Minnesota Journal of Law, Science & Technology

Volume 23 | Issue 1 Article 3

1-4-2022

Anonymous Expression and "Unmasking" in Civil and Criminal Proceedings

Leeza Arbatman

John Villasenor

Anonymous Expression and "Unmasking" in Civil and Criminal Proceedings

Leeza Arbatman* and John Villasenor†

---

* J.D. Candidate, UCLA School of Law.

† Professor of law, engineering, and public policy, UCLA; director of the UCLA Institute for Technology, Law, and Policy; non-resident senior fellow, the Brookings Institution. We thank Jane Bambauer, Brian Kulp, Madeline Lamo, Laurie Levenson, Paul Alan Levy, Nathaniel Plemons, and Barry Stricke for their valuable feedback on this article. We also thank the librarians at the UCLA Law Library for their research assistance, in particular librarian Rachel Green.

I. INTRODUCTION

Freedom of expression under the First Amendment includes the right to anonymous expression.[1] However, there are many circumstances under which speakers do *not* have a right to anonymity, including when they engage in defamation[2] or when they are providing testimony to a grand jury.[3] This sets up a complex set of tensions that raise important—and as yet unresolved—questions regarding the scope of First Amendment protections for anonymous speech.

At the core of these tensions are frameworks for determining when online anonymous speakers should be "unmasked" so that their true identities may be revealed. In civil litigation, courts in cases involving allegedly defamatory[4] posts on sites such as Yelp have generally used approaches that, to varying degrees, aim to balance the interests of plaintiffs seeking to identify defendants in order to obtain redress with those of defendants who wish to remain anonymous. But despite over two decades of adjudicating such cases, courts have yet to settle on a standard.[5] Furthermore, state legislatures have been reluctant to engage with this issue. While Virginia and Washington D.C. have

---

1. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (holding that the First Amendment protects the right to anonymous expression in relation to political speech).

2. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 269 (1964) ("[L]ibel can claim no talismanic immunity from constitutional limitations. It must be measured by standards that satisfy the First Amendment.").

3. *See* United States v. Calandra, 414 U.S. 338, 345 (1974) ("The power of a federal court to compel persons to appear and testify before a grand jury is . . . firmly established."). More generally, of course, constitutionally unprotected speech does not gain any extra protection simply by virtue of being anonymous. For example, true threats (Virginia v. Black, 538 U.S. 343 (2003)), incitements to imminent lawless action (Brandenburg v. Ohio, 395 U.S. 444 (1969)), copyright infringement, etc. are all unprotected, regardless of whether a speaker is anonymous.

4. Of course, defamation is not the only form of unprotected speech that arises in civil litigation involving unmasking demands. Another example is copyright infringement, i.e., when a rights-holding plaintiff is attempting to ascertain the identity of a person who has posted allegedly infringing material.

5. *See infra* Part III.

statutes addressing procedures for unmasking,[6] in the vast majority of states unmasking is addressed in the absence of any statutory framework.

This landscape has created both uncertainty and inefficiency for over two decades. Uncertainty arises because only a minority of jurisdictions have clear precedents,[7] meaning that both plaintiffs and parties arguing on behalf of anonymous defendants have little ability to predict which of the many possible approaches to unmasking a particular court will ultimately decide to adopt.[8] The lack of clarity also leads to inefficiency, as state and federal trial and appellate courts repeatedly grapple with variations on the same question of how to balance a plaintiff's interest in unmasking with the rights of defendants or third parties to remain anonymous, often arriving at different answers despite similar underlying fact patterns.

To further complicate matters, the question of what rules should govern unmasking can also arise in criminal proceedings in relation to grand jury investigations.[9] In the only published circuit court decision to date addressing this question, the Ninth Circuit held in 2017 in *In re Grand Jury Subpoena, No. 16-03-217, United States v. Glassdoor*[10] (hereinafter *Glassdoor*) that grand jury subpoenas seeking the identity of anonymous online

---

6. VA. CODE ANN. § 8.01-407.1*;* D.C. CODE § 16–5503. The D.C. statute is narrow, applying only to claims "arising from an act in furtherance of the right of advocacy on issues of public interest." There is also a California statute (CAL. CIV. PROC. CODE § 1987.2(c)) regarding unmasking, but it pertains only to the issue of when a California court should award attorney's fees and other expenses incurred in moving to "quash or modify a subpoena from a court of this state for personally identifying information" sought from an "interactive computer service" in relation to "an action pending outside the state."

7. Paul Alan Levy, *Legal Perils and Legal Rights of Internet Speakers: An Outline with Citations*, 18–19, https://mkus3lurbh3lbztg254fzode-wpengine.netdna-ssl.com/wp-content/uploads/internetlegalrightsoutlineV3-2.pdf (last visited Nov. 18, 2021).

8. *See infra* Part III. As will be discussed, one of the few jurisdictions in which there is a clear precedent is Delaware, where the Delaware Supreme Court squarely addressed the unmasking issue in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005).

9. Of course, unmasking questions can also arise in relation to criminal proceedings outside of grand jury investigations. The discussion herein, *infra* Part III, focuses on grand jury investigations as that was the context for *Glassdoor*.

