), *available at* http://www.cyberslapp.org/DoePressRelease.cfm.

19. *Id.*

20. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001); Dendrite Int'l, Inc. v. Doe No.

anonymous message on an online message board that is critical of another individual or corporation.[21] The target of the message files a lawsuit against the author for defamation and then subpoenas the author's Internet service provider ("ISP") for information that can be used to identify him.[22] Some ISPs notify their customers before complying with subpoenas but others may not.[23] If the ISP complies with the subpoena before the author can intervene then the author loses his constitutionally protected right to anonymous free speech.[24]

Anytime an individual decides to speak out anonymously online, someone may have an interest in quieting the speaker.[25] Anonymous online speech is a legitimate tool that can be used for many beneficial purposes, such as whistle blowing,[26] exposing fraud, criticizing a public official,[27] labor organization, or participating in political movements. Many times, anonymity is a critical factor that allows the speaker to speak freely when he otherwise might not, but empowering a speaker to speak freely also opens the door to nefarious uses[28] of anonymous online speech. Despite its positive uses, the cloak of anonymity also removes the fear of reprisal for Internet users who choose to harass and defame others.[29] This comment will address how Oklahoma's courts and legislature should balance the conflicting interests of the anonymous online speaker and his target while giving due weight both to the speaker's right to remain anonymous and the target's right to defend himself in the legal system.[30] As stated by one court, "the right to communicate anonymously must be balanced against the need to assure that those persons who choose to abuse the opportunities presented by this medium can be

3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

21. *See* cases cited *supra* note 20.

22. *See* cases cited *supra* note 20.

23. *See* Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1160 (Cal. Ct. App. 2008) (where ISP notified its customer before complying with a subpoena). *But see* Corcept Therapeutics, Inc. v. Rothschild, 339 F. App'x 789, 790 (9th Cir. 2009) (where ISP did not notify its customer and plaintiff learned defendant's identity).

24. *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960). The citations in this footnote support the constitutionally protected right to anonymity assertion, but not the online portions.

25. *See 2TheMart.com Inc.*, 140 F. Supp. 2d 1088; Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005).

26. *See* George F. du Pont, *The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils*, 6 J. TECH. L. & POL'Y 175, 184 (2001).

27. At least one cyber-SLAPP has been filed in Oklahoma, although the plaintiff dismissed his case before a decision was reached. *See* Burd v. Cole, No. CJ 2006-03717 (Okla. Dist. Ct. Tulsa Cnty. dismissed July 17, 2006). Burd was the superintendent of Sperry Public Schools and he alleged that the Cole and others slandered him on an Internet message board. *See* Petition at 2-3, Burd v. Cole, No. CJ 2006-03717 (Okla. Dist. Ct. Tulsa Cnty. June 13, 2006). He issued a subpoena to the defendants' ISP, which requested the identity of every person registered at the message board. Notice of Subpoena Duces Tecum at 4, Burd v. Cole, No. CJ 2006-03717 (Okla. Dist. Ct. Tulsa Cnty. June 22, 2006). Burd dismissed the case following Cole's motion to quash the subpoena, which argued that the subpoena should be quashed because it was overbroad and forced the defendants to unnecessarily give up their anonymity. Motion to Quash by Anonymous Speakers and Supporting Memorandum of Points and Authorities at 15, Burd v. Cole, No. CJ 2006-03717 (Okla. Dist. Ct. Tulsa Cnty.). *See also Burd v. Cole*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/cases/burd-v-cole (last visited Nov. 28, 2010).

28. du Pont, *supra* note 26, at 184.

29. *See* Jonathan D. Jones, Note, *Cybersmears and John Doe: How Far Should First Amendment Protection of Anonymous Internet Speakers Extend?*, 7 FIRST AMENDMENT L. REV. 421, 421 (2009) (describing an incident where online anonymity was used to harass a female law student).

30. *See infra* Part IV.A.

made to answer for such transgressions."[31] Although there are no Oklahoma statutes[32] or cases directly on point, courts and legislatures in other jurisdictions are developing a consensus[33] on how to balance these interests that can guide Oklahoma's approach. The Oklahoma legislature should respond to this litigation trend proactively by expanding the state's anti-SLAPP statute to protect its Internet users' First Amendment rights to anonymous online speech.

Part II of this comment provides an overview of Supreme Court decisions that have held that the First Amendment protects the right to anonymous speech.[34] Part II will also look at Supreme Court decisions that have held that the First Amendment protects speech on the Internet in the same way as speech through any other medium.[35] Part III of this comment identifies and analyzes the different provisions of state anti-SLAPP statutes and provides a look at cyber SLAPP cases from other jurisdictions.[36] Part III looks at how courts have applied existing anti-SLAPP laws to cyber SLAPP cases[37] and concludes by finding which provisions best protect the cyber SLAPP defendant. Part III also provides an overview of anti-SLAPP jurisprudence in Oklahoma and discusses the limited applicability of Oklahoma's anti-SLAPP statute.[38] Part IV of this comment discusses the two key principles that courts have used to protect defendants' anonymity.[39] Part IV also analyzes the effect that ISP privacy policies can have on anonymity in the absence of guidelines that regulate ISP compliance with civil subpoenas seeking a defendant's identifying information.[40] Finally, Part V of this comment concludes by recommending how Oklahoma's anti-SLAPP statute could be changed to reflect standards developing across the country.

II. THE CONSTITUTIONAL BASIS FOR PROTECTING ANONYMOUS ONLINE SPEECH

A. The Right to Speak Anonymously

Reformers throughout our country's history have long employed anonymous speech as a tool to spread their messages.[41] The Constitution's original advocates argued

31. *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 6 (Va. Cir. Ct. 2000).

32. *See* OKLA. STAT. tit. 12, § 1443.1 (2008) (the statute's limited range makes it practically inapplicable to cyber-SLAPPs).

33. *See* Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 325 (2008).

34. *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

35. *See* Reno v. ACLU, 521 U.S. 844 (1997).

36. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001); Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999); Krinsky v. Doe 6, 159 Cal. App. 4th 1154 (Cal. Ct. App. 2008); Doe v. Cahill, 884 A.2d 451 (Del. 2005); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *America Online*, 52 Va. Cir. 26.

37. *See* cases cited *supra* note 36.

38. OKLA. STAT. tit. 12, § 1443.1. For a detailed analysis of this statutory section, see Laura Long, Note, *Slapping Around the First Amendment: An Analysis of Oklahoma's Anti-SLAPP Statute and its Implications on the Right to Petition*, 60 OKLA. L. REV. 419, 430-38 (2007).

39. *See Krinsky*, 159 Cal. App. 4th at 1171 (discussing the requirements of notice and a prima facie case).

40. *See infra* Part IV.B.

41. *See* Miguel E. Larios, *ePublius: Anonymous Speech Rights Online*, 37 RUTGERS L. REC. 36, 37 (2010).

for its ratification under the pseudonym Publius in the Federalist Papers.[42] The Supreme Court has consistently held that the First Amendment protects the right to speak anonymously.[43] In *Talley v. California*, the Court examined the constitutionality of a Los Angeles city ordinance that prohibited the distribution of any handbills under any circumstances without giving the true name of the person who wrote or produced the bill.[44] In holding that the ordinance unconstitutionally abridged freedom of speech, the Court noted that anonymity has been used throughout history "for the most constructive purposes"[45] and that anonymous pamphlets "have played an important role in the progress of mankind."[46] Anonymous speech is a constitutionally protected activity because, as the Court recognized, identification of an author and his subsequent "fear of reprisal" can "deter . . . peaceful discussions" and thereby restrict freedom of speech.[47]

In 1995, *McIntyre v. Ohio Elections Commission* presented the Supreme Court with the issue of whether an Ohio law abridged freedom of speech by prohibiting the anonymous distribution of campaign literature.[48] The law in question prohibited the publishing of any material advocating any issue without also publishing the name of the author in a conspicuous place.[49] In *McIntyre*, Margaret McIntyre distributed leaflets to attendees of a meeting to discuss a proposed school tax, which advocated that the attendees vote against the tax.[50] The leaflets were signed "Concerned Parents and Tax Payers."[51] Later, a school official who supported the tax filed a complaint with the Ohio Elections Commission, asserting that the leaflets violated the law because they did not identify the author.[52] In holding that the law violated the First Amendment, the Court pointed out that "anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent."[53] Although Ohio had argued that the law was a valid attempt to prevent fraudulent and libelous statements[54] and to inform the electorate,[55] the Court found the prohibition on all anonymous pamphleteering too broad to serve those objectives.[56] While recognizing that the state does have an interest in preventing fraud and libel, especially during an election,[57] the Court balanced the state's interest with the individual's interest in free expression by recognizing that "our society accords greater weight to the value of free speech than to the dangers of its misuse."[58]

42. *See generally* Gregory E. Maggs, *A Concise Guide to the Federalist Papers as a Source of the Original Meaning of the United States Constitution*, 87 B.U. L. REV. 801 (2007).

43. Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 205 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 65 (1960).

44. *Talley*, 362 U.S. at 61.

45. *Id.* at 65.

46. *Id.* at 64.

47. *Id.* at 65.

48. *McIntyre*, 514 U.S. at 336.

49. OHIO REV. CODE ANN. § 3599.09(A) (1988), *invalidated by McIntyre*, 514 U.S. 334.

50. *McIntyre*, 514 U.S. at 337.

51. *Id.*

52. *Id.* at 338.

53. *Id.* at 357.

54. *Id.* at 348.

55. *Id.*

56. *Id.* at 351.

57. *See id.*

58. *Id.* at 357.

The most recent U.S. Supreme Court decision vindicating the right to anonymous speech is the 1999 case *Buckley v. American Constitutional Law Foundation*, which focused on the restrictions that three Colorado statutes placed on circulators of initiative-petitions.[59] Colorado allows its citizens to make laws directly by placing initiatives on election ballots.[60] The laws in question in this case required an individual who circulated a petition in favor of a given initiative to be a registered voter[61] and to wear an identification badge showing his or her name.[62] A third statute required that the backers of the initiative produce a report containing the names and addresses of paid circulators.[63] The Supreme Court affirmed the Tenth Circuit's judgment that all three statutes violated the First Amendment right to free speech.[64]

The Court placed weight on the testimony at trial from several organizers as to the effect that the identification requirement had on participation.[65] Testimony from one organizer stated that the badge requirement "limited the number of people willing to work" as circulators.[66] Others testified that people were not willing to work as circulators if they had to wear identification badges because "it [made] them afraid" and they were reluctant to face "recrimination and retaliation."[67] In holding the identification requirement unconstitutional, the Court found that the restraint on speech was "more severe than was the restraint in *McIntyre*"[68] and that forcing circulators to identify themselves "discourages participation in the petition circulation process."[69]

Discovery of an anonymous defendant's identity in a cyber SLAPP case defeats the same principles that these cases upheld.[70] The Court's recognition in both *Talley* and *Buckley* that fear of reprisal can produce a chilling effect on freedom of expression[71] is exactly the principle that should protect cyber SLAPP defendants. In order to assure the greatest possible participation in the public process, it is necessary to protect the individual's right to participate anonymously.[72] This is no less true with regard to participation on the Internet than it is with regard to participation in an election issue or a ballot initiative.[73] As in *McIntyre*, where there is no suggestion that "[speech is] false, misleading, or libelous,"[74] Internet users should feel free to exercise their rights to anonymous speech without fearing that they will later be identified.

---

59. Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 186 (1999).
60. *Id.*
61. COLO. REV. STAT. § 1-40-112(1) (1998), *invalidated by Buckley*, 525 U.S. 182.
62. COLO. REV. STAT. § 1-40-112(2) (1998), *invalidated by Buckley*, 525 U.S. 182.
63. COLO. REV. STAT. § 1-40-121 (1998), *invalidated by Buckley*, 525 U.S. 182.
64. *Buckley*, 525 U.S. at 187.
65. *Id.* at 198.
66. *Id.*
67. *Id.*
68. *Id.* at 199.
69. *Id.* at 200.
70. *See* Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1162 (Cal. Ct. App. 2008) (recognizing that "[t]he use of a pseudonymous screen name offers a safe outlet for the user to . . . express unorthodox political views . . . without fear of intimidation or reprisal").
71. *See* Talley v. California, 362 U.S. 60, 65 (1960); *Buckley*, 525 U.S. at 198-200.
72. *See Talley*, 362 U.S. at 64.
73. *See* ACLU v. Miller, 977 F. Supp. 1228, 1230-31 (N.D. Ga. 1997) (listing the reasons people may have to participate online anonymously).
74. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 337 (1995).

B. The Right to Speak Anonymously Online

As the cases above demonstrated, it is well established that the First Amendment's protection of free of speech extends to the right to speak anonymously,[75] but whether that protection extends to speaking online was not always clear. As Internet use became more widespread in the 1990's,[76] the U.S. Supreme Court addressed for the first time the extent of First Amendment protections that the new medium would enjoy in *Reno v. ACLU*.[77]

In *Reno*, the issue before the court was the constitutionality of two provisions of the Communications Decency Act of 1996,[78] by which lawmakers intended to protect minors from "indecent" and "patently offensive" online communications.[79] Section 223(a) of the Act prohibited the "knowing transmission of obscene or indecent messages to any recipient under 18 years of age,"[80] while section 223(d) prohibited transmitting such materials "in a manner that is available to a person under 18 years of age."[81] The American Civil Liberties Union ("ACLU"), joined by nineteen other plaintiffs,[82] challenged the constitutionality of the provisions on the grounds that they were overbroad.[83] In affirming the district court's holding that the statute was unconstitutional,[84] the Court distinguished the Internet as a medium from the broadcast media.[85] The "invasive,"[86] one-way nature of the broadcast media is such that the court has recognized that it may be subject to "special justifications for regulation . . . that are not applicable to other speakers."[87] By contrast, the Internet does not share this invasive nature; a user must take "a series of affirmative steps"[88] to access any given Internet communication. Therefore, the Court found that, unlike the broadcast media, with respect to the Internet there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[89]

After *Reno*, the Internet medium can fairly be regarded as analogous to the print media with respect to First Amendment protections and limitations on speech.[90] As shown in *ACLU v. Miller*,[91] the protection of anonymous speech through the Internet

75. *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); *McIntyre*, 514 U.S. 334; *Talley*, 362 U.S. 60.

76. *See* Reno v. ACLU, 521 U.S. 844, 850 (1997) (detailing the growth of Internet use between 1981 and 1996).

77. *Reno*, 521 U.S. 844.

78. 47 U.S.C. § 223(a)(1)(B), 223(d) (1994 ed. Supp. II), *invalidated by Reno*, 521 U.S. at 885.

79. *Reno*, 521 U.S. at 849.

80. *Id.* at 859.

81. *Id.*

82. *Id.* at 861.

83. *Id.*

84. *Id.* at 885.

85. *Id.* at 868.

86. *Id.* at 869 (internal quotation marks omitted).

87. *Id.* at 868.

88. *Id.* at 867.

89. *Id.* at 870.

90. Protections of speech through print media under the First Amendment are outside the scope of this comment. *See generally* Khaldoun Shobaki, Note, *Speech Restraints for Converged Media*, 52 UCLA L. REV. 333, 342 (2004).

91. ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997).

medium is no exception.[92] In *Miller*, the ACLU filed a lawsuit that asked the court to enjoin the state of Georgia from enforcing a statute that made it a crime for "any person . . . to transmit any data through a computer network . . . if such data . . . falsely [identifies] the person."[93] The ACLU argued that the statute unconstitutionally restricted the "right to communicate anonymously and pseudonymously over the Internet,"[94] and that the broad language of the act "allows for selective prosecution of persons communicating about controversial topics."[95]

The court granted the plaintiffs' motion for a preliminary injunction, holding that the plaintiffs were likely to succeed on their claims that the statute was overbroad and unconstitutionally vague.[96] It recognized that although the purpose of the statute was to prevent fraud,[97] the statute's wide range could "sweep[] innocent, protected speech within its scope."[98] The protected speech to which the court referred includes "the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy,"[99] all of which are "legitimate and important reasons for concealing"[100] one's identity online.

