CONSTITUTIONAL DRAG RACE: ANONYMOUS ONLINE SPEECH AFTER *DIGITAL MUSIC NEWS V. SUPERIOR COURT*

Thaddeus Houston†

Courts typically cite the First Amendment as the justification for the right to speak anonymously on the internet.[1] But in *Digital Music News v. Superior Court of Los Angeles, Escape Media Group* ("*Digital Music News*"), a California appeals court reversed an order compelling the identification of an anonymous speaker because the discovery order violated the online commenter's constitutional right to privacy provided by the California Constitution.[2] In finding for the first time that the right to anonymous online speech is grounded both in the First Amendment and the privacy clause of California's Constitution, the court recognized a novel legal theory that may prove to be influential in other states whose constitutions include a right to privacy, or in anonymous speech cases more generally.

Commentators immediately hailed the expanded right to privacy recognized by the *Digital Music News* court as the most significant aspect of the court's decision.[3] The court held that one who posts anonymous online comments has protection for those acts grounded in both the First

---

† J.D. Candidate, 2016, University of California, Berkeley, School of Law. The author served as a legal intern at the Electronic Frontier Foundation in the summer of 2014 and as a legal assistant at Google from 2010 to 2013, but no longer represents or is affiliated with either of these organizations. All views and errors are the author's alone.

1. *See, e.g.*, Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1091–92 (W.D. Wash. 2001); Highfields Capital Mgmt. v. Doe, 385 F. Supp. 2d 969, 974–75 (N.D. Cal. 2005); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237–38 (Cal. Ct. App. 2008); *see also* Alison Frankel, *California Finds 'Right to Privacy' for Anonymous Online Commenters*, REUTERS BLOG (May 16, 2014), http://blogs.reuters.com/alison-frankel/2014/05/16/california-finds-right-to-privacy-for-anonymous-online-commenters/.

2. The court also cited the First Amendment of the federal Constitution as a source of the commenter's right to anonymous online speech. *See* Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 809 (May 14, 2014); *see also* Paul Alan Levy, *California Court of Appeals Creates New Argument for Protecting Anonymous Online Speech*, PUB. CITIZEN CONSUMER LAW & POL'Y BLOG (May 14, 2014), http://pubcit.typepad.com/clpblog/2014/05/california-court-of-appeals-creates-new-argument-for-protecting-anonymous-online-speech.html.

3. *See* Frankel, *supra* note 1.

Amendment to the U.S. Constitution as well as the broader right to privacy protected by the 'privacy clause' of the California Constitution.[4] *Digital Music News* is one of the most recent California judicial opinions that provides a broad, but not unlimited, right to speak online anonymously—perhaps granting the broadest right yet. That said, the Ninth Circuit recently issued a decision in *Doe v. Harris*, where it struck down a California law that required sex offenders to register each new online account with the police because it could not survive First Amendment scrutiny and placed too great a burden on the sex offenders' First Amendment right to anonymous online speech.[5] Aspects of this decision will also be discussed throughout this Note.

This Note explores the history of the right to anonymous online speech and the privacy clause of the California Constitution, provides a more detailed analysis of *Digital Music News*, and attempts to place the reasoning contained in the *Digital Music News* decision in the larger context of a discussion between courts, scholars, and lawyers about how best to weigh the costs and benefits of anonymous online speech. Part I introduces anonymous online speech, describing its role on the internet and how that role has changed as the social uses of the internet have changed. It next explains what anonymity means in the context of online communication, and how it differs from pseudonymity. It then introduces some of the harmful behavior enabled by anonymous online communication and some of the solutions to these harmful behaviors proposed by legal scholars.

Parts II and III provide the legal background to the *Digital Music News* court's decision, discussed in detail in Part IV. Part II explains that anonymous online speech is afforded First Amendment protection and describes the framework that state and federal courts use to balance the constitutional right to anonymous online speech against the rights of the parties harmed by the speech; otherwise, the way that courts handle some of the issues described in Part I. Part III explores the privacy clause of the California Constitution, including where it came from and what problems it aimed to solve, how it should be interpreted in new contexts, and how it can be used in litigation. Part IV provides detailed analysis of *Digital Music News*, explaining the facts of the case, how the court reached its decision, and how the case fits into the larger conversation about anonymous online speech—considering that it combines the First

4. *Digital Music News*, 171 Cal. Rptr. 3d at 809–10.
5. Doe v. Harris, 772 F.3d 563, 583 (9th Cir. 2014).

Amendment and the privacy clause of the California Constitution in a novel way.

Part V expands on an aspect of the court's reasoning in *Digital Music News*: that courts ultimately want to protect the individual's ability to create her own identity when they attempt to determine whether an individual's identity should be disclosed to someone harmed by her anonymous online comment. The Part does this by highlighting the language that courts have used in "John Doe" and other anonymous online speech cases, the language used in urging the amendment of the privacy clause to the California Constitution, and the language used in *Digital Music News*. Part V also uses the example of a hypothetical legal challenge to Facebook's "Real Names" policy to show how all of these interests and concepts come together in a context familiar to today's internet users. Finally, Part V briefly restates the normative argument that "traceable pseudonymity" strikes the best balance between constitutionally-protected interests based on the First Amendment and the right to privacy on the one hand, and harm caused by anonymous online comments on the other.

I. ANONYMOUS ONLINE SPEECH

This Section explains what anonymous online speech is. It begins by briefly discussing the history of social uses of the internet, explaining some of the advantages that the internet offers to speakers and some of the social problems caused by those speakers' perception of anonymity. It next describes some solutions to these social problems proposed by legal scholars, in part to introduce the idea that civil society is engaged in a discussion about how best to balance the benefits of anonymous online speech against the problems it causes. Finally, this Section considers the differences between anonymity and pseudonymity.

A. ONLINE ANONYMITY AND PSEUDONYMITY FIRST FOUND TO SERVE NOBLE PURPOSES, LATER FOUND TO CAUSE PROBLEMS

The court's decision in *Digital Music News* is part of a larger judicial and scholarly conversation about the value of anonymous online speech. This discussion centers on a fundamental tension: on the one hand, anonymous online speech furthers constitutionally-protected liberty interests, but on the other hand, protection for anonymous online speech shields responsibility for bad and sometimes illegal conduct. When, in *Reno v. ACLU*, in 1997, the Supreme Court first considered the speech implications of the internet, it chose to highlight "electronic mail (e-mail), automatic mailing list services ('mail exploders,' sometimes referred to as 'listservs'), 'newsgroups,' 'chat rooms,' and the 'World Wide Web'" as the

uses of the internet relevant to the First Amendment.[6] The Web 1.0 internet[7] that the courts encountered when they began wrestling with online speech had "the advantage of allowing users, or 'posters,' to express themselves anonymously, by using 'screen names' traceable only through the hosts of the sites or their Internet service providers (ISPs)."[8]

Reno centered on the constitutionality of certain provisions of the Communications Decency Act of 1996 ("CDA").[9] While not specifically at issue in *Reno*, § 230(c) of the CDA operates in the background of this Note.[10] Section 230(c) of the CDA shields internet service providers ("ISPs"), like social networks or message boards, from liability for tortious comments posted by their users.[11] When an anonymous poster writes something harmful about a person in the United States, the transmitting ISP has no obligation to remove it upon request.[12] Instead, one must learn the identity of the poster by subpoenaing the ISP and then suing the poster if the ISP discloses—or is ordered to disclose—the poster's identity, or sue the poster directly, as an unknown "John Doe" defendant.[13]

A key feature of the earliest versions of online communications is that they enabled computer users to connect with others that shared similar interests; the offline identity of those posters was not essential for many of these virtual communities.[14] Web 1.0 communication technologies enabled internet speakers to communicate their views to many people simultaneously at low cost.[15] It was in this atmosphere that the Supreme

6. Reno v. ACLU, 521 U.S. 844, 851 (1997). Justice Stevens acknowledged that "[t]hese methods [of internet communication] are constantly evolving and difficult to categorize precisely." *Id.*

7. In this context, Web 1.0 refers to the first version of the social and commercial internet, which was characterized by the predominance of message boards, chat rooms, and GeoCities sites. Web 2.0, in contrast, generally means the internet as a social space dominated by social networks and blogs. *See generally* Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1320–25 (2009).

8. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 234 (Cal. Ct. App. 2008).

9. 47 U.S.C.A. §§ 223–230 (West 2014). Reno v. ACLU focused on § 223. *Reno v. ACLU*, 521 U.S. at 859–60.

10. 47 U.S.C.A. § 230(c)(1) (West 2014) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

11. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (recognizing that § 230(c) immunizes ISPs from tort-based lawsuits in the interest of protecting freedom of speech "in the new and burgeoning Internet medium.").

12. *See, e.g.*, *id.*

13. *See, e.g.*, *Krinsky*, 72 Cal. Rptr. 3d at 235 (explaining that plaintiff subpoenaed Yahoo to learn the identity of an anonymous poster of harmful comment).

14. *See* Gelman, *supra* note 7, at 1320–22.

15. Reno v. ACLU, 521 U.S. 844, 870 (1997).

Court welcomed the speech-enhancing possibilities of the internet, noting in *Reno*—the same decision that recognized the applicability of the First Amendment to the internet—that "[t]hrough 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."[16]

But courts since *Reno* have acknowledged the dangers inherent in inexpensive and relatively anonymous online speech.[17] Over the past decade, trolling,[18] cyberbullying,[19] and copyright infringement[20] have become common, with perceived poster anonymity undoubtedly a contributing factor. These unintended consequences can have serious adverse effects in the offline world.[21] Pseudonymous trolls also have persistent and troubling misogynistic tendencies.[22] One well-documented example of this disturbing phenomenon is the AutoAdmit controversy,

16. *Id.*

17. *See, e.g.*, Stanley Fish, *Anonymity and the Dark Side of the Internet*, N.Y. TIMES (Jan. 3, 2011), http://opinionator.blogs.nytimes.com/2011/01/03/anonymity-and-the-dark-side-of-the-Internet/?_php=true&_type=blogs&_r=0; Maria Konnikova, *The Psychology of Online Comments*, NEW YORKER (Oct. 23, 2013), http://www.newyorker.com/tech/elements/the-psychology-of-online-comments (citing research that shows comments on newspaper websites that allowed anonymous posting tended to be less civil than comments on newspaper websites that did not allow anonymous commenting).

18. Julie Zhuo, *Where Anonymity Breeds Contempt*, N.Y. TIMES, Nov. 30, 2010, at A31, *available at* http://www.nytimes.com/2010/11/30/opinion/30zhuo.html?scp=1&sq=Where%20Anonymity%20Breeds%20Contempt&st=cse (defining trolling as "the act of posting inflammatory, derogatory or provocative messages in public forums . . .").

19. Karen M. Bradshaw & Souvik Saha, *Academic Administrators and The Challenges of Social Networking Websites*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 140, 144–45 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011) (explaining how cyber-bullying can be more harmful than traditional bullying because it has "the potential to be more widely broadcast, to take place in groups rather than in individual capacities, and to occur without monitoring by educators and administrators.").