10. 875 F.3d 1179, 1188 (9th Cir. 2017).

speakers are valid so long as the investigation is conducted in good faith.[11]

Previous scholarship on unmasking has primarily focused on the civil context, expressing support[12] or criticism[13] for the various tests articulated in civil cases for evaluating whether an anonymous speaker's identity should be revealed, suggesting new ways for how these tests should be applied,[14] highlighting the lack of legislative attention this issue has received,[15] and asserting the need for Supreme Court guidance in order for anonymous online speech to be adequately protected.[16] With

---

11. *Id.* at 1990. Good faith is presumptively present in grand jury proceedings, and thus has no direct analog in civil litigation, where the issue of good faith can be examined, but it is not assumed. Thus, the question of whether a grand jury proceeding is being conducted in good faith is very different from the inquiry that some (but certainly not all) courts perform in relation to unmasking demands in civil litigation regarding whether plaintiffs have a good faith belief that they have been injured by legally actionable speech.

12. *See, e.g.*, Taylor McMallman, *The Shadow in the Comments Section: Revealing Anonymous Online Users in the Social Media Age*, 41 CAMPBELL L. REV. 225, 246 (2019) ("The approach suggested by [the] *Anonymous Online* [court] implicitly considers the type of speech at issue as a basis for revealing the defendant's identity . . . . If determining the [appropriate unmasking] standard was based on the type of speech, the unpredictability that arises from a wide-open value determination would be substantially reduced, if not cease to exist." (footnote omitted)).

13. *See, e.g.*, Kelly Waldo, *Signature Mgm't Team LLC v. Doe: The Right to Anonymous Speech Post-Judgment*, 19 N.C. J.L. & TECH. 253, 276 (2018) ("The [*Signature Management*] court's formulation of . . . [a] presumption in favor of unmasking does not show sufficient caution when deciding whether to reveal an identity, a move from which there is no going back.").

14. *See, e.g.*, Nathaniel Plemons, *Weeding Out Wolves: Protecting Speakers and Punishing Pirates in Unmasking Analyses*, 22 VAND. J. ENT. & TECH. L. 181, 208 (2019) ("Currently, many courts that have confronted plaintiffs seeking to unmask anonymous internet speakers have settled on either adopting or adapting one of two analyses: the *Dendrite* or *Cahill* approach . . . . [N]either of these approaches consider the strong legal basis for and overwhelming practical importance of lowering the plaintiff's burden to unmask anonymous [intellectual property] infringers. The test that best balances plaintiff and anonymous internet speaker interests is a *Dendrite* approach that implements a rebuttable presumption in favor of the plaintiff in IP infringement cases." (footnote omitted)).

15. *See, e.g.*, Ethan B. Siler, *Yelping the Way to a National Statutory Standard for Unmasking*, 51 WAKE FOREST L. REV. 189, 199–200 (2016) (underscoring the limited attention that state legislatures have given this issue) (footnote omitted).

16. *See, e.g.*, Jonathan Turley, *Registering Publius: The Supreme Court and the Right to Anonymity*, CATO SUP. CT. REV. 57, 82 (2002) ("The failure of the

respect to unmasking in relation to criminal proceedings, there is a noteworthy gap in both case law and scholarship. Just a few law review articles to date mention *Glassdoor*, and all only in passing.[17] And while there is some published commentary on *Glassdoor*,[18] there has been little legal scholarship devoted to analyzing its implications in detail.

Court to be clearer on the foundations and standard for a right to anonymity leaves a dangerous ambiguity when privacy and confidentiality are under increased attack. Just as the Court succeeded recently in reinforcing the long-neglected right of association, it was hoped that it would draw a bright line of protection around anonymous speech. It may still do so . . . . [T]he Court is inching closer to a clear and unambiguous recognition of anonymity, not as an 'aspect' or a 'condition,' but as a right of free speech and freedom of the press.") (footnote omitted).

17. *See, e.g.*, Evan Caminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 477 n.312 (mentioning *Glassdoor* as an example of how "[c]ourts moved to protect personal privacy interests implicated by subpoenas issued to corporations" will "do so, if at all, by ensuring the information is requested in good faith or tightening the required showing of relevance—not by requiring a showing of anything approaching probable cause"); Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. REV. 988, 1022 n.215 (2019) (noting in their discussion of why society should act cautiously when regulating bot speech that "[w]hile the Ninth Circuit's *Glassdoor* ruling has already been the subject of extensive criticism for its failure to take the unique qualities of online speech into account . . . it remains to be seen whether the Supreme Court will intervene"); Barry Stricke, *People v. Robots: A Roadmap for Enforcing California's New Online Bot Disclosure Act*, 22 VAND. J. ENT. & TECH. L. 839, 891 (2020) (citing *Glassdoor* in analyzing California's online bot disclosure act as an example of when a third-party publisher was unable to block a subpoena to protect its users' anonymity).