III. STATE ANTI-SLAPP LAWS AND THEIR APPLICATION TO CYBER-SLAPP CASES

A. State Anti-SLAPP Laws

As Part II shows, anonymous online speech is a constitutionally protected activity[101] subject only to the limitations imposed on speech through print media, such as the limitation on protection of libelous or defamatory speech.[102] Society traditionally places greater weight on the benefits derived from free speech than the detriments that may result from the exercise thereof.[103] Many states have codified this principle by enacting anti-SLAPP statutes to protect the legitimate exercise of First Amendment rights from the chilling effects of strategic, retaliatory litigation.[104] Anti-SLAPP statutes have proven to be an effective means of preventing such litigation, and in some cases courts have applied those statutes to protect online speech.[105]

Courts have likely applied California's anti-SLAPP statute more often than that of any other state.[106] It was enacted in 1992 to respond to a "disturbing increase"[107] in

92. *See id.* at 1235.
93. GA. CODE ANN. § 16-9-93.1 (West 1996), *invalidated by Miller*, 977 F. Supp. at 1235.
94. *Miller*, 977 F. Supp. at 1230.
95. *Id.* at 1231.
96. *Id.* at 1232.
97. *Id.*
98. *Id.*
99. *Id.* at 1233.
100. *Id.* at 1234.
101. *Miller*, 977 F. Supp. 1228.
102. *See supra* note 90.
103. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).
104. *See* sources cited *supra* note 16.
105. *See* Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d. 1261 (C.D. Cal. 2001).
106. During the time this article was written, a Westlaw search revealed 2,302 notes of decisions for CAL. CIV. PROC. CODE § 425.16.
107. CAL. CIV. PROC. CODE § 425.16 (West 2009).

litigation aimed at chilling legitimate speech, and courts have applied it to cyber-SLAPP cases.[108] The statute provides that any cause of action initiated against a defendant due to his exercise of the "right of petition" or right to "free speech . . . in connection with a public issue" is "subject to a special motion to strike," unless the plaintiff can show a likelihood that he will prevail on the claim.[109] In considering the motion in the context of a defamation claim, a California court must first determine whether the defendant spoke in connection with a public issue,[110] and then consider the pleadings and any affidavits to determine the plaintiff's likelihood of success.[111]

For the cyber-SLAPP defendant wishing to remain anonymous, the critical provision of California Civil Procedure section 425.16 is the special motion to strike, the filing of which initiates a stay on all discovery proceedings until the court rules on the motion.[112] If the defendant files a special motion to strike early enough, a stay on discovery precludes the plaintiff from gaining the defendant's identifying information via a subpoena to the defendant's ISP.[113]

Aside from California and Oklahoma, twenty-five other states have anti-SLAPP statutes.[114] Of those, eleven states have provisions similar to California that require the defendant to speak on an issue of public concern before invoking the protection of the statutes.[115] Eleven states also allow the defendant to file a special motion to strike or a motion to dismiss,[116] but of those eleven, only eight provide for a stay of discovery.[117] Subject to varying conditions, all eleven states that allow a special motion to strike or dismiss shift the burden to the plaintiff to prove that his action has a substantial basis in law in order to save his case.[118]

---

108. *Global Telemedia*, 132 F. Supp. 2d. 1261.

109. CAL. CIV. PROC. CODE § 425.16(b)(1) (West 2009).

110. *See* D.C. v. R.R., 106 Cal. Rptr. 3d 399 (Cal. Ct. App. 2010) (denying defendant's motion to strike made under CAL. CIV. PROC. CODE § 425.16 on the grounds that threatening speech made online by one student to another was not protected speech and not in connection with a public issue).

111. CAL. CIV. PROC. CODE § 425.16(b)(2) (West 2009).

112. § 425.16(g).

113. *See* Corcept Therapeutics, Inc. v. Rothschild, 339 F. App'x 789, 790 (9th Cir. 2009) (where defendant did not file special motion to strike in time and plaintiff obtained his IP address through discovery).

114. *See* sources cited *supra* note 16.

115. DEL. CODE ANN. tit. 10, §§ 8136 – 8138 (West 2009); GA. CODE ANN. § 9-11-11.1 (West 2008); HAW. REV. STAT. §§ 634F-1 to 634F-4 (2002); IND. CODE §§ 34-7-7-1 to 34-7-7-10 (2008); LA. CODE CIV. PROC. ANN. art. 971 (2008); ME. REV. STAT. ANN. tit. 14, § 556 (2008); MASS. GEN. LAWS. ANN. ch. 231, § 59H (West 2008); MINN. STAT. §§ 554.01 – 554.05 (2008); NEB. REV. STAT. §§ 25-21, 241 – 25-21, 246 (2008); N.Y. C.P.L.R. 3211(g); 3212(h) (MCKINNEY 2009); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (2008).

116. DEL. CODE ANN. tit. 10, §§ 8136 – 8138 (West 2009); GA. CODE ANN. § 9-11-11.1 (West 2008); HAW. REV. STAT. §§ 634F-1 to 634F-4 (2002); IND. CODE §§ 34-7-7-1 to 34-7-7-10 (2008); LA. CODE CIV. PROC. ANN. art. 971 (2008); ME. REV. STAT. ANN. tit. 14, § 556 (2008); MASS. GEN. LAWS. ANN. ch. 231, § 59H (West 2008); MINN. STAT. §§ 554.01 – 554.05 (2008); NEB. REV. STAT. §§ 25-21, 241 – 25-21, 246 (2008); N.Y. C.P.L.R. 3211(g); 3212(h) (MCKINNEY 2009); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (2008).

117. GA. CODE ANN. § 9-11-11.1 (West 2008); HAW. REV. STAT. §§ 634F-1 to 634F-4 (2002); IND. CODE §§ 34-7-7-1 to 34-7-7-10 (2008); LA. CODE CIV. PROC. ANN. art. 971 (2008); ME. REV. STAT. ANN. tit. 14, § 556 (2008); MASS. GEN. LAWS. ANN. ch. 231, § 59H (West 2008); MINN. STAT. §§ 554.01 – 554.05 (2008); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (2008).

118. DEL. CODE ANN. tit. 10, §§ 8136 – 8138 (West 2009); GA. CODE ANN. § 9-11-11.1 (West 2008); HAW. REV. STAT. §§ 634F-1 to 634F-4 (2002); IND. CODE §§ 34-7-7-1 to 34-7-7-10 (2008); LA. CODE CIV. PROC. ANN. art. 971 (2008); ME. REV. STAT. ANN. tit. 14, § 556 (2008); MASS. GEN. LAWS. ANN. ch. 231, § 59H (West 2008); MINN. STAT. §§ 554.01 – 554.05 (2008); NEB. REV. STAT. §§ 25-21, 241 – 25-21, 246 (2008); N.Y. C.P.L.R. 3211(g); 3212(h) (MCKINNEY 2009); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (2008).

While Oklahoma does not have a statute that is truly analogous to the anti-SLAPP statutes described above, the Oklahoma statute that is considered to be an anti-SLAPP statute[119] is section 1443.1 of Title 12.[120] Section 1443.1 was passed in 1981, seven years before Canan and Pring identified SLAPPs as a growing problem.[121] On its face, the entire scope of the statute is to classify certain types of communications as privileged and then to exempt those communications from a single cause of action, libel.[122] Under the statute, privileged communications include those made either in a judicial or legislative proceeding, or during the discharge of an official duty.[123] Also privileged are any fair and true reports of judicial or legislative proceedings or any other proceeding authorized by law, any opinions of those proceedings, and any criticism of the official acts of a public officer, with the exception of falsely imputing a crime to that officer.[124]

Though the statute's scope is limited, it reflects a principle recognized long ago by the Oklahoma Supreme Court that "[e]very one has a right to comment on matters of public interest and concern"[125] so long as they do so in "good faith"[126] and "without malice."[127] To those ends, Oklahoma courts have interpreted section 1443.1 liberally; for example, for the purpose of the statutory privilege, a "fair and true report"[128] might contain "[s]light inaccuracies of expression . . . provided that the defamatory charge is true in substance."[129] A statement made in a "judicial proceeding"[130] includes a statement made in an affidavit.[131] A newspaper editorial that criticized a group's efforts to argue for tort reform was held privileged[132] as "any other proceeding authorized by law."[133] The statutory privilege does not protect false statements, but statements of opinion are protected because they "are incapable of being false."[134]

In addition to the statutory privilege, Oklahoma also recognizes a common law fair comment defense to a defamation action that applies to comments made on issues of "public concern," based on "true facts," which are the "actual opinion of the speaker."[135]

---

119. *See* Long, *supra* note 38, at 431; Geoffrey Paul Huling, *Tired of Being Slapped Around: States Take Action Against Lawsuits Designed to Intimidate and Harass*, 25 RUTGERS L.J. 401, 418 n.76 (1994); Shaun B. Spencer, *Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493, 500 n.61 (2001); Rebecca Ariel Hoffberg, *The Special Motion Requirements of the Massachusetts Anti-SLAPP Statute: A Real Slap in the Face for Traditional Civil Practice and Procedure*, 16 B.U. PUB. INT. L.J. 97, 127 n.192 (2006).