20. *See, e.g.*, *Sony BMG Music Entm't v. Tenenbaum*, 660 F.3d 487, 491–92 (1st Cir. 2011) (discussing legal campaign by record labels to identify and prosecute internet users who downloaded copyrighted music files using peer-to-peer file-sharing networks).

21. *See* Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES, Nov. 26, 2008, at A25, *available at* http://www.nytimes.com/2008/11/27/us/27myspace.html (reporting on the legal proceeding stemming from the first widely-reported suicide caused by cyber-bullying); *see also* Bryan H. Choi, *The Anonymous Internet*, 72 MD. L. REV. 501, 529 nn.111–113 (2013) (explaining the same phenomena with more examples than provided here).

22. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 65–66 (2009).

where two female Yale law students were the targets of online posts by pseudonymous online posters that included violent and sexual content.[23] Another more recent example is "Gamergate," where female members of the video-gaming community have suffered unjustified real-world consequences for speaking out on the role of women in the video game industry, beginning with waves of attacks by pseudonymous trolls.[24]

The emergence of Web 2.0 and the accompanying rise of social networking have complicated the context surrounding anonymous online speech in part because online social dynamics have changed since the Supreme Court contemplated the First Amendment value of "mail exploders."[25] Unlike Web 1.0, which emphasized connection over common interests, Web 2.0 emphasizes identity. Some of the most widely used social networks require users to provide their real name when they sign up (at least until recently).[26] Scholar and attorney Lauren Gelman has explained that social networks have become more popular than the message boards of Web 1.0 in part because they allow users "to connect with people they cannot identify or find in advance, such as high school friends."[27] Gelman argues that users of social networking services tend to overshare private information to take advantage of the "blurry edges" of their social networks: people that the users want to share and connect with, but have not identified at the moment they post new content.[28] This

23. *See* Doe 1 v. Individuals (AutoAdmit), 561 F. Supp. 2d 249, 251–52 (D. Conn. 2008) (providing background on the trolling); *see also* Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 364–68 (2008) (summarizing the AutoAdmit controversy).

24. *See generally* Kyle Wagner, *The Future of the Culture Wars Is Here, and It's Gamergate*, DEADSPIN (Oct. 14, 2014), http://deadspin.com/the-future-of-the-culture-wars-is-here-and-its-gamerga-1646145844 (explaining what Gamergate is and tracing the development of the scandal over time).

25. Reno v. ACLU, 521 U.S. 844, 870 (1997).

26. Until recently, Facebook required users to sign up using their real names. This policy was at least partially premised on the idea that requiring real names increases the quality of the content that users post by making users "more accountable" and making it easier to fight spam accounts. *See* Valeriya Safronova, *Drag Performers Fight Facebook's 'Real Name' Policy*, N.Y. TIMES (Sept. 24, 2014), http://www.nytimes.com/2014/09/25/fashion/drag-performers-fight-facebooks-real-name-policy.html?_r=0. Google also required users to provide their "real names" when it first launched its Google+ social networking service, a policy that it abandoned after about three years. *See* Rebecca MacKinnon & Hae-in Lim, *Google Plus Finally Gives Up on Its Ineffective, Dangerous Real-Name Policy*, SLATE (July 14, 2014), http://www.slate.com/blogs/future_tense/2014/07/17/google_plus_finally_ditches_its_ineffective_dangerous_real_name_policy.html.

27. Gelman, *supra* note 7, at 1326.

28. *Id.* at 1317–18.

tendency to overshare creates interesting problems that are outside the scope of this Note.[29]

The majority of internet users now spend significant time on closed social networks that encourage users to merge their offline and online identities.[30] The shift toward social networks has driven anonymous speakers from the social mainstream of the internet to what Professor Brian Leiter has called cyber cesspools: portions of the social internet where trolls predominate and the level of discussion is vulgar and immature.[31] Cyber cesspools tend to grow in the corners of the internet that still allow anonymous and pseudonymous speech.[32] They tend to attract a disproportionately high number of trolls relative to other inhabitants, perhaps because people seek out these corners of the internet to experience the cathartic effects of trolling.[33] The shift in the social mainstream of internet users to social networks—where users are linked to their offline identities—adds to the common impression that all anonymous online speakers are trolls. Scholarly proposals to solve problems like trolling tend to reflect this sentiment.[34] But the view that the internet can be fixed by removing its anonymous aspects is problematic because it undervalues the constitutionally protected liberty interests furthered by anonymous online speech.

---

29. *Id.* at 1327–28 (explaining that the purpose of social networks "is to capture the economic benefit of users' blurry-edged networks" by ensuring that their users share more information, and with a wider group of people, than they otherwise would).

30. *See* Maeve Duggan & Aaron Smith, *Social Media Update 2013*, PEW RES. INTERNET PROJECT (Dec. 30, 2013), http://www.pewInternet.org/2013/12/30/social-media-update-2013/.

31. Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 155, 155 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011).

32. *Id.* at 166.

33. *See* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 238 (Cal. Ct. App. 2008) (noting that, on the internet:

> Hyperbole and exaggeration are common, and 'venting' is at least as common as careful and considered argumentation. The fact that many Internet speakers employ online pseudonyms tends to heighten this sense that 'anything goes,' and some commentators have likened cyberspace to a frontier society free from the conventions and constraints that limit discourse in the real world.

Id. (quoting Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 863 (2000)).

34. *See generally* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011).

B. THE NATURE OF ANONYMITY ONLINE

Courts are receptive to anonymous speech because it "is a shield from the tyranny of the majority."[35] Anonymity serves one of the noble "purpose[s] behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society."[36] But as a practical matter, true anonymity in online postings is difficult and beyond the technical capability of most internet users.[37] While Tor and other anonymizing technologies can enable truly anonymous communication if used carefully[38]—without logging in to a social networking site or any other site that requires login credentials—most internet users are not familiar with these technologies.[39]

As a result, few internet users, and practically none of the internet users featured in the cases discussed in this Note, are actually anonymous—the link between their offline and online identities is instead held by a third party like their ISP, a social network, or an online message board operator.[40] Much of the litigation involving anonymous online speech has centered on developing standards that appropriately balance an internet user's right to speak anonymously against the opposing party's right to unmask them when they have committed a tortious act such as posting a defamatory statement.[41]

---

35. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

36. *Id.*

37. *Krinsky*, 72 Cal. Rptr. 3d at 237 (noting that, in most cases "no one is truly anonymous on the Internet, even with the use of a pseudonym. Yahoo! warns users of its message boards that their identities can be traced, and that it will reveal their identifying information when legally compelled to do so."); *accord* Highfields Capital Mgmt. v. Doe, 385 F. Supp. 2d 969, 973 (N.D. Cal. 2005) (highlighting that Yahoo reminds its users to "'[n]ever assume that you are anonymous and cannot be identified by your posts.'").

38. *See* Nassim Nazemi, *DMCA §512 Safe Harbor for Anonymity Networks Amid a Cyber-Democratic Storm: Lessons from the 2009 Iranian Uprising*, 106 NW. U. L. REV. 855, 869 (2012) ("As information travels from one Tor operator's tunnel to another, the software adds a new 'layer' of encryption . . . such that no operator in the circuit can ever trace the transmission back more than one layer, protecting the Tor user who initiated it.").

39. *See* Mark Graham & Stefano De Sabbata, *The Anonymous Internet*, INFO. GEOGRAPHIES OXFORD INTERNET INST., http://geography.oii.ox.ac.uk/?page=tor (last visited Oct. 23, 2014) (noting that Tor has approximately 750,000 daily users; approximately 126,000 of those users are from the United States).

40. *See, e.g.*, *Krinsky*, 72 Cal. Rptr. 3d at 237.

41. These standards are discussed more extensively later in this Note. *See infra* Part II.B. *See also, e.g.*, Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (discussing the importance of finding an appropriate standard that balances the

C. POTENTIAL SOLUTIONS TO THE ISSUES POSED BY ANONYMITY ONLINE

Scholars have responded to the apparent injustice in particular instances of trolling and cyberbullying—or other tortious acts committed via online comments—primarily by proposing schemes to limit online anonymity, de-emphasizing the value provided by the anonymous internet.[42] Professor Daniel Solove has proposed rewriting CDA § 230(c) to require ISPs to exercise more editorial control over their platforms by imposing liability on the ISPs for content posted by their users.[43] Professor Danielle Keats Citron has called for a new law or set of laws that would provide remedies to those harmed by anonymous online communications.[44] Professor Martha C. Nussbaum has suggested that all internet users should be required to identify themselves—using their offline identities—before being able to post anything.[45] And Professor Saul Levmore has predicted that the law will settle on requiring ISPs to turn over identifying information to users harmed by online comments as long as the user seeking the other user's identity could clear some modest hurdle to weed out baseless requests.[46]

Scholar Bryan Choi has also proposed that we act to limit the anonymous aspect of the internet, but he instead advocates that anonymity should be offered as "bait" to regulators to preserve the generativity of the internet.[47] Choi agrees with Professor Jonathan Zittrain, who has posited

rights of an internet user to speak anonymously against the rights of a party harmed by those comments in unmasking the anonymous speaker by serving a subpoena on an ISP).

42. *See generally* THE OFFENSIVE INTERNET, *SUPRA* note 34.

43. Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 15, 23–28 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011) (proposing reform of CDA § 230).

44. Danielle Keats Citron, *Civil Rights in Our Information Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 31, 38–39 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011) (advocating for a comprehensive legal solution based on criminal law, tort, and civil rights law to the problem of anonymous online mobs and their disproportionate impact on marginalized communities).

45. Martha C. Nussbaum, *Objectification and Internet Misogyny*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 68, 85 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011) (emphasizing the importance of requiring identification as a condition of posting online to solve the often misogynistic harm inflicted by anonymous mobs on women).

46. Saul Levmore, *The Internet's Anonymity Problem*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 31, 57 (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011).

47. Choi, *supra* note 21, at 503.

that generativity is the key to the internet's success.[48] Zittrain, in turn, describes generativity as "a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences."[49] Choi's proposal is similar to the proposals discussed *supra*[50] in that he recommends that regulation should be permitted to remove anonymous communication from the internet, but provides a different justification for eliminating anonymity from the internet. Choi concedes that anonymity has some benefits, but argues that generativity creates more value than anonymity.[51] Assuming that increased regulation of the internet is inevitable—and assuming that generativity can be 'picked' over anonymity if the internet has to give up something—Choi proposes that anonymity should be sacrificed to allow generativity to continue to flourish.[52] Choi says this can be done by forcing identification upon internet users so that those harmed by their speech can seek legal remedies against them directly, obviating the need to impose more stringent requirements on online intermediaries—such as re-writing § 230(c) of the Communications Decency Act—that would likely have responded to more stringent requirements by restricting the output of tools that enable the internet's generativity.[53]

Still other scholars continue to recognize the value of anonymous online speech and have proposed solutions to the harm caused by anonymous online comments that preserve the ability to communicate anonymously online up to a point—where the illegality of a comment outweighs the benefits it provides. Professor Tal Zarsky, for example, argues that "traceable pseudonymity" strikes the best compromise "between our desire to use the rich personal information landscape now available, our privacy needs, and the ability of governments to track down lawbreakers."[54] In a system of traceable pseudonymity, intermediaries keep a record of who the person using their service is.[55] The user of the service

48. *Id.* ("In a set of recent publications, Jonathan Zittrain has posited that the key to the Internet's success is 'generativity' . . . .").

49. Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1980 (2006).

50. *See generally* THE OFFENSIVE INTERNET, *supra* note 34.

51. Choi, *supra* note 21, at 503.

52. *Id.* at 566.

53. *Id.* at 535–37.

54. Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1040 (2004).

55. *Id.* at 1031–32 (explaining the concept of traceable pseudonymity and how it would work in practice).

can correspond pseudonymously with others, but her identity can be obtained from one of the few intermediaries that provide access to online communication if she engages in illegal activity.[56] The connection between online and offline identities enabled by traceable pseudonymity also provides the benefit of allowing people to conduct business pseudonymously, as the intermediary can store financial information on the user's behalf.[57] So in a system of traceable pseudonymity, the user remains pseudonymous from the perspective of most other users, but her identity can be disclosed when necessary. Similarly, others have advocated for the adoption of "Identity 2.0" technology,[58] which would preserve pseudonymity to some degree, but would tie all pseudonyms to an internet user's offline identity through a single portal; her offline identity could be accessed if the user was engaged in illegal activity.[59]

D. THE RELATIONSHIP BETWEEN ANONYMITY AND PSEUDONYMITY

Providing anonymous online speakers with appropriate rights is difficult both because they can almost always be identified (and are therefore not really anonymous) and because many anonymous online speakers use a pseudonym that allows them to develop an online identity that is separate and distinct from their offline identity, sometimes over the course of many years.[60] The harm caused by unmasking the speaker behind a pseudonym that has been developed over time can be much greater than the harm caused by unmasking an online speaker with an identity that is used once and then discarded.[61] Many courts have conflated anonymity and pseudonymity in the past,[62] but the difference is best understood by

56. *Id.*

57. *Id.*

58. Jeffrey Aresty, *Digital Identity and the Lawyer's Role in Furthering Trusted Online Communities*, 38 U. TOL. L. REV. 137, 153 (2006) (explaining Identity 2.0, which is essentially an adoption of traceable pseudonymity but with a single login point—meaning that only one intermediary would have all of a particular user's identity information—and where the user retains ultimate control over all of that personal information).

59. *Id.* at 161–62.

60. *See, e.g.*, Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1090 (W.D. Wash. 2001) (mentioning that some internet users choose to consistently post online comments using the same pseudonym).

61. *See, e.g.*, Rebecca MacKinnon & Hae-in Lim, *Google Plus Finally Gives Up on Its Ineffective, Dangerous Real-Name Policy*, SLATE (July 14, 2014), http://www.slate.com/blogs/future_tense/2014/07/17/google_plus_finally_ditches_its_ineffective_dangerous_real_name_policy.html (explaining the importance of pseudonyms).

62. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342–43 (1995) (noting that "[p]ersecuted groups and sects from time to time throughout history have

considering that, "by serving as storehouses of reputational capital, pseudonymous entities add value to social interaction in a way that anonymous speech does not."[63] The price to the unmasked user who has cultivated a pseudonym is higher than the unmasking cost to a merely 'anonymous' user who has not built up social capital through the development of her online identity over time.[64]

In *Digital Music News*, the court held that the anonymous user identified only as Visitor had a privacy interest grounded both in the California Constitution and the right to anonymous speech provided by the First Amendment.[65] Visitor, who wrote a controversial comment about music streaming service Grooveshark, used the default name that Digital Music News ("DMN") appears to assign to visitors to its website—not a consciously developed pseudonym. The intentionally developed online pseudonym is more representative of the dignity and identity interests promoted by allowing anonymous online speech.[66] So the judicial tendency to conflate anonymity and pseudonymity will be helpful if an internet user subject to litigation related to content written under a pseudonym wants to rely on the reasoning in *Digital Music News* in making her case.[67]

Like many courts, the remainder of this Note will seem to conflate anonymity and pseudonymity, referring to online speakers using pseudonyms as "anonymous speakers" or "anonymous internet users."

been able to criticize oppressive practices and laws either anonymously or not at all," but using as an example the arguments advanced in favor of the ratification of the Constitution in the Federalist Papers, which were published under pseudonyms such as "An American Citizen."). *But see Anonymity*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/anonymity (last visited Sept. 22, 2014) (succinctly summarizing the difference between the two in noting that some "people choose to speak using pseudonyms (assumed names) or anonymously (no name at all).").

63. David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 160 (1996).

64. *See* Danah Boyd, *"Real Names" Policies Are an Abuse of Power*, APOPHENIA (Aug. 4, 2011), http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html (explaining the identity value of pseudonyms and listing reasons why people use pseudonyms).

65. *See* Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 810 (May 14, 2014).

66. *See* J. Bryan Lowder, *Why Is Facebook Cracking Down on Drag Names?*, SLATE (Sept. 9, 2014), http://www.slate.com/blogs/outward/2014/09/12/facebook_vs_drag_queens_why_is_facebook_cracking_down_on_drag_names.html (including commentary by users of pseudonyms noting that "although our names might not be our 'legal' birth names, they are still an integral part of our identities, both personally and to our communities.").

67. *See, e.g.*, Post, *Pooling Intellectual Capital*, *supra* note 63, at 160.

While technically incorrect, this conflation is often necessary because it reflects the amalgam of the two concepts by the courts. For example, Doe 6 in *Krinsky* is referred to as "the anonymous defendant" though he used the pseudonym "Senor-Pinche-Wey" in all of his contentious online postings.[68] In some of the internet speech cases discussed below, the speakers used pseudonyms.[69] Other cases involved "anonymous" speakers because the implicated speaker selected the default name assigned by the website they chose to comment on. But in all of the cases discussed below, the online speakers are not anonymous in the sense that it is impossible to determine who they are; rather, they are anonymous in that is not immediately apparent who they are in the real world by looking at their online posting alone.[70]

In most cases, third parties like Yahoo! provide the necessary link between the poster's online and offline identities, because users have to provide personal information before they are allowed to post a comment or sign up for an online service.[71] Regardless of how the posters of online comments are characterized in the remainder of this Note—as anonymous or pseudonymous—it is important to keep the conceptual distinction between the two in mind: "[p]seudonymous speech is valuable in a way that anonymous speech is not and cannot be, because it permits the accumulation of reputational capital and 'goodwill' over time in the pseudonym itself, while simultaneously serving as a liability limitation insulating the speaker's 'true identity' from exposure . . . ."[72]

II. JUDICIAL APPROACHES TO ANONYMOUS ONLINE SPEECH

This Section discusses how courts handle cases involving anonymous online speech. It first describes the initial application of First Amendment doctrine to the internet and then discusses the evolution of First Amendment doctrine as it applies to anonymous online speech.

68. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 235 (Cal. Ct. App. 2008).

69. *See, e.g.*, *id.*

70. Richard Clayton, *Anonymity and Traceability in Cyberspace*, Cambridge University Technical Report Number 653, UCAM-CL-TR-653, at 12 (2005), *available at* https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf.

71. *Krinsky*, 72 Cal. Rptr. 3d at 237–38.

72. Post, *supra* note 63, at 142.

A. THE FIRST AMENDMENT PROTECTS ANONYMOUS ONLINE SPEECH

The First Amendment to the U.S. Constitution provides, in part, that "Congress shall make no law . . . abridging the freedom of speech, or the press,"[73] which is a limitation on the power of the federal government, as well as state governments via the Fourteenth Amendment.[74] Court orders, "even when issued at the request of a private party in a civil lawsuit," constitute state action and are therefore subject to constitutional limitations.[75] Political speech is the core content protected by the First Amendment,[76] but other types of speech—deemed less valuable—are also protected.[77] However, freedom of speech under the First Amendment "has its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity, and [some types of] pornography . . . ."[78]

First Amendment rights extend to online speech.[79] The First Amendment protects the right to speak anonymously.[80] The decision to speak anonymously "may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."[81] Regardless of the motivation, courts allow anonymous speech because its value in the marketplace of ideas outweighs "any public interest in requiring disclosure

---

73. U.S. CONST. amend. I.

74. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1091 (W.D. Wash. 2001) (citing First Nat'l Bank v. Bellotti, 435 U.S. 765, 779–80 (1978)).

75. *Id.* at 1091–92.

76. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346–47 (1995).

77. New York Times Co. v. Sullivan, 376 U.S. 254, 271 (1964).

78. Ashcroft v. Free Speech Coal., 535 U.S. 234, 245–46 (2002); *see also* KATHLEEN ANN RUANE, CONGRESSIONAL RESEARCH SERVICE, FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT 1–5 (2014).

79. Reno v. ACLU, 521 U.S. 844, 870 (1997):

> 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. . . . [O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

Id.

80. *See, e.g.*, *McIntyre*, 514 U.S. at 341–42; Watchtower Bible & Tract Soc'y v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002); Talley v. California, 362 U.S. 60, 64 (1960).

81. McIntyre, 514 U.S. at 341–42 ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.").

as a condition of entry."[82] In the context of online speech, the First Amendment right to speak anonymously protects both the identity of the speaker when the speaker is pursued as a named "John Doe" defendant[83] and preserves the ability of a third party publisher to resist turning over identifying information about the speaker in response to a subpoena stemming from a controversy litigated by two other parties.[84]

B. "JOHN DOE" INTERNET SPEECH CASES

In *Digital Music News*, the plaintiff sought disclosure of the identity of an anonymous internet user who posted a controversial comment. In this type of case—often called a "John Doe" case—one of the key questions is whether parties to a legal proceeding can learn the identity of the poster of an online comment.[85] Historically, the most influential standard for determining when to unmask an anonymous online speaker has been the five-factor scheme developed by the New Jersey Appellate Division court in *Dendrite International v. Doe*.[86] The standard is:

> 1. **Give Notice**: Require reasonable notice to the potential defendants and an opportunity for them to defend their anonymity before issuance of any subpoena;
>
> 2. **Require Specificity**: Require the plaintiff to allege with specificity the speech or conduct that has allegedly violated its rights;
>
> 3. **Ensure Facial Validity**: Review each claim in the complaint to ensure that it states a cause of action upon which relief may be granted based on each statement and against each defendant;
>
> 4. **Require an Evidentiary Showing**: Require the plaintiff to produce evidence supporting each element of its claims; and
>
> 5. **Balance the Equities**: Weigh the potential harm (if any) to the plaintiff from being unable to proceed against the harm to the

82. *Id.* ("Whatever the motivation may be . . . the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry.").