18. *See, e.g.*, Aaron Mackey & Sophia Cope, *Appeals Court's Disturbing Ruling Jeopardizes Protections for Anonymous Speakers*, ELEC. FRONTIER FOUND. (Nov. 14, 2017), https://www.eff.org/deeplinks/2017/11/appeals-courts-disturbing-ruling-jeopardizes-protections-anonymous-speakers ("The Ninth Circuit's decision in *U.S. v. Glassdoor, Inc.* is a significant setback for the First Amendment."); Brian Kulp, *US v. Glassdoor: Ninth Circuit Compels Website to Disclose Anonymous Users' Identities*, JOLT DIGEST (Nov. 20, 2017), https://jolt.law.harvard.edu/digest/us-v-glassdoor-ninth-circuit-compels-website-to-disclose-anonymous-users-identities ("The setback for anonymity of online speech could have a wide-reaching impact as the [*Glassdoor*] decision sends ripples out from the Ninth Circuit."); Minda Zetlin, *Federal Court Will Decide—in Secret—Whether to Unmask Anonymous Glassdoor Reviewers*, INC. (Jul. 21, 2017), https://www.inc.com/minda-zetlin/federal-court-is-deciding-in-secret-whether-onli.html (lamenting the fact "that [the *Glassdoor*] decision . . . [was] being made behind closed doors" and that the public would potentially "not know anything about it until well after the decision ha[d] been made"); Lisa A. Hayes, *Anonymous Speech Online Dealt a Blow in U.S. v. Glassdoor Opinion*, CTR. FOR DEMOCRACY & TECH. (Nov. 8, 2017),

Against this backdrop, there is also another recent and concerning development: As part of the broader discussion about potential new regulation of social media companies, proposals have been made in Congress and in the pages of the *Wall Street Journal* to mandate banking industry-style identity verification to users creating new accounts on social media services.[19] While these proposals target the process of *creating* accounts on social media companies, as opposed to *using* accounts to post pseudonymously, they are clearly intended to make it easier for plaintiffs to unmask the people behind pseudonymous postings deemed problematic.

Given that the Supreme Court has confirmed that both online speech[20] and anonymous speech[21] are protected by the First Amendment, state or federal legislation aimed specifically at undermining the ability to speak anonymously online would clearly run into constitutional challenges. But the fact that such proposals are even being contemplated demonstrates both the timeliness and importance of greater attention in the legal academic press to online anonymous speech.

To that end, this Article articulates a set of approaches that would enable far more clarity, consistency, and balance than has heretofore been present in court proceedings involving unmasking demands. With respect to civil litigation, the Article provides an overview and comparison of the approaches

---

https://cdt.org/blog/anonymous-speech-online-dealt-a-blow-in-us-v-glassdoor-opinion ("If [*Glassdoor*] stands, it will have far-reaching consequences for the ability of companies to protect anonymous speech online.").

19. *See, e.g.*, Andy Kessler, *Online Speech Wars Are Here to Stay*, WALL ST. J. (Jan. 24, 2021, 5:15 PM), https://www.wsj.com/articles/online-speech-wars-are-here-to-stay-11611526491 (suggesting legislation should compel social media companies to follow "know your customer" requirements inspired by analogous requirements in the financial industry); *see also* Ron Johnson (@SenRonJohnson), TWITTER (Jan. 26, 2021, 4:04 PM), https://twitter.com/SenRonJohnson/status/1354218776670203905 ("One solution may be to end user anonymity on social media platforms. Social media companies need to know who their customers are so bad actors can be held accountable.").

20. Reno v. Am. Civ. Liberties Union, 521 U.S. 844, 870 (1997) (holding that the First Amendment protects online speech).

21. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[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.").

articulated to date, arguing that the best approach is a prima facie standard inspired by a 2001 New Jersey court ruling (*Dendrite International, Inc. v. Doe No. 3*),[22] but augmented by a more specific balancing test based on a set of three factors: (1) the type of speech at issue; (2) whether the anonymous speaker is a party to the litigation; and (3) the comparative harms that would result from making an incorrect unmasking decision.

The Article also analyzes unmasking in grand jury proceedings, endorsing the approach used by the Western District of Wisconsin in *In re Grand Jury Subpoena to Amazon.com Dated 7, 2006*.[23] In that decision, the court fashioned a filtering mechanism to limit the power and scope of a government subpoena, protecting the First Amendment rights of anonymous Amazon customers while still giving the government the ability to identify witnesses for its investigation.[24] This approach is more protective than that used in *Glassdoor* and comports more properly with the underlying First Amendment considerations that arise (though in different form) in both civil and criminal proceedings.

The remainder of this Article proceeds as follows: Part II provides an overview of the technological aspects of how users' digital communications platforms and services are unmasked and also briefly notes some pre-digital-era precedents regarding anonymous speech. Part III presents a table and discussion comparing various approaches to unmasking in civil litigation. It then provides an analysis of the *Glassdoor* decision and its implications. Part IV presents recommendations for addressing unmasking in civil (and separately) criminal cases. Conclusions are presented in Part V.