120. OKLA. STAT. tit. 12, § 1443.1 (2008).

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. Holway v. World Pub. Co., 44 P.2d 881, 886 (Okla. 1935) (citing Bearce v. Bass, 34 A. 411, 412, 413 (Me. 1896)).

126. *Id.*

127. *Id.*

128. OKLA. STAT. tit. 12, § 1443.1 (2008).

129. McGhee v. Newspaper Holdings, Inc., 115 P.3d 896, 898 (Okla. Civ. App. 2005) (quotations and citations omitted).

130. OKLA. STAT. tit. 12, § 1443.1 (2008).

131. Joplin v. Sw. Bell Tel. Co., 753 F.2d 808, 810 (10th Cir. 1983).

132. Gaylord Entm't Co. v. Thompson, 958 P.2d 128, 146 (Okla. 1998).

133. OKLA. STAT. tit. 12, § 1443.1 (2008).

134. Hennessee v. Mathis, 737 P.2d 958, 962 (Okla. Civ. App. 1987).

135. Sturgeon v. Retherford Publ'ns, Inc., 987 P.2d 1218, 1225 n.4 (Okla. Civ. App. 1999).

While Oklahoma courts have often invoked both the statutory and common law privileges to protect a defendant's legitimate speech, these protections are inadequate for the cyber-SLAPP defendant due to the substantial harm[136] that is inflicted when the defendant is wrongly stripped of his anonymity. The statutory protection is also inadequate in that it only applies to libel causes of action, while cyber-SLAPPs have been filed under several different causes of action, including business torts and conspiracy.[137] Instead of providing the defendant with procedural shortcuts to identify meritless suits, shifting the burden to the plaintiff, and preserving the defendant's anonymity, Oklahoma law would force the defendant to incur the time and expense of defending the meritless suit in court.[138]

B. Anti-SLAPP Laws Applied to Cyber-SLAPP Cases

One example of an anti-SLAPP statute applied to a cyber-SLAPP case is *Global Telemedia International, Inc. v. Doe 1*.[139] In *Global Telemedia*, Global Telemedia International, Inc. ("GTMI") sued Defendants King and Reader over allegedly libelous comments that each defendant made about GTMI on an Internet message board.[140] King and Reader argued that GTMI brought the case against them in an attempt to "intimidate and silence" critics of the company,[141] and King and Reader brought separate motions to strike under California's anti-SLAPP statute, California Civil Procedure section 425.16.[142]

The state of California passed section 425.16 with an eye towards encouraging "participation in matters of public significance"[143] and preventing such participation from being "chilled through abuse of the judicial process."[144] Section 425.16 gives a defendant the ability to file a special motion to strike when the lawsuit against him comes as a result of his "free speech 'in connection with a public issue.'"[145] Under section 425.16, if the defendant can show that his speech was indeed in connection with a public issue, "the burden shifts to [the] plaintiff to [either] demonstrate a probability of success,"[146] or have his lawsuit dismissed.

Section 425.16(e) provides that free speech exercised in connection with a public issue includes "any written or oral statement or writing made in a place open to the

136. Doe v. Cahill, 884 A.2d 451, 459 (Del. 2005).

137. *See* Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1159 (Cal. Ct. App. 2008) (where the plaintiff's causes of action included "intentional interference with a 'contractual and/or business employment relationship' . . . libel, . . . fraud, improper professional conduct, and criminal activity to plaintiff"); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 759-60 (N.J. Super. Ct. App. Div. 2001) (where the plaintiff's causes of action included "breach of employment or confidentiality agreements; breach of fiduciary duty; misappropriation of trade secrets; interference with a prospective business advantage; defamation; and other causes of action").

138. *See* Erin Malia Lum, Note, *Hawai'i's Response to Strategic Litigation Against Public Participation and the Protection of Citizens' Right to Petition the Government*, 24 U. HAW. L. REV. 411, 416 (2001) (describing the cost of defending meritless lawsuits).

139. Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d. 1261 (C.D. Cal. 2001).

140. *Id.* at 1264.

141. *Id.*

142. *Id.*

143. *Id.* (quoting CAL. CIV. PROC. CODE § 425.16(a)).

144. *Id.* (quoting CAL. CIV. PROC. CODE § 425.16(a)).

145. *Id.* at 1265.

146. *Id.* at 1266.

public or a public forum in connection with an issue of public interest."[147] Here, GTMI was a publicly traded company with nearly 18,000 investors.[148] The message board in question had over 30,000 messages devoted to GTMI.[149] Both of these facts weighed heavily on the court's determination that King and Reader's postings were in fact in connection with a public issue.[150]

After the court determined that the comments at issue were in connection with a public issue, the burden shifted to GTMI to show a probability of success on the merits.[151] Ultimately, the court agreed with King and Reader's argument that the comments in question "were opinion[s]."[152] The court also agreed with King and Reader's argument that "opinions are not actionable under either trade libel or libel per se,"[153] and granted both King's and Reader's motions to strike.[154]

C. *When Should John Doe be Unmasked?*

Courts in other jurisdictions have gained experience in handling cyber SLAPP cases.[155] The central issue in each of the following cases is how the court should balance the defendant's First Amendment interest in anonymous online speech with the plaintiff's interest in identifying the defendant so that he may seek relief for an alleged wrong.[156] Courts have struggled with this issue since 1999, when the court in *Columbia Insurance Co. v. seescandy.com* established one of the first standards for unmasking an anonymous online defendant.[157] In *seescandy.com*, Columbia Insurance Company ("Columbia") sued the unidentified defendants who registered the seescandy.com domain name for various claims relating to trademark infringement.[158] The record showed that the names and contact information for the owners of seescandy.com had changed several times in the months preceding the lawsuit.[159] Due to its inability to determine the true owner of the allegedly infringing website and its inability to serve that person with the complaint, Columbia sought the court's permission to determine the plaintiff's identity through discovery.[160]

The court issued a four-part standard to govern whether the pre-service use of discovery to determine the defendant's identity is appropriate.[161] It held that Columbia

147. *Id.* at 1265.
148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.* at 1266.
152. *Id.*
153. *Id.*
154. *Id.* at 1266-67, 1270.
155. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001); Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); Krinsky v. Doe 6, 159 Cal. App. 4th 1154 (Cal. Ct. App. 2008); Doe v. Cahill, 884 A.2d 451 (Del. 2005); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26 (Va. Cir. Ct. 2000).
156. *See, e.g.*, *2TheMart.com Inc.*, 140 F. Supp. 2d 1088; *Cahill*, 884 A.2d 451.
157. *seescandy.com*, 185 F.R.D. 573.
158. *Id.* at 576.
159. *Id.*
160. *Id.* at 577.
161. *Id.* at 578-80.

must: (1) provide enough information for the court to determine that the defendant is a person who can be served in federal court;[162] (2) identify all steps previously taken to locate the defendant;[163] (3) demonstrate that its suit could withstand a motion to dismiss;[164] and (4) establish that there is a reasonable likelihood that the information sought through discovery will lead to identifying the defendant.[165] While the court recognized that "[p]eople who have committed no wrong should be able to participate online"[166] without fear of having their identities exposed through frivolous lawsuits, the motion to dismiss standard that it gave for identifying defendants would prove to be weak in comparison to the standard applied by later courts.[167]