83. *See, e.g.*, Highfields Capital Mgmt. v. Doe, 385 F. Supp. 2d 969, 971 (N.D. Cal. 2005).

84. *See, e.g.*, Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 251–52 (Cal. Ct. App. 2008).

85. *See* Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn From John Doe?*, 50 B.C. L. REV. 1373, 1378 (2009).

86. Dendrite Int'l v. Doe, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

> defendant from losing the First Amendment right to anonymity.[87]

The *Dendrite* test was developed in response to earlier cases that allowed plaintiffs pursuing anonymous online defendants to proceed *ex parte*, which allowed plaintiffs to unmask anonymous defendants both without the defendant's knowledge and without making a showing that the anonymous speaker's statements were actually unlawful.[88] *Ex parte* proceedings raise legitimate due process concerns.[89] A modified version of the *Dendrite* standard is now used in most cases where the plaintiff alleges defamation or other tortious conduct on the part of a "Doe" defendant.[90]

The modified *Dendrite* standard most courts now use in "John Doe" First Amendment cases is exemplified by the analysis of the Supreme Court of Delaware in *Doe v. Cahill*.[91] In *Cahill*, the court explicitly rejected the final 'balancing' stage of the *Dendrite* test and instead adopted "a modified Dendrite standard consisting only of Dendrite requirements one and three: the plaintiff must make reasonable efforts to notify the defendant and must satisfy the summary judgment standard."[92] By 2012, three states were following the *Cahill* standard, while five states were following the *Dendrite* standard.[93]

The leading *John Doe* case in California is *Krinsky v. Doe 6*, where the court essentially adopted the *Cahill* standard but declined to attach the procedural label of summary judgment to the "showing required of a plaintiff seeking the identity of an anonymous speaker on the Internet" because it was "unnecessary and potentially confusing."[94] In *Krinsky*, the plaintiff, an executive of a Florida-based drug development company, sued ten anonymous defendants in Florida who posted scathing criticism of her and the company on a Yahoo! Finance message board.[95] Krinsky served a subpoena on Yahoo! to unmask the critical online posters.[96] In response to the subpoena, Yahoo! notified the posters that their identities would be

87. Paul Alan Levy, *Developments in Dendrite*, 14 FLA. COASTAL L. REV. 1, 10–11 (2012) (citing *Dendrite*, 775 A.2d at 760–61) (emphasis added).

88. *See* Gleicher, *supra* note 23, at 330 ("If the subpoena becomes ex parte, one of the defendant's most important defenses—his own vigorous advocacy—is eliminated.").

89. *Id.*

90. *See, e.g.*, Doe v. Cahill, 884 A.2d 451, 462–63 (Del. 2005).

91. *Id.*

92. *Id.* at 461.

93. *Developments in Dendrite*, *supra* note 87, at 12.

94. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 244 (Cal. Ct. App. 2008).

95. *Id.* at 234–35.

96. *Id.*

disclosed in ten days if they did not file a motion to quash.[97] Doe 6—also known on the message board as "Senor-Pinche-Wey"—moved to quash, but the superior court denied his motion because it determined he appeared to be engaged in a "pump and dump" scheme to drive down the stock price of the drug development company.[98] The Court of Appeal for the Sixth District reversed the Superior Court and granted Doe 6's motion to quash, holding that Doe 6's right to anonymous online speech outweighed Krinsky's right to unmask him because she failed to state a claim for defamation and intentional interference with business or contractual relations.[99] The court noted that, viewed in context, Doe 6's statements—like "[F]unny and rather sad that the losers who post here are supporting a management consisting of boobs, losers and crooks."—constituted "crude, satirical hyperbole which, while reflecting the immaturity of the speaker, constitute protected opinion under the First Amendment."[100]

The Ninth Circuit addressed the topic of anonymous online speech in 2011, where it upheld the district court's use of the *Cahill* standard under the "clear error" standard of review.[101] This decision has been criticized for failing to adequately account for different online contexts in determining the presumed accuracy of online speech and failing to provide a definitive standard for lower courts to analyze anonymous online speech cases.[102] However, the fact that the Ninth Circuit declined to reverse the district court's use of the *Cahill* standard suggests that the *Cahill* standard remains the appropriate framework to analyze online anonymous speech cases in California—essentially the same framework employed by the *Krinsky* court. The Ninth Circuit addressed anonymous online speech more recently in *Doe v. Harris*, but the court's opinion did not address which standard should be used when determining whether a "John Doe" poster of anonymous online comments should be unmasked.[103]

97. *Id.*
98. *Id.* at 236.
99. *Id.* at 246–52.
100. *Id.* at 248–50.
101. *In re* Anonymous Online Speakers, 661 F.3d 1168, 1177 (9th Cir. 2011).
102. *See generally* Musetta Durkee, *The Truth Can Catch the Lie: The Flawed Understanding of Online Speech In re Anonymous Online Speakers*, 26 BERKELEY TECH. L.J. 773 (2011).
103. Doe v. Harris, 772 F.3d 563, 579–80 (9th Cir. 2014) (characterizing the case as, in part, an anonymous online speech case, but not discussing the standards for unmasking 'John Doe' defendants).

Several public interest organizations—including the Public Citizen Litigation Group, the American Civil Liberties Union and the Electronic Frontier Foundation—have spearheaded a campaign to develop more consistent legal standards for unmasking anonymous online speakers that balance the rights of the anonymous internet user against the rights of plaintiffs harmed by anonymous online speech. Paul Alan Levy of the Public Citizen Litigation Group—brought in as counsel *pro hac vice* in *Digital Music News*—has been involved in at least fifty-six cases involving anonymous online speech.[104]

Scholars and state legislatures have also weighed in on how best to handle anonymous online speech. Many scholars have proposed standards to balance the First Amendment rights of anonymous and pseudonymous online speakers with the rights of defendants harmed by allegedly tortious online content.[105]

In addition, state legislatures have experimented with ways to regulate anonymity online. In 1997, for example, a court struck down a state law criminalizing internet transmissions that falsely identified their sender because it violated the first amendment rights of pseudonymous online

104. *See* Supplemental Memorandum by Newly Retained Counsel in Opposition to Motion to Compel Subpoena Compliance, In re Subpoena Issued to Digital Music News, LLC, UMG Recordings, Inc. v. Escape Media Group, Inc., No: SS 022 099 (Cal. Super. Ct. May 15, 2012), *available at* http://www.citizen.org/documents/Supplemental-Memo-Opposition-Motion-Compel.pdf. Paul Alan Levy leads Public Citizen's Internet Free Speech Project and maintains a helpful website on anonymous online speech. *See Internet Free Speech - Right To Speak Anonymously*, PUB. CITIZEN LITIG. GROUP, http://www.citizen.org/Page.aspx?pid=2702 (last visited Sept. 24, 2014); *Internet Free Speech*, PUB. CITIZEN LITIG. GROUP, http://www.citizen.org/Page.aspx?pid=396 (last visited Sept. 24, 2014). The Digital Media Law Project at Harvard University's Berkman Center for Internet and Society, which includes a state-by-state guide, is another excellent general resource on legal protections for anonymous online speech. *See, e.g.*, *Legal Protections for Anonymous Speech*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/legal-protections-anonymous-speech (last visited Sept. 9, 2014); *Legal Protections for Anonymous Speech in California*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/legal-protections-anonymous-speech-california (last visited Sept. 9, 2014).

105. *See, e.g.*, Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn From John Doe?*, 50 B.C. L. REV. 1373 (2009); Gleicher, *supra* note 23; Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing Over Legal Standards*, 83 OR. L. REV. 795 (2004); Susanna Moore, *The Challenge of Internet Anonymity: Protecting John Doe on the Internet*, 26 J. MARSHALL J. COMPUTER & INFO. L. 469 (2009); Jonathan D. Jones, Note, *Cybersmears and John Doe: How Far Should First Amendment Protection of Anonymous Internet Speakers Extend?*, 7 FIRST AMEND. L. REV. 421 (2009); Clay Calvert, et al., *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers*, 43 J. MARSHALL L. REV. 1 (2009).

speakers and was void for being unconstitutionally vague.[106] And in *Doe v. Harris*, the Ninth Circuit struck down a California law that required convicted sex offenders to register any new online account within twenty-four hours of opening it, in part because it violated sex offenders' First Amendment right to anonymous online speech.[107]

III. THE RIGHT TO PRIVACY IN THE CALIFORNIA CONSTITUTION

Digital Music News is one of the most recent "John Doe" anonymous online speech cases, but it is especially noteworthy because of the court's holding that Visitor's right to anonymous online speech is partially grounded in the privacy clause of the California Constitution. At least eleven states have expressly incorporated a privacy clause into their state constitutions.[108] Indeed, "[t]hese express provisions provide fertile ground for the recognition of expansive privacy rights."[109] The courts of last resort of other states, including Alabama,[110] Texas,[111] and Tennessee,[112] have interpreted their state constitutions to contain an implicit right to privacy. This Section will explain the privacy clause of the California Constitution, including its history, the rights it confers on California citizens, and how it can be used in litigation.

---

106. ACLU of Georgia v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997).

107. Doe v. Harris, 772 F.3d 563, 582 (9th Cir. 2014).

108. *See* Privacy Protections in State Constitutions, NAT'L CONF. STATE LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-Constitutions.aspx (last visited Sept. 23, 2014). In addition to the states on this list, Missouri also added a privacy clause to its state Constitution in 2014. Missouri's new privacy clause is explicitly aimed at extending Fourth Amendment protections to electronic communications data. *See* Becca Stanek, *Missouri Passes Constitutional Amendment to Protect Electronic Privacy*, TIME (Aug. 6th, 2014), http://time.com/3087608/missouri-electronic-privacy-amendment/.

109. Jeffrey M. Shaman, *The Right of Privacy in State Constitutional Law*, 37 RUTGERS L. J. 971, 975 (2006).

110. Jegley v. Picado, 80 S.W.3d 332, 350 (Ala. 2002) ("[a] fundamental right to privacy is implicit in the Arkansas Constitution.").

111. Texas State Emp. Union v. Texas Dept. of Mental Health and Mental Retardation, 746 S.W.2d 203, 205 (Tex. 1987) ("[a] right of individual privacy is implicit among those 'general, great, and essential principles of liberty and free government' established by the Texas Bill of Rights.").

112. Davis v. Davis, 842 S.W.2d 588, 600 (Ten. 1992) ("The right to privacy, or personal autonomy ('the right to be let alone'), while not mentioned explicitly in our state Constitution, is nevertheless reflected in several sections of the Tennessee Declaration of Rights . . .").