II. TECHNOLOGICAL AND HISTORICAL CONTEXT

A. THE TECHNOLOGY OF UNMASKING

While the term "anonymous" is often used (including in this Article) to describe online postings in which publishers wish to hide their identity, as a strictly technical matter such postings are nearly always pseudonymous. True anonymity is extremely difficult to achieve online. Far more commonly, people who wish

22. 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).
23. 246 F.R.D. 570 (W.D. Wis. 2007).
24. *Id.*

to keep their identities private publish under pseudonyms, or use websites like Techdirt that do not require users to register before posting comments. The information necessary to tie a pseudonym to the person behind it is generally (though not always) available in the internal logs of the communications services and devices used for the publication.

Consider what happens when reviewers post reviews on Yelp of businesses they have frequented. Reviewers can publish using screen names that may have little or no clear connection to their real names. But that connection can nonetheless be made through a combination of information from one or more of Yelp, an internet service provider, a mobile phone company, and the device used by the user.[25] Each time a user of Yelp (or of any other online service) signs on and engages with the service, records are created that can typically identify the person and or the device that made the connection.

For instance, consider a person posting to Yelp from a laptop computer connected to a wireless network located in a workplace. When connected to the internet, the laptop computer will be associated with a public[26] internet protocol (IP) address known to the internet service provider. This association is often indirect. It is common for businesses (and homes, etc.) to receive internet service using a particular public IP address used for communication from an internet service provider to a router

---

25. *Cf.* Cale Guthrie Weissman, *What is an IP Address and What Can It Reveal about You?*, INSIDER (May 18, 2015), https://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5 (describing what an IP address does and does not reveal).

26. The term "public" here does not mean that any member of the public could look up the IP address online and trace it to a specific home or business address. Rather, it means that the fact that a given IP address is among those used by a particular internet service provider (ISP) would be a matter of public record, though the specific way in which an ISP chooses to allocate IP addresses to its customers is not generally public. *See* Tim Fischer, *What is a Public IP Address?*, LIFEWIRE (Sept. 9, 2021), https://www.lifewire.com/what-is-a-public-ip-address-2625974. However, the information to tie a particular IP address to a particular street address typically is available within the ISP's own internal records, and thus accessible to litigants through legal process. *See* Weissman, *supra* note 25 (describing an instance "where the authorities, knowing only the IP address, contacted the ISP and were able to find the identity of a person sending harassing emails").

located in a particular building.[27] Within a company or residence, there is often also an internal, private network that is used to allow multiple devices to connect to the router, and from there to the internet.[28]

In the case of a user posting to Yelp from a laptop computer on a company wireless network, Yelp would know the username (and other account information) of the user as well as the IP address being used to communicate with the user. Even if the user were to register for a Yelp account by providing a false name and an e-mail address created for the sole purpose of facilitating anonymous posting to Yelp, the communications with Yelp would still be traceable using the IP address to a particular router. That router in turn would often be associated with a private subnetwork of devices internal to the company. Within that subnetwork, each device would have its own unique address known to the router, though not to the ISP.

In this scenario, identifying a particular laptop computer used to communicate via a company wireless network with Yelp would, from a technological standpoint, require several steps. The first step would involve obtaining from Yelp the IP address and therefore the location of the router being used for the communications. The second step could involve obtaining records from within the router. These records would provide device address data for the internal (to the company) network and time stamps to identify the specific laptop computer used in the Yelp posting.[29]

And in the scenario above, there is an additional way that the user's identity might be ascertained: Suppose that the user

---

27. *See* Weissman, *supra* note 25 ("Routers, instead, connect to individual computers, and it's the routers that then connect to the rest of the internet using their own individual IP address.").

28. *See id.* ("Think of routers as the bridge between the network within your house (or business, library, coffee shop, etc.) and the outside world network (that is, the internet).").

29. The foregoing description is exemplary, but by no means limiting. There are many other variations on how devices such as laptop computers connect to the internet. For instance, virtual private networks add an additional layer of complexity. In addition, there are many wireless networks (such as those in airports, restaurants, and public buildings) in which identifying the specific person who accessed the internet using the network could be more difficult. However, unless an internet user has gone to significant lengths to electronically mask their identity, it is usually possible, given sufficient access and resources, to identify which specific computer was used in relation to internet activity that has come under scrutiny.

created a special e-mail address to use only for posting to Yelp. The fact of creating and using that address would also facilitate identification. For instance, if the user creates and uses a custom Gmail account for this purpose, a subpoena to Google would reveal information about the IP address(es) used to create and utilize the associated e-mail address—and from there it would often be fairly straightforward to identify the individual behind the e-mail account.

Of course, there are also tools available for people wishing to hide their online identity by thwarting the technological unmasking approaches described above. Tor, for example, is a browser that intentionally promotes anonymity by routing internet traffic through a series of intermediary nodes so that the web site being accessed (e.g., Yelp) only knows the identity of the node in the chain that it directly communicates with—and does not know the identity of the upstream nodes, including the computer of the Tor user.[30] Alternatively, or in addition, a user might choose to register for and access an online service using a mobile phone specifically procured for anonymity (i.e., a phone for which there is no database at a mobile network company tying the user to the phone).[31]

When anonymity-conferring tools such as Tor or "burner" mobile phones are used, unmasking involves both legal and technical barriers. Even if a court concludes that a user posting to the internet via Tor should be unmasked, it would not know who to name in an order to actually do the unmasking. An additional complication is that many of the nodes in a Tor network may be overseas, raising jurisdictional challenges.[32] However, the overwhelming majority of internet users do not go to such lengths to remain anonymous. This Article therefore focuses on unmasking as a legal question, while also recognizing

---

30. Aliya Chaudhry, *How to Use the Tor Browser's Tools to Protect Your Privacy*, THE VERGE (Feb. 21, 2020), https://www.theverge.com/2020/2/21/21138403/tor-privacy-tools-private-network-browser-settings-security.