The court in *in re Subpoena Duces Tecum to America Online, Inc.* gave another early standard for identifying anonymous defendants.[168] In *America Online*, Anonymous Publicly Traded Company ("ATPC") filed suit against five John Does.[169] ATPC alleged that the Does were current or former employees who made defamatory statements about ATPC and released confidential information about ATPC in an America Online ("AOL") chat room.[170] Four of the Does were AOL subscribers, and ATPC obtained a court order compelling AOL to "produce any and all documents from which the identity of the four AOL subscribers could be ascertained."[171] AOL was unwilling to comply with the subpoena out of concern for its customers' First Amendment rights, and asked the court to quash the subpoena.[172]

In denying AOL's motion to quash, the court developed a two-part test for whether to force an ISP to identify its customer: (1) whether, on the basis of evidence or pleadings, the party requesting the subpoena demonstrates a good faith basis for his claim; and (2) whether the "subpoenaed identity information is centrally needed to advance that claim."[173] While both the *America Online* court and the *seescandy.com* court expressed concern about the strength of the plaintiff's claim and the relevance of the information sought,[174] the *America Online* court required only that a plaintiff have a good faith basis for his claim before the court would force identification of the defendant.[175] A later court rejected the *American Online* court's good faith standard, which is an even weaker standard than the *seescandy.com* court's motion to dismiss standard, because it "offers no practical, reliable way to determine the plaintiff's good

162. *Id.* at 578.
163. *Id.* at 579.
164. *Id.*
165. *Id.* at 580.
166. *Id.* at 578.
167. *See, e.g.*, Doe v. Cahill, 884 A.2d 451, 461 (Del. 2005) (promulgating a stronger, summary judgment standard).
168. *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26 (Va. Cir. Ct. 2000).
169. *Id.* at 1.
170. *Id.*
171. *Id.*
172. *Id.* at 2.
173. *Id.* at 8.
174. Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); *America Online, Inc.*, 52 Va. Cir. 26.
175. *America Online, Inc.*, 52 Va. Cir. 26, at 8.

faith and leaves the speaker with little protection."[176]

In 2001, the U.S. District Court for the Western District of Washington issued an often-cited order in *Doe v. 2TheMart.com*.[177] This matter came before the Washington court on Doe's motion to quash a subpoena stemming from 2TheMart.com's ("TMRT") defense of a shareholder's derivative suit in the Central District of California.[178] The two issues for the Washington court to decide were: first, whether Doe could proceed under a pseudonym,[179] and second, whether the court should grant Doe's motion to quash TMRT's subpoena.[180] TMRT served a subpoena to Seattle-based Internet service provider InfoSpace, Inc. that sought identifying information for twenty-three anonymous participants, including Doe, who participated on an Internet message board operated by InfoSpace.[181]

TMRT issued the subpoena as part of its defense to the California shareholder's derivative suit.[182] In response to the plaintiff-shareholders' allegation that fraud on the market caused TMRT's falling stock price,[183] one of TMRT's affirmative defenses was that it was not the cause of the falling stock price.[184] TMRT's theory was that Doe and the other anonymous users of the message board caused the stock price to fall through their postings.[185] In support of that defense, it issued the subpoena at issue to InfoSpace.[186]

InfoSpace operated a website called Silicon Investor, which was a collection of online message boards on which users could discuss various publicly traded companies, including TMRT.[187] The TMRT message board contained nearly 1,500 messages posted by users using pseudonyms, some of which were highly critical of the company.[188] TMRT's subpoena to InfoSpace sought "among other things, '[a]ll identifying information and documents, including, but not limited to, computerized or computer stored records and logs, [email], and postings on your online message boards,'" which would be used to identify Doe and the other twenty-two users.[189] TMRT subpoenaed this information on the theory that the twenty-three users were the cause of TMRT's falling stock price because the users "'manipulated the [TMRT] stock price using the Silicon Investor message boards.'"[190] When InfoSpace received the subpoena, it notified the users that their identifying information was the subject of a subpoena, which gave Doe time to file a motion to quash.[191]

176. Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1167 (Cal. Ct. App. 2008).
177. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1089 (W.D. Wa. 2001).
178. *Id.* at 1089.
179. *Id.*
180. *Id.*
181. *Id.* at 1090.
182. *See id.* at 1089.
183. *Id.* at 1097.
184. *Id.* at 1090.
185. *Id.* at 1097.
186. *Id.* at 1090.
187. *Id.*
188. *Id.*
189. *Id.* (quoting TMRT's subpoena to InfoSpace).
190. *Id.* at 1095 (quoting TMRT's complaint).
191. *Id.* at 1091.

The court recognized that the constitutional implications of TMRT's request required careful balancing of the broad rules of discovery against Internet users' right to communicate anonymously.[192] The court developed a four-factor test for determining whether to grant a motion to quash a civil subpoena when the subpoena seeks to uncover the identity of an anonymous Internet user who is not a party to the underlying litigation.[193] The court gives weight to each factor "as the court determines is appropriate under the circumstances of each case."[194] First, the court looks at whether the subpoena was "issued in good faith."[195] Second, whether "the information sought relates to a core claim or defense."[196] Third, whether the "identifying information is directly and materially relevant to that claim or defense."[197] Finally, whether "information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[198]

In applying the four-factor test to Doe's motion, the court found that although the subpoena was not necessarily brought in bad faith,[199] the information the subpoena sought did not "relate to a core defense."[200] Further, since TMRT did not know the identities of Doe and the other users when they posted their messages, Doe and the other users' identifying information could not have related to TMRT's core defense that the users posted the messages in order to manipulate TMRT's stock price.[201] The court also weighed the fourth factor in favor of Doe, finding that TMRT did not show that it could not obtain the information it needed to establish its defense from another source.[202] Since each of the four factors weighed against TMRT, the court granted Doe's motion to quash the subpoena.[203]

2TheMart.com remains an influential case for courts confronting the delicate balance of interests presented in cyber SLAPP cases.[204] Several state and federal courts have applied, in whole or in part, the *2TheMart.com* court's standard for whether to quash a civil subpoena when it seeks to identify an anonymous non-party Internet user.[205] As the court pointed out in *2TheMart.com*, the standard for identifying a non-party Internet user must be more stringent than the standard for identifying an Internet user who is a party to the underlying litigation.[206]

In 2005, the Supreme Court of Delaware issued standards for identifying an

192. *See id.* at 1093.
193. *Id.* at 1095.
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.* at 1096.
200. *Id.*
201. *Id.* at 1097.
202. *Id.*
203. *Id.* at 1098.
204. *See 2TheMart.com Inc.*, 140 F. Supp. 2d 1088.
205. *See, e.g.*, Enterline v. Pocono Med. Ctr., 751 F. Supp. 2d 782, 787 (M.D. Pa. 2008); Sedersten v. Taylor, No. 09-3031-CV-S-GAF, 2009 WL 4802567, at *2 (W.D. Mo. Dec. 9, 2009).
206. *2TheMart.com Inc.*, 140 F. Supp. 2d at 1095.

anonymous defendant through discovery in *Doe v. Cahill*.[207] In *Cahill*, an anonymous Internet user, Doe, posted comments on a blog that were critical of Patrick Cahill, a city councilman in Smyrna, Delaware, where both parties resided.[208] Specifically, two of Doe's comments were the subject of the ensuing action for defamation and invasion of privacy,[209] and both comments related to Cahill's performance in his capacity as a city councilman.[210] In order to identify Doe, Cahill deposed the blog's owner and found that Comcast owned the IP address associated with Doe's comments.[211] The court's explanation of an Internet user's IP address, as it relates to his anonymity, is instructive.