The right to privacy is explicitly recognized by California's Constitution[113] and is broader than the implied federal right to privacy.[114] Proposition 11 added the "privacy clause" to the California Constitution in 1972, as a constitutional amendment presented to California voters.[115] It has been construed to provide each California citizen with a self-executing, enforceable right to privacy.[116] Further, the privacy clause creates a cause of action against private entities; it is not limited by the state action doctrine.[117] However, the right to privacy recognized by the California Constitution is no broader than federal Fourth Amendment privacy rights in the area of search and seizure.[118] In applying the privacy clause to new factual contexts, courts must interpret it "in a manner consistent with the probable intent of the body enacting it: the voters of the State of California," by referring to the ballot arguments offered to California voters when the amendment was passed.[119]

The ballot arguments that accompanied Proposition 11 are therefore essential to understanding the scope and nature of the privacy right conferred by the privacy clause, especially considering the relative lack of other legislative materials to shed light on its meaning.[120] The argument

113. CAL. CONST. Art. 1, § 1 (West 2014) ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

114. Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 809 (May 14, 2014) (citing Am. Acad. of Pediatrics v. Lungren, 66 Cal. Rptr. 2d 210, 221 (Cal. Ct. App. 1997)).

115. Right of Privacy, Proposition 11 (Cal. 1972), *available at* http://repository.uchastings.edu/ca_ballot_props/762; *see also* JOSEPH R. GRODIN, CALVIN R. MASSEY, & RICHARD B. CUNNINGHAM, THE CALIFORNIA STATE CONSTITUTION: A REFERENCE GUIDE 23–25, 39 (1993).

116. White v. Davis, 120 Cal. Rptr. 94, 106 (Cal. 1975).

117. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012).

118. Lewis v. Sup. Court, 172 Cal. Rptr. 3d 491, 500 (Cal. Ct. App. 2014).

119. Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 843 (Cal. Ct. App. 1994):

> When, as here, the language of an initiative measure does not point to a definitive resolution of a question of interpretation, it is appropriate to consider indicia of the voters' intent other than the language of the provision itself. Such indicia include the analysis and arguments contained in the official ballot pamphlet.

Id (citations and quotations omitted).

120. J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 351, 358, 417 (1992). Much of Professor Kelso's argument in his Article actually relies upon other documents that he located through his own research and which help to shed light on the legislative intent behind Proposition 11. The thrust of Professor Kelso's argument in his Article is that the privacy clause should not create a cause of action

that supported a "yes" vote on Proposition 11 characterized the constitutional amendment as necessary in the face of increasing electronic data collection and as a solution to the lack of "effective restraints on the information [gathering] activities of governments and business."[121] The main arguments for a "no" vote on Proposition 11 were: (1) a state constitutional right to privacy will encourage welfare fraud and tax evasion by making it easier for citizens to decline to disclose income information, and (2) adding the word privacy to the constitution is surplusage that works against efforts to make the California Constitution shorter.[122] The California Supreme Court has noted that the privacy clause implicitly incorporates common-law privacy jurisprudence because the ballot argument that accompanied Proposition 11 characterized the right offered to voters as "the right to be left alone."[123]

The arguments offered in support of adding the privacy clause to the California Constitution are also imbued with overtones that speak to the dignity aspect of our identities. The ballot argument in favor of Proposition 11 states, in part, "The right of privacy is the right to be left alone . . . . It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose."[124] And in defining the common law privacy right incorporated into the privacy clause, the California Supreme Court has discussed the psychological foundations of privacy rights, which

> emanat[e] from personal needs to establish and maintain identity and self-esteem by controlling self-disclosure. . . . In a society in

against purely private entities. However, the California Supreme Court disagreed with Professor Kelso three years after the publication of his Article by using only the ballot arguments to determine the legislative intent behind Proposition 11 and ultimately determining that the privacy clause did create a cause of action against private entities. *See Hill*, 26 Cal. Rptr. 2d at 843.

121. *Argument in Favor of Proposition 11*, Right of Privacy, Proposition 11 (Cal. 1972), *available at* http://repository.uchastings.edu/cgi/viewcontent.cgi?Note=1761&context=ca_ballot_props.

122. *Argument Against Proposition 11*, Right of Privacy, Proposition 11 (Cal. 1972), *available at* http://repository.uchastings.edu/cgi/viewcontent.cgi?Note=1761&context=ca_ballot_props.

123. *Hill*, 26 Cal. Rptr. 2d at 848. The reference is, of course, to the famous law review article *The Right to Privacy* (Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198, 205 (1890)). The court in *Hill* then notes that the ideas expressed in Warren & Brandeis' law review article were eventually incorporated into the law through Brandeis' dissent in Olmstead v. United States 277 U.S. 438, 478 (1928) and Prosser's Restatement, Second of Torts.

124. Argument in Favor of Proposition 11, *supra* note 121.

> which multiple, often conflicting role performances are demanded of each individual, the original etymological meaning of the word 'person'—mask—has taken on new meaning. . . . Loss of control over which 'face' one puts on may result in literal loss of self-identity, and is humiliating beneath the gaze of those whose curiosity treats a human being as an object.[125]

Finally, the ballot argument in support of Proposition 11 stated, "Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom."[126]

The California Supreme Court established the necessary elements of a cause of action against a private entity under the privacy clause in *Hill v. Nat'l Collegiate Athletic Ass'n*.[127] In *Hill*, Stanford University athletes brought an unsuccessful challenge against the NCAA's mandatory drug-testing policy under the privacy clause.[128] While the athletes lost, the *Hill* court established the framework that California courts continue to use in privacy clause cases.[129] To state a claim for a violation of the California constitutional right to privacy, a plaintiff must "establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy."[130] The privacy clause protects informational[131] and autonomy privacy,[132] but informational privacy is the

125. *Hill*, 26 Cal. Rptr. 2d at 849 (quoting Briscoe v. Reader's Digest Ass'n, 93 Cal. Rptr. 866, 869 (Cal. 1971)) (citations and quotations omitted).

126. Argument in Favor of Proposition 11, *supra* note 121.

127. 26 Cal. Rptr. 2d at 859.

128. *Id.* at 838.

129. *Id.* For examples of courts applying this framework, see also 420 Caregivers, LLC v. City of L.A., 163 Cal. Rptr. 3d 17, 40–41 (Cal. Ct. App. 2012); Medical Bd. of Cal. v. Chiarottino, 170 Cal. Rptr. 3d 540, 546 (Cal. Ct. App. 2014); *In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016 (N.D. Cal. 2012).

130. *Hill*, 26 Cal. Rptr. 2d at 859.

131. *Id.* at 856:

> Informational privacy is the core value furthered by the Privacy Initiative. A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity. Such norms create a threshold reasonable expectation of privacy in the data at issue. As the ballot argument observes, the California Constitutional right of privacy prevents government and business interests from [1] collecting and stockpiling unnecessary information about us and from [2] misusing information gathered for one purpose in order to serve other purposes or to embarrass us.

"core value" furthered by the privacy clause.[133] Whether a legally protected privacy interest exists in a given case is a question of law, whereas whether a reasonable expectation of privacy existed and whether the defendant's conduct constituted a serious invasion of privacy are mixed questions of law and fact.[134] However, courts that have assessed more recent claims under the privacy clause have noted that it presents a "high bar" for plaintiffs to clear:[135] even disclosure of sensitive personal information has been found not to breach the California constitutional right to privacy.[136]

IV. *DIGITAL MUSIC NEWS V. SUPERIOR COURT*

A. FACTS OF THE CASE

Escape Media Group owns Grooveshark, which is an online service that allows its users to upload, share, download, and stream music files.[137] UMG Recordings, Inc. ("UMG") is a record label that owns a large music catalogue, including the work of many well-known recording artists.[138] UMG sued Escape in New York state court for state common law copyright infringement and unfair competition, alleging that Escape encouraged Grooveshark users and employees to upload copyright-infringing music files.[139]

Digital Music News, LLC ("DMN") is a California-based company that operates a website dedicated to reporting on the music industry. DMN ran a story consisting primarily of an exchange between a member of the British band King Crimson and Grooveshark.[140] The exchange

Id. (citations and quotations omitted).

132. *Id.* ("Autonomy privacy is also a concern of the Privacy Initiative. The ballot arguments refer to the federal Constitutional tradition of safeguarding certain intimate and personal decisions from government interference in the form of penal and regulatory laws.")

133. *Id.*

134. *Id.* at 865.

135. *In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016 (N.D. Cal. 2012).

136. *Id.* (citing Belluomini v. Citigroup, Inc., No. CV 13–01743 CRB, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012)).

137. Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 801–02 (May 14, 2014).

138. *Id.*

139. UMG Recordings, Inc. v. Escape Media Group, Inc., 964 N.Y.S. 2d 106 (N.Y. App. Div. 2013).

140. Rochell Abonalla, *King Crimson Can't Get Their Music Off of Grooveshark. So They cc'd Digital Music News* . . ., DIGITAL MUSIC NEWS (Oct. 13, 2011), http://www.digitalmusicnews.com/permalink/2011/10/13/cc.

reflected the musician's attempts to ensure that his copyrighted music would no longer appear on Grooveshark without his permission.[141] An anonymous commenter ("Visitor") posted two comments on the website, stating (a) he was an employee of Grooveshark; (b) he was required by Grooveshark executives to upload copyright-infringing content; and (c) there was no way for King Crimson to remove its music from the online platform.[142] Visitor is the handle DMN appears to assign by default to all users who do not wish to provide their name when commenting.[143]

Visitor's comments contradicted positions that Escape took in its New York dispute with UMG.[144] Escape claimed that it exclusively hosted third-party content and removed content when it received copyright complaints. Considering that Visitor's claims would harm Escape's case if they could be verified and introduced as evidence, Escape sought to unmask the identity of "Visitor" by subpoenaing DMN. DMN refused to comply with the subpoena, so Escape petitioned the Los Angeles County Superior Court to enforce the subpoena under the Interstate and International Depositions and Discovery Act.[145]

B. PROCEDURAL HISTORY

The trial court held there was (a) a possibility that fragmented data remained on DMN's servers that could be used to identify Visitor; and (b) Escape made a successful *prima facie* case that Visitor's comments were libelous and therefore unprotected by the First Amendment.[146] The trial court ordered DMN to comply with the subpoena.[147] The court issued a supplemental order outlining the compliance process, which required Escape to purchase a backup server where DMN would upload a virtual machine image of its server. A court-appointed third party forensic examiner was then to examine the virtual machine image and determine if

141. *Id.*

142. *See id.*; *see also* Peter Menell, Commentary, *Jumping the Grooveshark: A Case Study in DMCA Safe Harbor Abuse* at 2 (Dec. 21, 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1975579 (reprinting and discussing the comment left by "Visitor" that received the most attention).

143. *See generally* Abonalla, *supra* note 140.

144. UMG Recordings, Inc., 964 N.Y.S. 2d at 107.

145. CAL. CIV. PROC. CODE § 2029.300 (West 2014); *see also* Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 804 (May 14, 2014).

146. *Digital Music News*, 171 Cal. Rptr. 3d at 809.