31. This mobile phone scenario assumes that the user would access the internet only using the cellular network, as using nearby Wi-Fi access points would lead to the same unmasking procedures described in the previous paragraphs.

32. From a strictly legal standpoint, the use of overseas servers to provide electronic communication with a U.S. user provides a nexus that might resolve the jurisdictional question. But that would still leave the *practical* challenge of obtaining information from these servers.

that there are circumstances where a court ordering unmasking could also face technological hurdles.

Most of the case law on unmasking has arisen in civil litigation. This is a direct consequence of the enormous growth in online platforms that allow users publicly identified only by pseudonyms to publish on the internet, and the resulting expansion in the amount of content hosted by such sites.

To take one example, Yelp was founded in 2004.[33] It was home to one million reviews by 2007, 100 million reviews by 2016, and 200 million reviews by 2019.[34] Between Q4 2019 and Q4 2020, the total number of reviews on Yelp grew by 19 million, corresponding to about 52,000 new reviews per day.[35] Given that volume, it is inevitable that some owners of businesses reviewed on Yelp will conclude, rightly or wrongly, that they have been defamed. It is also inevitable that some subset of them will choose to pursue litigation, knowing that unmasking a defendant is a necessary step to succeed on a claim.

Yelp is far from the only web site that hosts content that might lead to an unmasking demand. Twitter is another such site.[36] Twitter users have enormous latitude in choosing their "handles"—that is, the username by which the account is publicly known. Some Twitter accountholders choose handles that unambiguously identify the owners of the account—for example, handles like @nytimes and @elonmusk leave no doubt about who actually owns an account. But some Twitter users post using handles that do not convey the identity of the account owner. When tweets from such accounts lead to legal action, unmasking becomes a key goal of the litigation.[37]

---

33. *Fast Facts*, YELP, https://www.yelp-press.com/company/fast-facts/default.aspx (last visited February 23, 2021).

34. *Id*.

35. *Id*.

36. Facebook, on the other hand, requires accountholders to use their real names. *See What Names are Allowed on Facebook?*, FACEBOOK HELP CTR., https://www.facebook.com/help/112146705538576 (last visited Nov. 17, 2021) ("The name on your Facebook account should be the name that your friends call you in everyday life. This name should also appear on an ID or document from our ID list.").

37. To take one example, in 2019 Rep. Devin Nunes (R-CA) filed a defamation claim in a Virginia court naming (among other defendants, including Twitter) the owners of two Twitter accounts, identified in the complaint only by their handles. Complaint, Nunes v. Twitter, Inc., No. C49-

While unmasking demands are a common feature of online defamation cases, they can also arise in relation to allegations of trademark infringement, breach of confidentiality obligations, copyright infringement, and more. The content in question is often published through internet services such as Yelp and Twitter that host third-party postings, but can also be published through other mechanisms, e.g., by a defendant publishing through its own web site.

B. ANONYMOUS AND ONLINE SPEECH

Anonymous speech has played a vital role since (and before) the founding of the United States. As Allison Hayward has written: "From the United States' earliest days, speakers addressing controversial public questions have sought anonymity. The authors of the Federalist Papers, which supported ratification of the Constitution, published under the pseudonym Publius, and the revolutionary-era pamphleteers had published under assumed names, often to escape prosecution."[38]

The right to anonymous expression is closely tied to another right grounded in, though not explicitly stated in, the First Amendment: that of free association.[39] Association involves

---

1715 (Va. Cir. Ct. Mar. 18, 2019), https://www.courthousenews.com/wp-content/uploads/2019/05/nunes-complaint.pdf. The complaint anticipated that unmasking would be a part of the litigation, stating that "[t]he Twitter attacks on Nunes were pre-planned, calculated, orchestrated, and undertaken by multiple individuals acting in concert, over a continuous period of time exceeding a year. The full scope of the conspiracy, including the names of all participants and the level of involvement of donors and members of the Democratic Party, is unknown at this time and will be the subject of discovery in this action." *Id*. at *23. In June 2020, a judge ruled that Twitter was shielded by Section 230 from liability for posts by its users. Brian Fung, *Nunes Cannot Sue Twitter Over Accounts Posing as his Mother and a Cow, Judge Rules*, CNN (June 24, 2020), https://www.cnn.com/2020/06/24/politics/devin-nunes-twitter-lawsuit-cow/index.html; *see also* 47 U.S.C. § 230 (protecting online platforms from liability for content users post to their platforms).

38. Allison Hayward, *Anonymous Speech*, THE FIRST AMEND. ENCYCLOPEDIA (June 2017), https://www.mtsu.edu/first-amendment/article/32/anonymous-speech.