> An IP address is an electronic number that specifically identifies a particular computer using the internet. IP addresses are often owned by internet service providers who then assign them to subscribers when they use the internet. These addresses are unique and assigned to only one ISP subscriber at a time. Thus, if the ISP knows the time and the date that postings were made from a specific IP address, it can determine the identity of its subscriber.[212]

After Cahill obtained Doe's IP address, he secured a court order that required Comcast to reveal Doe's identity.[213] At the time, there was a federal statute[214] in place that prohibited an ISP from disclosing its subscribers "personally identifiable information"[215] unless the disclosure was made "pursuant to a court order"[216] and the subscriber was "notified of such order."[217] In this case, Comcast complied with the statute by notifying Doe of the court order, which gave Doe time to file a motion for a protective order to preserve his anonymity.[218] The trial court denied Doe's motion while accepting Cahill's argument that he should only have to demonstrate a "good faith basis" for his defamation claim before Comcast should be required to identify Doe.[219] The Supreme Court of Delaware accepted Doe's interlocutory appeal of the trial court's order.[220] The issue on appeal was whether the trial court's good faith standard

207. Doe v. Cahill, 884 A.2d 451 (Del. 2005).
208. *Id.* at 454.
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.* at 454-55.
213. *Id.* at 455.
214. 47 U.S.C.A. § 551(c) (West 2001). *But see In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D) Directed to Cablevision Sys. Corp., 158 F. Supp. 2d 644, 648 (D. Md. 2001) (holding that the provision of 47 U.S.C.A § 551 requiring a cable company to notify a subscriber that the cable company was ordered by a court to release the subscriber's personally identifiable information was "implicitly repealed" when Congress subsequently passed an inconsistent provision in The Electronic Communications Privacy Act, which specifically bars a cable company from providing such notice to subscribers provided certain conditions are met). *See also* The Electronic Communications Privacy Act, 18 U.S.C.A § 2705(b) (West 2001).
215. 47 U.S.C.A. § 551(c) (West 2001).
216. *Id.* § 551(c)(2)(B).
217. *Id.*
218. Doe v. Cahill, 884 A.2d 451, 455 (Del. 2005).
219. Cahill v. Jon Doe-Number One, 879 A.2d 943, 945 (Del. Super. Ct. 2005).
220. *Cahill*, 884 A.2d at 455.

"appropriately balance[d] [Doe's] right to speak anonymously against [Cahill's] right to protect his reputation."[221]

The good faith standard applied by the trial court is a low standard.[222] To satisfy the trial court's good faith standard, a plaintiff must establish only a "good faith basis" for his claim, that the information he seeks is "directly and materially related to [the] claim," and that the information cannot be "obtained from any other source."[223] Applying such a standard could result in a defendant's loss of anonymity when the plaintiff's defamation claim is "not very strong."[224] To allow defendants to be unmasked so easily "discourage[s] debate on important issues of public concern,"[225] and the *Cahill* court worried that the standard would "chill potential posters from exercising their First Amendment right to speak anonymously."[226]

The Supreme Court of Delaware reversed the trial court's denial of Doe's motion for protective order with instructions to dismiss the plaintiff's claim with prejudice.[227] In doing so, it adopted a summary judgment standard for unmasking an anonymous defendant.[228] The summary judgment standard that the court adopted was a modified version of a standard created by a New Jersey appellate court in *Dendrite International Inc. v. Doe*.[229]

The facts in *Dendrite* were very similar to the facts in *Cahill*, except that the target of the *Dendrite* defendant's anonymous online criticism was a corporation rather than a city councilman.[230] The *Dendrite* court required that, in order to force identification of an anonymous defendant, a plaintiff first must attempt to notify the defendant that his identifying information is being subpoenaed, and thereby provide him a chance to oppose the subpoena.[231] The plaintiff must then "set forth the exact statements" made by the defendant and present a "prima facie cause of action" for defamation.[232] Before allowing the plaintiff to proceed, the court must weigh the "strength of the prima facie case presented" against the defendant's "First Amendment right of anonymous free speech."[233]

After discussing the *Dendrite* standard, the *Cahill* court adopted a modified standard for unmasking anonymous defendants.[234] Under *Cahill*, a plaintiff who wishes to identify an anonymous defendant must attempt to "notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure."[235] When a case arises in the context of the Internet, this notification provision also requires a plaintiff to

221. *Id.* at 456.
222. *See id.* at 457.
223. *Id.* at 455.
224. *Id.* at 457.
225. *Id.*
226. *Id.*
227. *Id.* at 468.
228. *Id.* at 457.
229. *Id.* at 461.
230. Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 761 (N.J. Super. Ct. App. Div. 2001).
231. *Id.* at 760.
232. *Id.*
233. *Id.* at 760-61.
234. Doe v. Cahill, 884 A.2d 451, 461 (Del. 2005).
235. *Id.* at 460.

post a message in the same place as the allegedly defamatory comments that notifies the "anonymous defendant of the plaintiff's discovery request."[236] Second, the plaintiff must satisfy the summary judgment standard[237] by submitting "sufficient evidence to establish a prima facie case for each essential element of the claim in question."[238]

Underlying the *Cahill* court's decision to adopt a more stringent standard than the one applied by the trial court was a recognition of the potential value of anonymous online speech.[239] Such speech allows the speaker to speak to a large and diverse audience[240] while knowing that her ideas will be evaluated "on her words alone."[241] Not only is this form of speech constitutionally protected, but it has a positive effect on public debate[242] and in some cases "can become the modern equivalent of political pamphleteering."[243]

The 2008 California case *Krinsky v. Doe 6* considered each of the above standards when it decided whether a subpoena to Yahoo! should be quashed. Krinsky, who was the president of a Florida company, alleged that Doe 6 and others made defamatory statements about Krinsky on a Yahoo! message board, and served a subpoena to Yahoo! that requested identifying information about the defendants.[244] Yahoo! notified the defendants of the subpoena, which gave the defendants time to file a motion to quash on First Amendment grounds.[245] The trial court denied the motion to quash and Doe 6 appealed.[246]

In trying to balance the interests of both parties, the court provided a thorough discussion of each different standard from above.[247] It immediately foreclosed the possibility of applying the *America Online* standard because it provides such a "low threshold for disclosure."[248] While the *Dendrite* standard applies "greater scrutiny [to] the plaintiff's cause of action,"[249] the *Krinsky* court declined to expressly adopt the *Dendrite* standard.[250] The court agreed with the *Cahill* court that the *Dendrite* requirement that the defendant himself notify the plaintiff of the pending subpoena was "unrealistic" due to the possibility that the forum on which the comment was made "may no longer exist . . . by the time the plaintiff brings suit."[251] However, the *Krinsky* court

236. *Id.* at 461.
237. *Id.*
238. *Id.* at 463 (emphasis omitted) (quoting Colgain v. Oy-Partek Ab (In re Asbestos Litig.), 799 A.2d 1151, 1152 (Del. 2002).
239. *See id.* at 455.
240. *Id.* (quoting Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 895 (2000)).
241. *Id.* at 456 (citation and internal quotation marks omitted).
242. *See id.*
243. *Id.*
244. Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1159-60 (Cal. Ct. App. 2008).
245. *Id.* at 1160.
246. *Id.* at 1160-61.
247. *Id.* at 1167.
248. *Id.*
249. *Id.*
250. *Id.* at 1171.
251. *Id.*

agreed with *Cahill* and *Dendrite* in two key aspects[252] that can guide Oklahoma's approach.

IV. THE EMERGING JUDICIAL CONSENSUS

A. Two Requirements

The *Krinsky*, *Cahill*, and *Dendrite* standards overlap in two areas that are critical for cyber-SLAPP defendants who wish to remain anonymous; all three courts would require the plaintiff to make a prima facie case and to give notice to the defendant before the courts would allow the plaintiff to determine the defendant's identity through discovery.[253] The requirement that the plaintiff make a prima facie case is essential to protecting the defendant from the dangers of SLAPPs, because it "ensures that the plaintiff is not merely seeking to harass or embarrass the speaker or stifle legitimate criticism."[254] In the context of a cyber-SLAPP, where the allegedly tortious statement is posted on the Internet, this requirement does not pose an undue burden on the plaintiff because "[the] plaintiff knows the statement that was made and [can] produce[] evidence of its falsity and the effect it had on her."[255]

While the *Krinsky* court rejected[256] the *Dendrite* court's requirement that the *plaintiff* notify the defendant that his identifying information has been subpoenaed, *Dendrite* and *Cahill* both require that the plaintiff notify the defendant of the pending subpoena.[257] This point is sometimes rendered moot; if the ISP has taken it upon itself to notify its customers of the pending subpoena, there is no need to require the plaintiff to notify the defendant.[258] Whether it is the plaintiff or the ISP that notifies the defendant, and whether it is the courts or the legislature that imposes the requirement, the defendant's opportunity to receive notice of the subpoena and the chance to respond effectively defines the scope of the defendant's right to anonymous online speech. Several Oklahoma ISPs have been proactive in this area by notifying their customers of pending subpoenas,[259] but others have not.[260] With no law that requires an ISP to notify

252. *Id.* at 1172.