147. *Id.*

Visitor could be identified, but only make Visitor's identifying information available to Escape if the court directed the examiner to do so.[148]

DMN appealed both the order requiring compliance with the subpoena and the order that laid out the procedure to be followed. The California Court of Appeal for the Second District requested supplemental briefing on two questions: whether disclosure of Visitor's identity was reasonably calculated to lead to admissible evidence under applicable California discovery laws and whether Escape's need for discovery was outweighed by Visitor's privacy interests under the California Constitution.[149]

C. THE CALIFORNIA COURT OF APPEALS' ANALYSIS

The California Court of Appeals reversed the trial court's order, refusing to provide Escape with Visitor's identity.[150] The court's decision was based on two, alternative holdings: (1) California discovery law prohibits disclosure of Visitor's identity because it "is not reasonably calculated to lead to the discovery of admissible evidence in the underlying lawsuit between UMG and Escape,"[151] and (2) Visitor's privacy rights—grounded both in the First Amendment and California's constitutional right to privacy—outweighed Escape's need for disclosure of Visitor's identity.[152]

1. California Discovery Law Prohibits Disclosure of Visitor's Identity

Escape subpoenaed DMN under the Interstate and International Depositions and Discovery Act to obtain Visitor's identity.[153] DMN refused to comply with the subpoena from the New York court; Escape countered by attempting to compel compliance with the subpoena in

148. *Id.* The backup server provided by Escape was to be wiped of all data upon the conclusion of the court proceeding.

149. Order Requesting Supplemental Letter Briefs, *In re* Matter of Subpoena in UMG Recordings, No. B242700 (Los Angeles Superior Court No. SS022099) (Cal. Ct. App. Jan. 31, 2014), *available at* http://www.citizen.org/documents/OrderRequestingSupplementalLetterbriefs.pdf.

150. *Digital Music News*, 171 Cal. Rptr. 3d at 810. The court reversed the trial court's discovery order even though it was reviewing trial court's order under the "deferential abuse-of-discretion standard." *Id.* at 805. The Court of Appeals treated Digital Music News's appeal from the trial court's order as an extraordinary writ because the extraordinary writ is the judicial review mechanism provided by § 2029.600 of the California Code of Civil Procedure (which incorporates the Interstate and International Depositions and Discovery Act into California law).

151. *Id.* at 809.

152. *Id.*

153. *Id.* at 804; CAL. CIV. PROC. CODE § 2029.900 (West 2014).

California court.[154] The discovery dispute was governed by California civil discovery rules, which permit discovery when the material sought by the party is relevant to the subject matter of the action and "either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence."[155] A California appellate court may reverse a trial court's grant of discovery if it concludes there is not a "reasonable possibility" that the information sought will lead to admissible evidence that is relevant to the underlying dispute, meaning it has "tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action."[156]

Considering that the scope of civil discovery is "broad," but not "limitless,"[157] the appellate court reversed the trial court's order requiring compliance with Escape's subpoena request because Visitor's identity was neither relevant to the underlying dispute between UMG and Escape, nor was it "reasonably calculated to lead to the discovery of admissible evidence."[158] Visitor's identity was held irrelevant to the underlying dispute between Escape and UMG because UMG's claims centered on the allegedly copyright infringing conduct of Grooveshark's users, not its employees.[159]

The court also rejected Escape's supplemental arguments that Visitor's identity was relevant to its case against UMG. Escape alleged that UMG authored Visitor's comments in support of Escape's interference with business relations counterclaim against UMG.[160] Escape also argued that Visitor's identity was relevant to separate litigation in federal court involving the same parties, where UMG cited Visitor's comment as part of its allegation that Grooveshark employees were required to upload copyright-infringing content.[161] The court rejected both of these arguments: Escape's interference with business relations counterclaim did not mention Visitor's comment and Visitor's identity was irrelevant to the federal suit because "an anonymous comment on the Internet is nugatory

154. *Digital Music News*, 71 Cal. Rptr. 3d at 804.
155. *Id.* at 805.
156. *Id.* (quoting Forthmann v. Boyer, 118 Cal. Rptr. 2d 715, 723 (Cal. Ct. App. 2002); CAL. EVID. CODE § 350; CAL. EVID. CODE § 210).
157. *Id.* (quoting Calcor Space Facility, Inc. v. Super. Ct., 61 Cal. Rptr. 2d 567, 572 (Cal. Ct. App. 1997)).
158. *Id.* at 807.
159. *Id.* at 807–08.
160. *Id.*
161. *Id.*

both as a matter of pleading and of proof."[162] The court thus held that Visitor's identity was not reasonably calculated to lead to the discovery of admissible evidence—sufficient grounds to reverse the trial court's order.[163]

2. *Visitor's Privacy Interests Outweigh Escape's Need for Discovery*

The court in *Digital Music News* began its analysis of Visitor's privacy rights with the observation: "The right to speak anonymously draws its strength from two separate constitutional wellsprings: the First Amendment's freedom of speech and the right of privacy in Article I, Section I of the California Constitution."[164] But the court also noted that the California constitution alone provides California internet users the right to anonymous online speech.[165] In California, the privacy rights of online speakers must be weighed heavily against any pressure to reveal that user's identity when a third party attempts to unmask her with a subpoena.[166] The court ultimately determined that Visitor's right to privacy outweighed Escape's "practically nonexistent" need for discovery.[167]

The court in *Digital Music News* highlighted the identity and autonomy enhancing aspects of online anonymity in discussing the reasons for constitutional protection of anonymous online speech. Visitor has a right to speak anonymously because she needs "a venue from which to be heard without fear of interference or suppression" and Visitor's anonymity freed her from "fear of retaliation."[168] Additionally, "the online forum

---

162. *Id.* at 808–09.

163. *Id.* at 809.

164. *Id.* (citing Rancho Publ'ns v. Super. Ct., 81 Cal. Rptr. 2d 274, 275 (Cal. Ct. App. 1999)).

165. *Id.*

> The California privacy right protects the speech and privacy rights of individuals who wish to promulgate their information and ideas in a public forum while keeping their identities secret, and limits what courts can compel through civil discovery. Both California courts and federal courts have recognized the value in extending the protections afforded anonymous speech to speech made via the Internet.

Id. (citations and quotations omitted). Again, the express right to privacy in the California Constitution is broader than the implied federal right to privacy in this area. Am. Acad. of Pediatrics v. Lungren, 66 Cal. Rptr. 2d 210, 221–22 (Cal. Ct. App. 1997).

166. *Digital Music News*, 171 Cal. Rptr. 3d at 809–10 ("The party seeking discovery must demonstrate a compelling need for discovery, and that compelling need must be so strong as to outweigh the privacy right when these two competing interests are carefully balanced.") (citing Lantz v. Super. Ct., 34 Cal. Rptr. 2d 358, 366-67 (Cal. Ct. App. 1994)).

167. *Id.* at 810.

168. *Id.*

allows individuals of any economic, political, or social status to be heard without suppression or other intervention by the media or more powerful figures in the field."[169] Finally, "[t]he ability to speak one's mind on the Internet without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."[170]

To balance Visitor's privacy rights against Escape's interest in Visitor's identity, the *Digital Music News* court did not apply a First Amendment balancing test—like the *Cahill* standard—or the *Hill* standard for establishing an invasion of the California constitutional right to privacy by a private entity.[171] Instead, the court applied the standard for balancing privacy rights under the California Constitution against a private party's need for that information in the civil discovery context developed in *Lantz v. Superior Court* and *Planned Parenthood Golden Gate v. Superior Court*.[172] The *Lantz* standard requires the party who seeks discovery—if the discovery request implicates the California constitutional right to privacy—to go beyond normal discovery requirements[173] and show "a compelling need for discovery" that is "so strong as to outweigh the privacy right when these two competing interests are carefully balanced."[174] A litigant establishes "compelling need" by "establishing the discovery sought is directly relevant and essential to the fair resolution of the underlying lawsuit."[175]

The court held that Visitor's privacy interest outweighed Escape's weak interest in Visitor's identity because Visitor's identity was not essential to a fair resolution of the UMG lawsuit.[176] Visitor's privacy interest was strong because Visitor needs a "venue from which to be heard without fear of interference or suppression" and "[v]isitor's anonymity also

169. *Id.* (citing Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237 (Cal. Ct. App. 2008)).

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

171. See discussion of *Cahill* standard, *supra* Part II.B and see discussion of the *Hill* standard, *supra* Part III.

172. *Digital Music News*, 171 Cal. Rptr. 3d at 809–10.

173. Normally, a party to civil litigation in California may obtain discovery on any matter that is "relevant to the subject matter involved in the pending action or to the determination of any motion made in that action, if the matter either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence." CAL. CIV. PROC. CODE § 2017.010 (West 2014).

174. *Digital Music News*, 171 Cal. Rptr. 3d at 809 (citing Lantz v. Superior Court, 34 Cal. Rptr. 2d 358, 366–67 (Cal. Ct. App. 1994); Planned Parenthood Golden Gate v. Super. Ct., 99 Cal. Rptr. 2d 627, 636 (Cal. Ct. App. 2000)).

175. *Id.* at 810 (citing Planned Parenthood Golden Gate, 99 Cal. Rptr. 2d at 367).

176. *Id.* at 810.

frees him or her from fear of retaliation, an even more compelling interest if Visitor truly is an Escape employee, as represented, because exposure could endanger not only his or her privacy but also livelihood."[177] Visitor's privacy interest thus outweighed Escape's "practically nonexistent" need for discovery.[178] The court concluded:

> Visitor has done nothing more than provide commentary about an ongoing public dispute in a forum that could hardly be more obscure—the busy online comments section of a digital trade newspaper. Such commentary has become ubiquitous on the Internet and is widely perceived to carry no indicium of reliability and little weight. We will not lightly lend the subpoena power of the courts to prove, in essence, that Someone Is Wrong On The Internet.[179]

V. FUTURE EXPANSION AND APPLICATION OF THE RIGHT TO ANONYMOUS ONLINE SPEECH RECOGNIZED IN *DIGITAL MUSIC NEWS V. SUPERIOR COURT*

There is a semantic and substantive difference between identity in the simple sense of determining who posted a comment online and the more robust version of identity through which we define who we are, but these concepts are closely related.[180] This Note has discussed some of the many

---

177. *Id.*

178. *Id.* The court explained:

> If Visitor is not an Escape employee, his or her opinion about Grooveshark not only lacks foundation but would be undermined by Visitor's misrepresentation concerning employment, and would therefore be of little or no probative value in this or any litigation. And as discussed above, Visitor's comments, even if made by an employee, are only tangentially related to UMG's lawsuit, as Visitor makes allegations UMG does not make and undermines a defense Escape is now barred from raising.

Id.

179. *Id.* Here, Judge Chaney is referring to a well-known online comic strip called xkcd. In the particular iteration of xkcd that the Judge refers to, a character typing away on its computer refuses to come to bed because "Someone is wrong on the Internet." *See* Randall Munroe, *Duty Calls*, XKCD, http://xkcd.com/386/.

180. Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 122 (1996) ("The link between identity and interaction is not limited to communication, or even personal privacy; it bears on how we define ourselves and how

cases that have weighed the right of an anonymous online speaker not to have her identity disclosed against the rights of someone allegedly harmed by her speech.[181] In many cases when courts determine that an online commenter's identity should not be disclosed—a decision to protect the poster's identity in the simple sense—courts justify their decisions by explaining the identity interests of the online commenter in the robust sense.[182] The identity right ultimately protected when a court decides not to unmask an online speaker is really a type of dignity or autonomy right. It is the right to define who we are, which allows us to work towards self-actualization.[183] The robust identity right consistently protected by the courts should not be confined to a single persona, but also provide an affirmative right to maintain multiple online pseudonyms, because the process of defining who we are includes trying out different roles.[184]

The court's opinion in *Digital Music News v. Superior Court* is notable because it explicitly makes the connection between the First Amendment and the right to privacy in its more robust form,[185] as guaranteed by the

we are defined by others. This aspect of anonymity is especially significant in the online milieu, because compelling identity revelation, while neutral on its face, forces online activity into pre-existing identity-conscious social practices.") (citations omitted).

181. *See, e.g.*, Dendrite Int'l v. Doe, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 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.").

182. Krinsky v. Doe, 72 Cal. Rptr. 3d 231, 237 (Cal. Ct. App. 2008) ("The use of a pseudonymous screen name offers a safe outlet for the user to experiment with novel ideas, express unorthodox political views, or criticize corporate or individual behavior without fear of intimidation or reprisal. In addition, by concealing speakers' identities, the online forum allows individuals of any economic, political, or social status to be heard without suppression or other intervention by the media or more powerful figures in the field.").

183. *See* Tien, *supra* note 180, at 133 (providing the example of an artist working in a new medium as somebody who would not want her name associated with her work); *see also* Lawrence Lessig, Code: Version 2.0 89–90 (2006), *available at* http://www.codev2.cc/download+remix/Lessig-Codev2.pdf (describing the power that the pseudonym 'StrayCat' gives to its owner to develop her identity in multifaceted and conflicting ways that she could not offline).

184. *See* Tien, *supra* note 180, at 164–65 (explaining how people have multiple selves that contribute to their identity as a singular being).

185. *See* Am. Acad. of Pediatrics v. Lungren, 66 Cal. Rptr. 2d 210, 221–22 (Cal. Ct. App. 1997) (explaining that right to privacy under the California Constitution is broader than the implied federal right to privacy).

California Constitution.[186] In so doing, the court implicitly dismisses the overly simplistic argument that the First Amendment and the right to privacy work at cross-purposes in all circumstances.[187] While the problems caused by anonymous online speech are undeniably significant, the approach taken in *Digital Music News* is an increasingly rare example of the counterargument to the contention that the internet user's ability to communicate anonymously should be limited to solve these problems: that some degree of online anonymity should be preserved because anonymous speech furthers constitutionally provided liberty interests.[188] Thus, *Digital Music News* is not only important because it provides California internet users a clear understanding of the source of their right to post anonymous online comments, but also because it persuasively combines First Amendment and privacy rights, recognizing a right to develop one's own identity.[189]

A. A HYPOTHETICAL LEGAL CHALLENGE TO FACEBOOK'S REAL NAMES POLICY

The recent controversy surrounding Facebook's "Real Names" policy—involving the mass disabling of the Facebook accounts of drag queens—is a helpful example to explore some of the issues implicated by anonymous and pseudonymous online speech. Historically, Facebook only allowed new users to sign up for its service on the condition that they use their legal names, meaning names that could be supported with various forms of identification.[190] Facebook, however, tended to under-enforce its own policy.[191] Many drag queens created Facebook pages using their stage

186. Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 809 (May 14, 2014).

187. *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 402 n.94 (2008).

188. These problems, which are very serious and certainly must be dealt with, include cyberbullying and trolling. *See* Parts I.B and I.C (discussing these problems and proposed solutions that focus on reducing internet users' ability to communicate anonymously, or at least operating under a perception of anonymity).

189. *See* Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 849 (quoting Briscoe v. Reader's Digest Ass'n, Inc., 93 Cal. Rptr. 866, 869 (Cal. 1971)) ("Privacy rights also have psychological foundations emanating from personal needs to establish and maintain identity and self-esteem by controlling self-disclosure . . . .") (citations and quotations omitted).

190. *See* Lowder, *supra* note 66 (explaining Facebook's "'real name policy,' which stipulates that 'people use their real identities' and 'provide their real names, so you always know who you're connecting with.' The rule is designed to 'keep the community safe.'").

191. *Id.* ("[M]any queens note that they've used their drag names in their profiles without incident for years.").

names, such as "Sister Roma" and "Lil Miss Hot Mess." They used their Facebook pages undisturbed for years. In the fall of 2014, Facebook mass-disabled the accounts of many drag queens, prompted, apparently, by flags from a Facebook user who reported the queens' technical noncompliance with Facebook's real names policy.

Drag queens' names encapsulate the dignity interest in pseudonymous identities that should be protected by a combination of the First Amendment and the right to privacy: the names are used for an expressive purpose,[192] contribute to the development of the identity of their owner, and may physically protect their owners. After discovering that their accounts had been disabled, Sister Roma and Lil Miss Hot Mess led an online campaign on other platforms to raise awareness of their plight.[193] Many commentators weighed in on the harm caused by not allowing pseudonyms on Facebook,[194] some drawing parallels to the successful campaign waged against Google that led to the permissible use of pseudonyms on the Google+ social network[195]—known as the "Nymwars."[196] Some users left Facebook to join a new social networking service called Ello in protest because it allowed anonymous and

192. *See, e.g.*, Hurley v. Irish-American Gay, Lesbian & Bisexual Group, 115 S. Ct. 2338, 2347 (1995) (reversing the decision of a group who administered a parade, which denied the Irish-American Gay, Lesbian & Bisexual Group's application to have a float in the parade because the denial violated the First Amendment's protection for expressive conduct).

193. *See* Lowder, *supra* note 66:

> Sister Roma started a Twitter hashtag, #MyNameIsRoma, as a way of illustrating that for many queens, their drag name is more 'real' than the words on their birth certificate. A coalition of performers has started a Change.org petition to challenge the policy, writing that "although our names might not be our 'legal' birth names, they are still an integral part of our identities, both personally and to our communities."

Id.; *see also* Safronova, *supra* note 26.

194. *See, e.g.*, Jillian C. York, *Facebook's 'Real Names' Policy is Legal, But It's Also Problematic for Free Speech*, GUARDIAN (Sept. 29, 2014), http://www.theguardian.com/commentisfree/2014/sep/29/facebooks-real-names-policy-is-legal-but-its-also-problematic-for-free-speech.

195. *See* Eva Galperin & Jillian C. York, *Victory! Google Surrenders in the Nymwars*, ELECTRONIC FRONTIER FOUND. (Oct. 19, 2011), https://www.eff.org/deeplinks/2011/10/victory-google-surrenders-nymwars.

196. "Nymwars" was the phrase coined to explain the fight to force Google to allow Google+ users to sign up using pseudonyms. The same phrase has been used in the context of the dispute between the drag queens and Facebook. *See* Eva Galperin, *2011 in Review: Nymwars*, ELECTRONIC FRONTIER FOUND. (Dec. 26, 2011), https://www.eff.org/deeplinks/2011/12/2011-review-nymwars.

pseudonymous use, did not sell advertising, and purported to put users' privacy first.[197] A contingent of drag queens secured a meeting with Facebook aided by David Campos, a member of the San Francisco Board of Supervisors.[198]

On Wednesday, October 1st, 2014, Facebook announced a change in its policy[199] allowing drag queens to use Facebook with their stage names.[200] "Although our names might not be our 'legal' birth names, they are still an integral part of our identities, both personally and to our communities." Days later, news surfaced that Facebook was developing a new app explicitly focused on anonymous communication.[201] In short, Facebook appears to have voluntarily reversed its position on pseudonymous and anonymous online communication.

If Facebook had not reversed its real names policy itself, perhaps Lil Miss Hot Mess could have compelled Facebook to reverse its policy in California state court, building her legal argument by combining the reasoning found in *Digital Music News* with the framework for establishing a cause of action against a private entity under the privacy clause of the California Constitution from *Hill v. NCAA*.[202] Lil Miss Hot Mess's legal arguments in a hypothetical action against Facebook would be further buttressed by the language courts have used in the anonymous and online speech cases discussed throughout this Note, which provide strong support for the protection of identity interests by allowing anonymous online communication.

To state a claim for a violation of the California constitutional right to privacy under *Hill v. NCAA*, a plaintiff must establish "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious

197. *See* Nidhi Subbaraman, *Online Identity Matters: Facebook, Ello, and the Right to Pseudonyms*, BETABOSTON (Oct. 1, 2014), http://betaboston.com/news/2014/09/30/online-identity-matters-facebook-ello-and-the-right-to-pseudonyms/.

198. *See* Safronova, *supra* note 26.

199. *See* Christopher Cox, Post of Oct. 1, 2014 at 11:49am, FACEBOOK (Oct. 1, 2014), https://www.facebook.com/chris.cox/posts/10101301777354543.

200. *See* Amanda Holpuch, *Victory for Drag Queens as Facebook Apologises for 'Real-Name' Policy*, GUARDIAN (Oct. 1, 2014), http://www.theguardian.com/technology/2014/oct/01/victory-drag-queens-facebook-apologises-real-name-policy.

201. *See* Mike Isaac, *Facebook Developing App That Allows Anonymity*, N.Y. TIMES (Oct. 7, 2014), http://bits.blogs.nytimes.com/2014/10/07/facebook-readies-app-allowing-anonymity/?_php=true&_type=blogs&_r=0.

202. Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 809 (May 14, 2014); Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 845.

invasion of privacy."[203] In this hypothetical challenge to Facebook's real names policy, drag queens would argue that they have a legally protected privacy interest in using their stage names on Facebook. Like in *Digital Music News*, where the court held that Visitor's privacy interest was strong because Visitor needs a "venue from which to be heard without fear of interference or suppression," drag queens have a strong privacy interest that supports their ability to use their Facebook accounts with their stage names because they too need a venue from which to be heard without fear of suppression.[204] Further, like Visitor in *Digital Music News*, the relative anonymity provided by the use of a pseudonym on Facebook "frees him or her from fear of retaliation;"[205] from, say, homophobic members of her offline neighborhood, based on views she expressed on Facebook.[206] A drag queen that uses Facebook with her stage name therefore has a legally protected privacy interest.[207]

The drag queens' reasonable expectation of privacy in the circumstances and Facebook's conduct that constituted a serious invasion of that privacy can both be alleged from the actual facts of the controversy. Many drag queens, such as Lil Miss Hot Mess, had been using Facebook accounts associated with their stage name for years—the duration of time that they were allowed to use their accounts supports the argument that they had a reasonable expectation that they would be able to continue to use their accounts.[208] Their longstanding ability to use a pseudonym creates an expectation of privacy: the privacy provided by the pseudonym itself. Further, Facebook's sudden disabling of many drag queens' Facebook accounts set up using stage names is a serious invasion of privacy because they were not provided with any way to recover the information associated with their disabled account and—at least when their accounts

203. *Hill*, 26 Cal. Rptr. 2d at 859.