39. *See, e.g.*, United Transp. Union v. State Bar of Michigan, 401 U.S. 576, 578–79 (1971) ("We held in [Brotherhood of Railroad Trainmen v. Virginia State Bar, 377 U.S. 1 (1964)] that the First Amendment guarantees of free speech, petition, and assembly give railroad workers the right to cooperate in helping and advising one another in asserting their rights under the [Federal

discourse, and in some cases may involve discourse among persons who wish to keep their identities hidden from non-participants, and sometimes even from each other as well.[40] As such, pre-digital analogs to contemporary unmasking questions often arose through government attempts to compel disclosure of associational relationships.

In the mid-20th century, the Supreme Court issued a series of decisions stemming from McCarthy-era investigations by the House Committee on Un-American Activities and from broader government investigations of the NAACP's civil rights advocacy. In *Watkins v. United States*,[41] *NAACP v. Alabama*,[42] and *Bates v. Little Rock*,[43] the Court blocked the government's attempts to compel disclosures of membership lists. On the other hand, in *Barenblatt v. United States*,[44] the Court sided with the government after Barenblatt was held in contempt of Congress for refusing to disclose information regarding whether he and another person were members of the Communist Party.[45]

All of these cases addressed a form of unmasking, though not in the digital context in which it most commonly occurs today: The government sought to obtain the identities of people who, through their association with one another, were engaged in activities—including expression—that the government deemed concerning. Their identities were sought primarily because of government interest in the organizations to which they belonged. In other words, it was the *fact* of their membership, not the authorship of any particular published statement, that the government wished to ascertain.

Employers' Liability Act]. While not deciding every question that possibly could be raised, our opinion left no doubt that workers have a right under the First Amendment to act collectively to secure good, honest lawyers to assert their claims against railroads.").

40. For instance, as will be discussed in more detail *infra*, consider a Facebook group for persons who have a particular rare medical condition. Anonymity allows participants in the group to retain their medical privacy—including from one another—while still benefiting from being members of that online community.

41. 354 U.S. 178 (1957).

42. 357 U.S. 449 (1958).

43. 361 U.S. 516 (1960).

44. 360 U.S. 109 (1959).

45. *Id*. at 113–15.

This contrasts with the frequently encountered form of unmasking in the digital era, where a plaintiff in a civil case, or the government in a criminal case, is attempting to connect the dots between public online expression and the non-public identity of the person who authored it. Contemporary cases are thus different from those of the mid-twentieth century, as they often involve speakers who have elected to speak publicly under the protections of anonymity that digital technology can facilitate and that an adverse party seeks to use the legal system to remove. And while the growth of online expression has changed many things, it has not changed the underlying fact that such speech is presumptively protected: In *Reno v. ACLU*,[46] a 1997 decision arising from a challenge to the Communications Decency Act (CDA),[47] the Court struck down much of the CDA and offered a broader conclusion regarding the scope of online freedom of expression: "[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[48]

The landscape regarding online anonymity will also be influenced by *Americans for Prosperity Foundation (AFPF) v. Bonta, Attorney General of California*, a 2021 Supreme Court decision that addressed a related but different issue, associational privacy rights in relation to information collected by the government about charitable donors.[49] *AFPF* arose out of a challenge to a California law requiring tax-exempt charities to submit confidential lists of their major donors' names and addresses.[50] The AFPF contended that this requirement violates freedom of association rights as recognized in *NAACP v. Alabama*.[51] California argued that the requirement is necessary to prevent fraud.[52] In finding for AFPF, the Court wrote "[w]e are left to conclude that the Attorney General's disclosure

46. 521 U.S. 844 (1997).

47. The CDA was Title V of the Telecommunications Act of 1996 (Pub. L. No. 104-104, 110 Stat. 56 (1996)).

48. *Reno*, 521 U.S. at 870.

49. 141 S. Ct. 2373 (2021).

50. *Id.* at 2379–80.

51. Brief for Petitioner at 1, 2, AFPF v. Bonta, 141 S. Ct. 2373 (2021) (No. 19-251), 2021 WL 722924, at *1, *2.

52. Brief for Respondent at 1, AFPF v. Bonta, 141 S. Ct. 2373 (2021) (No. 19-251, 19-255), 2020 WL 7345503, at *4.

requirement imposes a widespread burden on donors' associational rights . . . . We therefore hold that the up-front collection of [donor information] is facially unconstitutional."[53] While this decision addressed disclosures to the government in relation to charitable giving, the Court's strong support for associational privacy rights will undoubtedly influence lower courts in future online unmasking cases.

Finally, it is important to note that the right to anonymous speech is not monolithic; rather, some forms of speech, and therefore some forms of anonymous speech, get more protection than others. The *McIntyre v. Ohio Elections Commission* Court gave a nod to these variations in 1995 when it wrote in relation to "core political speech" that "[n]o form of speech is entitled to greater constitutional protection."[54] By contrast, there is less protection for anonymous commercial speech,[55] that is defamatory,[56] infringes copyright,[57] or violates criminal law. For instance, a state can criminalize incitement to imminent lawless action, or the making of certain threats, without running afoul of the First Amendment.[58]

---

53. AFPF, 141 S. Ct. at 2389.

54. 514 U.S. 334, 347 (1995).