253. *Id.*; Doe v. Cahill, 884 A.2d 451, 457 (Del. 2005); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 769 (N.J. Super. Ct. App. Div. 2001).

254. *Krinsky*, 159 Cal. App. 4th at 1171.

255. *Id.* at 1172.

256. *See id.* at 1171 (in *Krinsky*, notification by the plaintiff was a moot point because the defendant had already been notified of the pending subpoena by his ISP).

257. *Cahill*, 884 A.2d at 461; *Dendrite*, 775 A.2d at 760.

258. *See Krinsky*, 159 Cal. App. 4th at 1171 (where the defendant's ISP notified him of the subpoena); *Cahill*, 884 A.2d at 461 (where the defendant's ISP notified him of the subpoena due to federal law in place at the time); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1091 (W.D. Wash. 2001) (where the defendant's ISP notified him of the subpoena).

259. *See AOL Civil Subpoena Policy*, AOL LEGAL, http://legal.web.aol.com/aol/aolpol/civilsubpoena.html (last visited Nov. 28, 2010); *EarthLink Civil Subpoena Policy*, EARTHLINK (Sep. 23, 2008), http://www.earthlink.net/about/policies/civil.faces (last visited Nov. 28, 2010); *MegaPath Subpoena Response Policy*, MEGAPATH, INC., http://www.megapath.com/pdfs/subpoena_policy.pdf (last visited Nov. 28, 2010); *PeoplePC Civil Subpoena Policy*, PEOPLEPC ONLINE (July 1, 2009), http://www.peoplepc.com/about/index.faces?popupId=privacy (last visited Nov. 28, 2010).

260. *See AT&T Privacy Policy*, AT&T, http://www.att.com/Common/about_us/privacy_policy/print_policy.html (last visited Nov. 28, 2010); *Hughes Subscriber Privacy Policy*, HUGHESNET.COM (Oct. 1, 2008), http://legal.hughesnet.com/SubscriberPolicies.cfm

its customers of civil subpoenas[261] and no judicial standard that requires the plaintiff to do so, an Oklahoma defendant's right to anonymous online speech goes only so far as the privacy policy of his ISP, in that the ISP may or may not identify the defendant without his knowledge.[262]

B. The ISP's Effect on the Right to Anonymous Speech

A brief survey of the privacy policies of a few of Oklahoma's ISPs shows how the identifying information of Oklahoma residents is subject to different standards for disclosure pursuant to a civil subpoena, depending on who provides their Internet service. For example, Cox Communications' ("Cox") privacy policy states that it "reserve[s] the right to disclose Your Information . . . [that] is necessary to . . . comply with the law."[263] It further states that Cox "[cannot] assume any duty to notify [its customers] of receipt of any legal requests."[264]

Similarly, AT&T's privacy policy states that it may "provide Personal Information to . . . third parties . . . without your consent . . . [t]o comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements."[265] AT&T's policy makes no mention of giving its customers notice that their identifying information was subpoenaed, with the single exception that when the information was "collected from AT&T U-verse TV subscribers as a result of the subscriber's use of AT&T's U-verse TV service," AT&T will provide "prior notice to the subscriber."[266] Presumably, this exception would not apply to an AT&T customer who only uses the company as an ISP and does not subscribe to its TV service.

NetZero and Juno give themselves broad latitude for disclosing their customers identifying information.[267] NetZero's policy states that it may, "without notice" share your personal information "to law enforcement or government agencies in response to subpoenas, court orders, or other legal process (including civil and criminal) or otherwise as required by law" without making any mention of notifying its customers of the existence of a order, or giving them the opportunity to respond before complying.[268] Juno's policy is simply to share an individual's "personal Identifier Information" when such information is "required or requested by law, regulation or order authority."[269] Like

(last visited Nov. 28, 2010); *Legal: Subscriber Privacy Policy*, WILDBLUE (July 11, 2005), http://get.wildblue.com/privacy-policy.html (last visited Nov. 28, 2010); *Privacy Policy*, NETZERO (Mar. 19, 2012), http://www.netzero.net/start/landing.do?page=www/legal/privacy (last visited Mar. 31, 2012); *Privacy Statement for Juno Members*, JUNO, http://www.juno.com/start/landing.do?page=www/legal/privacy (last visited Nov. 28, 2010); *Your Privacy Rights as a Cox Customer and Related Information*, COX (Nov. 18, 2011), http://ww2.cox.com/aboutus/tulsa/policies/annual-privacy-notice.cox#law (last visited Mar. 31, 2012).

261. Federal law may prevent an ISP from notifying its customer of a subpoena when the subpoena is sought by a government entity. *See, e.g.*, 18 U.S.C.A. § 2703(b)(1)(A) (West 2009) (allowing governmental entities to obtain subscriber information from ISPs without notice to the subscriber, provided certain conditions are met).

262. *See supra* notes 259-60.

263. *Your Privacy Rights as a Cox Customer and Related Information*, *supra* note 260.

264. *Id.*

265. *AT&T Privacy Policy*, *supra* note 260.

266. *Id.*

267. *See Privacy Policy*, *supra* note 260; *Privacy Statement for Juno Members*, *supra* note 260.

268. *Privacy Policy*, *supra* note 260.

269. *Privacy Statement for Juno Members*, *supra* note 260.

NetZero, Juno's policy makes no mention of notifying its customers of the existence of the subpoena or giving them the opportunity to respond.[270]

On the other hand, EarthLink's Civil Subpoena policy gives customers notice and the opportunity to respond to a civil subpoena before EarthLink discloses the customer's identifying information.[271] According to the policy, before EarthLink responds to a civil subpoena it will "notify the customer of the civil request for their information."[272] Further, EarthLink gives its customers a chance to respond to the subpoena by providing that, "[i]n non-emergency situations, EarthLink will generally respond after approximately fifteen . . . days, unless the customer presents EarthLink with notice of having filed a motion to quash the subpoena or having sought similar protection from a court."[273]

Like EarthLink, America Online's ("AOL") Civil Subpoena Policy gives its customers notice of a civil subpoena and the opportunity to respond. Under the policy, when AOL receives a subpoena seeking identifying information, it "promptly send[s] notification to the account holder whose information is sought."[274] The policy further states that AOL will not provide the requested information for approximately ten days after notification, "so that the account holder whose information is sought will have adequate opportunity to take legal action."[275] Similar to EarthLink and AOL, MegaPath has a Subpoena Response Policy that also gives its customers "notice of the subpoena's existence to allow the customer the opportunity to quash the subpoena."[276]

A resident of Tulsa or Oklahoma City may be able to choose from any of the ISPs above, but some rural areas are underserved or unserved.[277] For some rural areas, the best option for Internet access may be through a satellite ISP, like HughesNet and WildBlue.[278] HughesNet's Subscriber Privacy Policy states that it may "use or disclose information about you, including your Personal Information, . . . [i]n response to a subpoena, court order, or other legal process," with no provision for notice or an opportunity to respond.[279] While WildBlue's policy states that it will "make every reasonable effort to protect subscriber privacy," there is no guarantee in the policy that its reasonable efforts include giving customers notice and the opportunity to respond.[280]

The result of having an inadequate anti-SLAPP statute is that the scopes of Oklahoma Internet users' First Amendment rights to anonymous online speech vary

---

270. *Id.*

271. *EarthLink Civil Subpoena Policy*, *supra* note 259.

272. *Id.*

273. *Id.; see also PeoplePC Civil Subpoena Policy*, *supra* note 259 (People PC, which is a subsidiary of EarthLink, has the same policy).

274. *AOL Civil Subpoena Policy*, *supra* note 259.

275. *Id.*

276. *MegaPath Subpoena Response Policy*, *supra* note 259.