204. *See* Digital Music News, 171 Cal. Rptr. 3d at 810.

205. *Id.*

206. *See* Safronova, *supra* note 26 (including a quotation from Lil Miss Hot Mess: "It's not like I'm hiding from the world, but it's important for me to keep these identities separate.")

207. *Id. See also* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237 (Cal. Ct. App. 2008) (noting that use of a pseudonymous screen name offers "a safe outlet for the user to experiment with novel ideas . . . or criticize corporate or individual behavior without fear of intimidation or reprisal.").

208. *See* Lowder, *supra* note 66 ("[M]any queens note that they've used their drag names in their profiles without incident for years.").

were first disabled—were locked out from future pseudonymous communication.[209]

Taken together, the facts of the recent controversy involving Facebook's real names policy and the privacy interest in anonymous online speech as defined by the court in *Digital Music News* suggest that the drag queens kicked off Facebook for creating accounts with their stage names may have been able claim for an invasion of privacy under the privacy clause of the California Constitution.[210] However, the drag queens would likely encounter other issues, such as standing, CDA § 230(c), and their relationship with Facebook as dictated by Facebook's Terms of Service, that may stop their legal challenge from proceeding successfully.[211] This hypothetical legal challenge is merely intended to show how the reasoning of *Digital Music News* could be extended in the future, as well as the ways in which pseudonymous online communication contributes to identity formation. Facebook profiles made using the drag queens' stage names both contribute to their sense of self and allow them to develop their identities over time.

B. COURTS SHOULD SUPPORT TRACEABLE PSEUDONYMITY

Turning to the more general issue of what to do about anonymous online speech, proposals that preserve the ability to communicate anonymously or through a pseudonym should be preferred for the reasons discussed throughout this Note. Solving the trolling problem by de-anonymizing the internet undervalues internet users' identity-formation interests that are fostered by anonymous and pseudonymous online speech.[212] And simply removing the anonymous aspect of the internet does

---

209. *See* Safronova, *supra* note 26 (noting that many drag queens' Facebook accounts were suddenly disabled).

210. *See Hill*, 26 Cal. Rptr. 2d at 843 (determining that the privacy clause created a cause of action against private entities).

211. This challenge against Facebook is also entirely hypothetical because Facebook voluntarily changed its real names policy.

212. *See* Jillian C. York, *A Case for Pseudonyms*, ELECTRONIC FRONTIER FOUND. (Jul. 29, 2011), https://www.eff.org/deeplinks/2011/07/case-pseudonyms; J. Nathan Matias, *Nymrights: Protecting Identity in the Digital Age*, MIT CENTER FOR CIVIC MEDIA (Sept. 30, 2014), https://civic.mit.edu/blog/natematias/nym-rights-protecting-identity-in-the-digital-age:

> Many people use a variety of names. Maybe they're a sex worker who needs to protect their identity. In some cases, people who face judgment and harassment maintain separate identities to maintain safe spaces for conversation. Others use pseudonyms to create divides between their professional and personal lives. People sometime share

not appropriately weigh the justifications provided by courts for protecting the First Amendment rights of anonymous or pseudonymous online speakers. [213] Consider some of the justifications for anonymous online speech that courts have relied upon in the past: online anonymity "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."[214] Online anonymity also "permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment."[215] Using a pseudonymous screen name allows users of any socioeconomic or political status "a safe outlet for the user to experiment with novel ideas, express unorthodox political views, or criticize corporate or individual behavior without fear of intimidation or reprisal."[216] The internet provides "unique opportunities for cultural development[] and myriad avenues for intellectual activity."[217] Finally, the "ability of Internet users to communicate anonymously" drives the free exchange of ideas that has made the Internet so culturally important.[218] And the 9th Circuit recently affirmed these justifications in *Doe v. Harris*, where the court noted that fear of unmasking necessarily chills anonymous online speech—citing to the same cases discussed in this paragraph—including *McIntyre* and *2themart.com*.[219]

> the same name for carrying out a common activity under a shared identity, like publishing a book or hosting at Couchsurfing and Airbnb.

Id.

213. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("[I]n general, our society accords greater weight to the value of free speech than to the dangers of its misuse.").

214. *Id.* at 342.

215. Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

216. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237 (Cal. Ct. App. 2008).

217. Ashcroft v. ACLU, 535 U.S. 564, 566 (2002).

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

219. Doe v. Harris, 772 F.3d 563, 581(9th Cir. 2014) ("[F]ear of disclosure in and of itself chills their speech. If their identity is exposed, their speech, even on topics of public importance, could subject them to harassment, retaliation, and intimidation. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995) ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."); Brown v. Socialist Workers '74 Campaign Comm. (Ohio), 459 U.S. 87, 100 (1982) (holding that disclosure requirements may subject unpopular minority groups to "threats, harassment, and reprisals"). Anonymity may also be important to sex offenders engaged in protected speech because it "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent." *McIntyre*, 514 U.S. at 342; *see also* Doe v. 2TheMart.com

In *Digital Music News*, the court recognized that the right to privacy and the First Amendment right to freedom of speech work together to create a powerful justification for anonymous online speech.[220] Neil Richards' theory of intellectual privacy is a helpful framework to understand the initially surprising argument that freedom of speech and privacy work together instead of at cross-purposes:

> Intellectual privacy is the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others. Surveillance or interference can warp the integrity of our freedom of thought and can skew the way we think, with clear repercussions for the content of our subsequent speech or writing. The ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy. In this way, intellectual privacy is a cornerstone of meaningful First Amendment liberties.[221]

Richards argues that there is no freedom of speech without freedom of thought. And freedom of thought is the ability to make up our minds. Freedom of thought liberates us, giving us the space to construct our own identities. The protection extended to Visitor in *Digital Music News* amounts to the provision of a legally protected zone of intellectual privacy. *Digital Music News* should thus be instructive to future courts faced with anonymous online speech cases.

Considering the constitutional significance of intellectual privacy, future approaches to anonymous online speech that are closer to the "traceable pseudonymity" approach described by Tal Zarsky[222] should be preferred over the schemes proposed by other scholars that solve the problems caused by anonymous online speech by attempting to remove the anonymous aspect of online communication.[223] Indeed, entirely removing the anonymous aspect of the internet could harm marginalized communities[224] and restrict individuals' ability to create and understand

Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) ("Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas.").

220. Digital Music News v. Super. Ct. of L.A. Cnty., 171 Cal. Rptr. 3d 799, 809 (May 14, 2014).

221. Richards, *supra* note 187, at 389.

222. *See* Zarsky, *Thinking Outside the Box*, *supra* note 54, at 1031-32.

223. *See generally* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (Saul Levmore & Martha C. Nussbaum eds., Harvard University Press 2011).

224. Nadia Kayyali, *Privacy, Identity, and Facebook*, S.F. BAY GUARDIAN ONLINE (Sept. 23, 2014), http://www.sfbg.com/2014/09/23/privacy-identity-and-

their identities:[225] "The people who most heavily rely on pseudonyms in online spaces are those who are most marginalized by systems of power."[226] But of course, trolling, cyberbullying, and defamatory content pose significant problems for the internet users that are harmed by them. Traceable pseudonymity balances the need to handle these problems against the constitutionally important dignity and identity interests furthered by anonymous and pseudonymous communication, and is more in line with historical judicial approaches to these issues.

VI. CONCLUSION

The ability to speak online has lowered the barriers to entry for any citizen who seeks to communicate to a broad audience.[227] In order to have something to say, that citizen needs a private space to formulate their ideas and develop their identity.[228] Courts have previously endorsed individuals' right to speak out on important issues and discussed how the act of speaking contributes to the identity of the speaker. Sometimes, the construction of a robust identity requires experimentation in the form of multiple online identities, each attached to a different pseudonym.[229]

As the *Digital Music News* case reveals, the First Amendment and the right to privacy can sometimes work together to protect the identity-construction aspect of anonymous and pseudonymous online speech. If we want the internet to really be a democratic communications medium, we must protect the ability to speak out anonymously, or using a pseudonym. To do otherwise would end "an honorable tradition of advocacy and of dissent."[230]

facebook?page=0%2C0 ("For trans women, who make up 72 percent of the victims of anti-LGBTQ homicide, being forced to reveal their birth names can be deadly.")

225. Jade Sylvan, *Dear Facebook: This is Why Your New 'Real Name' Policy Hurts Queers Like Me*, WASH. POST (Sept. 22, 2014), http://www.washingtonpost.com/posteverything/wp/2014/09/22/dear-facebook-this-is-why-your-new-real-name-policy-hurts-queers-like-me/ (describing how maintaining an online identity that was separate from the author's online identity allowed the author to develop her persona as an artist and LGBTQ activist while remaining safe from violence in the author's religious hometown).

226. Boyd, *supra* note 64.

227. Reno v. ACLU, 521 U.S. 844, 870 (1997).

228. Richards, *supra* note 187, at 389.

229. *See* Tien, *supra* note 180, at 164–65 (explaining how people have multiple selves that contribute to their identity as a singular being).

230. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

As the Supreme Court has noted in the past, "[a]nonymity is a shield from the tyranny of the majority."[231] And pseudonyms are enshrined in United States history as the tools that the nation's Founders used to spread their message of democracy while insulating themselves from political and physical harm.[232] Preserving these tools of advocacy and dissent is critically important for our constitutional rights as American citizens, for allowing us to formulate our own identities, and to preserve a unique and important feature of online communication: speaking to anybody regardless of your social status, where others can weigh your opinions without taking your gender, race, or any other external indicator of who you are into account.

By recognizing that Visitor's identity, in the narrow sense, should be protected in *Digital Music News*, the California Appeals Court has provided a thoughtful approach for understanding how our identities, in the robust sense, should be protected online. Other courts should follow the *Digital Music News* approach to extend affirmative constitutional protection to freedom of thought and communication.[233] In general, courts should support "traceable pseudonymity," where internet users have the right to maintain one or more online pseudonyms, subject to unmasking when a party harmed by the internet user's pseudonymous speech makes a clear case for illegal conduct.[234]

231. *Id.*

232. *Id.* at 367-69 (Thomas, J., concurring).

233. *See* Richards, *supra* note 187, at 408.

234. The *Dendrite* standard could even continue to serve as the framework for determining when to unmask the user, as it balances the interests of the online speaker against the plaintiff harmed by the speech while remaining sensitive to the Constitutional liberties at play. *See generally* Levy, *Developments in Dendrite*, *supra* note 87.