55. Cent. Hudson Gas v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 563 (1980) ("The Constitution . . . accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.").

56. Of course, a defendant can only be held liable for defamation of a public or private figure if he or she made the statements at issue with the requisite mental state. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (holding that a public official can only recover for defamation if the statements were made with "actual malice"); Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974) (broadening the "actual malice" standard to encompass public figures, not just public officials).

57. Copyright infringement is most often addressed through civil litigation, though it is also addressed through criminal statutes. *See, e.g.*, 17 U.S.C. § 506(a).

58. *See*, *e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (holding that speech advocating illegal activity is punishable only if it is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action"); *see also* 18 U.S.C. § 875.

III. ONLINE UNMASKING APPROACHES

A. UNMASKING IN CIVIL LITIGATION

While there are many examples of recent litigation involving unmasking, some of the most-used approaches were created in rulings dating from the early growth years of the internet, as that is when courts first began grappling with complaints filed against defendants known only by online pseudonyms. Courts in recent years have consistently looked to (but have not always adopted the approaches used in) these early cases as they fashion their own responses to demands by plaintiffs to unmask defendants.

1. Comparing Civil Unmasking Standards

The table below provides an overview and comparison of the standards most commonly articulated in civil cases that have been relied on by courts, and also includes the Virginia unmasking statute.[59] The statute and standards are listed in order of least protective of anonymous speech to most protective.[60]

---

59. An analogous, though less detailed, table was provided in Daniel J. Solove & Paul M. Schwartz, *Privacy and the Media*, *in* PRIVACY LAW FUNDAMENTALS 1, 9-10 (3d ed. 2017). We have not included the D.C. or California statutes in this table because, as explained earlier (*see supra* note 6), the D.C. statute applies only to claims regarding "the right of advocacy on issues of public interest," and the California statute does not provide a standard for unmasking, and is instead limited only to the issue of attorney's fees.

60. All of the cases detailed in this table deal with unmasking in the discovery context. By contrast, the Sixth Circuit recently addressed post-judgment unmasking in *Signature Mgmt. Team, LLC v. Doe,* 876 F.3d 831 (6th Cir. 2017). The court explained that at this stage, there is a presumption in favor of unmasking similar to the presumption of access to judicial records and that courts "must consider both the public interest in open records and the plaintiff's need to learn the anonymous defendant's identity in order to enforce its remedy." *Id.* at 837. The court outlined factors weighing in favor of unmasking—namely, if the expression reaches a large number of people, if it concerns a well-known or public figure, if it is not protected (e.g., defamatory), and if the plaintiff needs to enforce an ongoing injunction. *Id.* Factors weighing against unmasking include "engag[ing] in substantial protected speech that unmasking would chill" and if a defendant named in an unmasking demand has already "willingly participated in litigation and complied with all relief ordered." *Id.*

UNMASKING STANDARDS: CIVIL LITIGATION	
Case/Statute	**Standard**
VA. CODE ANN. § 8.01-407.1 (2002): Identity of Persons Communicating Anonymously Over the Internet	**Showing That the Conduct *May Be* Tortious or Illegal** The Virginia statute requires, among other things, showing "that one or more communications that are or may be tortious or illegal have been made by the anonymous communicator, or that the party requesting the subpoena has a legitimate, good faith basis to contend that such party is the victim of conduct actionable in the jurisdiction where the suit was filed."[61]
In re Subpoena Duces Tecum to America Online, Inc.[62] (Va. Cir. Ct. 2000) (*America Online*)	**Good Faith** A third-party platform can be ordered to unmask an anonymous defendant if: (1) "the court is satisfied by the pleadings or evidence supplied to that court[;] (2) . . . the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed[;] and (3) the subpoenaed identity information is centrally needed to advance that claim."[63]
Columbia Insurance Co. v. Seescandy.com[64] (N.D. Cal. 1999) (*Seescandy.com*)	**Motion to Dismiss** To unmask an anonymous defendant, the plaintiff must: (1) Identify the missing party with "sufficient specificity;"

61. VA. CODE ANN. § 8.01-407.1 (2002).

62. 52 Va. Cir. 26, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds*, 542 S.E.2d. 377 (Va. 2001).

63. *Id.* at *8.

64. 185 F.R.D. 573 (N.D. Cal. 1999).

	(2) "identify all previous steps taken to locate the elusive defendant" in order to ensure that they made "a good faith effort to comply with the requirement of service of process and specifically identifying defendants;" (3) establish that the suit can survive a motion to dismiss; and (4) file a discovery request, showing the "limited number of persons or entities" who will be served and why the information sought is necessary.[65]
Doe v. 2TheMart.com, Inc.[66] (W.D. Wash. 2001) (*2TheMart.com)*	**Between Motion to Dismiss and Prima Facie** In determining if it should grant or deny a motion to quash a subpoena, the court considers whether: "(1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[67] Some courts have found this standard appropriate when the anonymous speaker is not a party to the suit.[68]

65. *Id.* at 578–80.

66. 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

67. *Id.* at 1095.