277. *See* Press Release, State of Oklahoma, Oklahoma Broadband Mapping Initiative Seeks Oklahomans Assistance at http://BroadbandMapping.OK.gov (June 23, 2010), *available at* http://www.ok.gov/about/Media_Center/Press/2010_-_Oklahoma_Broadband_Mapping_Initiative_Seeks_Oklahomans_Assistance.html.

278. *See* Special to the E-E, *WildBlue Satellite Internet Available*, EXAMINER-ENTERPRISE (Mar. 17, 2007, 11:02 PM) (on file with author).

279. *Hughes Subscriber Privacy Policy*, *supra* note 260.

280. *See Legal: Subscriber Privacy Policy*, *supra* note 260.

widely depending on which company provides their service.[281] While the lack of Oklahoma cases may indicate that this right is not often invoked, that fact does not diminish the right's importance.[282]

Many Oklahomans post anonymous reviews of businesses on websites, but they might not realize that their words could cause them to be unmasked and sued.[283] In Chicago, a doctor sued a former patient over anonymous criticisms she posted on Yelp.com and Citysearch.com.[284] If the patient was an Oklahoman, his right to remain anonymous could depend on his choice of ISP, which could also depend on where he happens to live. A Tulsa defendant who uses EarthLink would have the opportunity to ask a court to quash a subpoena to his ISP seeking identifying information because his ISP would notify him of the subpoena.[285] Oklahoma City defendants who use Cox[286] and rural defendants who use a satellite provider do not have guarantees from their ISPs that they will be notified of a subpoena.[287] This disparity effectively creates different levels of rights to anonymous online speech and is impermissible under a Virginia law that deserves consideration by the Oklahoma legislature.[288]

C. *The Consensus Codified*

Virginia Code Annotated section 8.01-407.1 was passed in 2002[289] and it "[provides] a procedure governing certain subpoenas in civil proceedings where it is alleged that an anonymous individual has engaged in tortious Internet communications."[290] Under the statute, a plaintiff seeking to identify an anonymous defendant via a subpoena to the defendant's ISP must first file evidentiary material with the court that shows that the plaintiff has a "legitimate, good faith basis" to believe the communication was tortious.[291] A copy of the evidentiary material and the subpoena must be sent to the defendant's ISP,[292] which must attempt to notify the defendant of the subpoena within five days of receipt, by both email and at his last known address.[293] The statute allows "any interested person [to] file a detailed written objection, motion to

281. *See Your Privacy Rights as a Cox Customer and Related Information*, *supra* note 260 (noting Cox does not assume the duty to notify customers of any legal requests). *But see AOL Civil Subpoena Policy*, *supra* note 259 (stating AOL notifies customers of pending legal requests).

282. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (stating "[w]hatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry").

283. *See* Mark Saxenmeyer, *Chicago Doctor Sues Patients Over Yelp, Citysearch Reviews*, FOX CHICAGO NEWS (Nov. 15, 2010, 9:44 AM), http://www.myfoxchicago.com/dpp/news/investigative/dr-jay-pensler-yelp-citysearch-reviews-20101115 (updated Nov. 16, 2010, 6:45 AM).

284. *Id.*

285. *See EarthLink Civil Subpoena Policy*, *supra* note 259; *AOL Civil Subpoena Policy*, *supra* note 259.

286. *See Your Privacy Rights as a Cox Customer and Related Information*, *supra* note 260.

287. *See Hughes Subscriber Privacy Policy*, *supra* note 260; *Legal: Subscriber Privacy Policy*, *supra* note 260.

288. VA. CODE ANN. § 8.01-407.1 (2010).

289. *Id.*

290. VA B. Summ., 2002 H.B. 819.

291. § 8.01-407.1.

292. *Id.*

293. *Id.*

quash, or motion for protective order"[294] which states reasons for "denying the disclosure sought in the subpoena."[295] The filing of such an objection, motion to quash, or motion for protective order prevents the defendant's ISP from complying with the subpoena until the court rules on the objection or motion.[296]

Although the statute's good faith standard is a lower standard than the *Krinsky*, *Cahill*, and *Dendrite* prima facie case requirement,[297] the statute expressly adopts the *Krinsky*, *Cahill*, and *Dendrite* requirement of notice of the subpoena and the opportunity to respond.[298] A codification of these two principles will enable Oklahoma to avoid the chilling effects of cyber-SLAPP suits by giving defendants the tools to preserve their anonymity. Perhaps most importantly, codifying these two principles also ends the disparity between different Oklahomans' rights to anonymous online speech.[299]

Oklahoma recently launched the Oklahoma Broadband Initiative, whose goal is to expand access to broadband services throughout the state.[300] With it, the state recognizes that "[a]ccess to technology for the provision of enhanced education, healthcare and emergency services plus job growth and development, have long been identified as one of the most essential tools a community must have to expand its economic potential and community livability."[301] Access to technology is also an essential tool that an individual must have to exercise his right to free speech.[302] In order to allow Oklahomans to fully exercise that right, the Oklahoma legislature should enact a statute that embodies the principles deduced by the *Krinsky*, *Cahill*, and *Dendrite* courts and codified by the state of Virginia.[303]

V. CONCLUSION

Cyber-SLAPP suits that are filed in order to unmask anonymous defendants and chill the right to free speech are antithetical to Oklahoma values. Anonymous speech has a long history of use throughout the country.[304] The Supreme Court has long recognized that the right to anonymous speech is protected under the First Amendment,[305] as is the right to online speech.[306] The ever-increasing prevalence of Internet use brings the potential for increasing infringements on online rights. This potential came to fruition in

294. *Id.*

295. *Id.*

296. *Id.*

297. *See supra* note 253 and accompanying text (explaining the *Krinsky*, *Cahill*, and *Dendrite* prima facie case requirement).

298. *See supra* note 253 and accompanying text.

299. *See supra* notes 263-81 and accompanying text (explaining how different privacy policies effectively create different levels of rights to anonymous online speech).

300. *About the Oklahoma Broadband Initiative*, ST. OKLAHOMA, http://www.ok.gov/broadband/ (last visited Nov. 28, 2010).

301. *Id.*

302. *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 427 (2009).

303. *See supra* notes 255-60 and accompanying text (explaining the two principles deduced by the *Krinsky*, *Cahill*, and *Dendrite* courts); VA. CODE ANN. § 8.01-407.1 (2010).

304. *See* Maggs, *supra* note 42.

305. *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

306. *See supra* notes 89-100 and accompanying text.

the line of cases from *seescandy.com* to *Krinsky*, which pitted the defendant's right to anonymous speech against the plaintiff's interest in obtaining relief for allegedly tortious statements.[307] As courts decided these cases, a judicial consensus emerged that strikes a balance between both parties' interests by recognizing two important principles: before an anonymous defendant can be unmasked, a plaintiff must show a firm basis for his allegations and the defendant must be provided with the opportunity to respond to a subpoena seeking his identifying information.[308]

Current Oklahoma law does not provide protection for cyber-SLAPP defendants. In the absence of a statute that defines procedures for handling civil subpoenas seeking to identify anonymous online speakers, an anonymous Oklahoma defendant can be identified at the discretion of his ISP.[309] While some ISPs voluntarily notify their customers when a third party seeks to identify them, others are not willing to assume that duty.[310] The variance among the policies of different ISPs creates an inequality among Oklahomans' rights to anonymous online speech.

As Oklahoma moves to increase Internet access throughout the state, it should also move to increase online rights. By forcing the plaintiff to show that his case has merit and by giving the defendant the opportunity to object to a request for his identity before his identity is exposed, Virginia avoids the chilling effects of cyber-SLAPP suits and ensures that its Internet users enjoy the full extent of their First Amendment rights.[311] The Oklahoma legislature should follow Virginia's lead and enact a statute that affords Oklahomans the same protections.

—Sean Kilian*

307. *See supra* Part III.C.

308. *See supra* Part IV.A.

309. *See supra* Part IV.B.

310. *See AOL Civil Subpoena Policy*, *supra* note 259; *EarthLink Civil Subpoena Policy*, *supra* note 259. *But see Your Privacy Rights as a Cox Customer and Related Information*, *supra* note 260.

311. VA. CODE ANN. § 8.01-407.1 (2010).

* The author would like to thank his family for their invaluable support during the writing of this article, and the members of Tulsa Law Review, for their hard work in preparing this article for publication.