68. *See*, *e.g.*, Rich v. Butowsky, Case No. 20-mc-80081-DMR, 2020 WL 5910069 (N.D. Cal. Oct. 6, 2020); Sedersten v. Taylor, No. 09–3031–CV–S–GAF, 2009 WL 4802567 (W.D. Mo. Dec. 9, 2009); Enterline v. Pocono Med. Ctr., 751 F. Supp. 2d 782 (M.D. Pa. 2008).

In re Anonymous Online Speakers[69] (9th Cir. 2011) (*Anonymous Speakers*)	Court suggests that the nature of speech should dictate what standard applies.[70] In so doing, it rejects a broad application of *Cahill* (see below).
Doe v. Cahill[71] (Del. 2005) (*Cahill*)	**Summary Judgment** To unmask an anonymous defendant: (1) The plaintiff "must introduce evidence creating a genuine issue of material fact for all elements of a defamation claim *within the plaintiff's control*[;]"[72] and (2) to the extent possible, "the plaintiff must undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure . . . [and must] withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the discovery request."[73]
Highfields Capital Management, L.P. v. Doe[74] (N.D. Cal. 2005) (*Highfields*)	**Prima Facie** In determining if it should grant or deny a motion to quash a subpoena, the court considers whether: (1) There is a "real evidentiary basis" for believing that the speaker "engaged in wrongful conduct that has caused real harm[;]"[75] (This means "the plaintiff must adduce *competent evidence*—and the evidence plaintiff adduces must address *all* of the inferences of fact that plaintiff would need to prove in order to prevail

69. 661 F.3d 1168 (9th Cir. 2011).
70. *Id.* at 1177.
71. 884 A.2d 451 (Del. 2005).
72. *Id.* at 463 (emphasis in original).
73. *Id.* at 460–61.
74. 385 F. Supp. 2d 969 (N.D. Cal. 2005).
75. *Id.* at 975.

	under at least one of the causes of action plaintiff asserts.")[76] (2) (If the answer to #1 is yes) the "magnitude of the harms that would be caused to the competing interests by a ruling in favor of plaintiff and by ruling in favor of defendant."[77] *Highfields* is quite similar to *Dendrite* (below), though—in contrast with *Dendrite*—it does not require notice to the defendant or a separate step showing that the plaintiff can survive a motion to dismiss.[78] It does, however, ask the court to engage in a similar, vague balancing analysis.[79] The Northern District of California's (where many unmasking cases have arisen) tends to use *Highfields* as opposed to *Dendrite*.[80]
Dendrite International, Inc. v. Doe No. 3[81] (N.J. Super. Ct. App. Div. 2001) (*Dendrite*)	**Prima Facie** To unmask an anonymous defendant: (1) The plaintiff must "undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure," and the court must "withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application[;]"[82]

76. *Id.* (emphasis in original).

77. *Id.* at 976.

78. *Compare id.* at 974–81 (analyzing unmasking without requiring notice or showing the ability to survive a motion to dismiss), *with* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001) (requiring notice and a showing of the ability to survive a motion to dismiss).

79. *Highfields*, 385 F. Supp. 2d at 980–81.

80. *See, e.g.*, Tokyo Univ. of Soc. Welfare v. Twitter, Inc., No. 21-MC-80102-DMR, 2021 WL 4124216, at *4–5 (N.D. Cal. Sept. 9, 2021) (applying *Highfields*).

81. 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

82. *Id.* at 760. The court explained that this notification effort "should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board." *Id.*

	(2) the plaintiff must present the specific statements that are purportedly actionable;[83] (3) the plaintiff must establish "that its action can withstand a motion to dismiss for failure to state a claim for which relief can be granted[;]"[84] (4) "the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis[;]"[85] and (5) if the "court concludes that the plaintiff has presented a prima facie cause of action," it must weigh the defendant's First Amendment right of anonymous speech with the strength of the evidence presented against him and the need for disclosure to allow the plaintiff to proceed with his cause of action.[86]

2. Clarifying the Terminology

Courts—and therefore the table above—use terminology such as "good faith," "prima facie," "motion to dismiss," and "summary judgment" as a shorthand to convey the varying burdens that different courts have placed on plaintiffs seeking unmasking. While convenient, these terms also mask complexities and risk oversimplifying what in fact are approaches that cannot be fully categorized with a single term. For instance, while both *Highfields* and *Dendrite* are in the prima facie category, they involve significantly differing procedural steps.

There can also be potential confusion as two of these terms—motion to dismiss and summary judgment—actually refer to the need for a plaintiff to provide sufficient information to *survive* a hypothetical motion (i.e., a motion to dismiss or a motion for summary judgment, respectively) made by an

83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.* at 760–61.

opposing party. There is no requirement in these standards that such a motion actually be made and ruled on; rather the terms are used to convey the level of robustness that must be present in the claim in order for unmasking to proceed.[87] By contrast, evaluating "good faith" does not require considering what an opposing party might argue to defeat a motion, but it does, by definition, require consideration of the state of mind of the plaintiff. An additional complexity arises because "prima facie" in this context can mean different things. For instance, *Dendrite* requires not only that the court make the binary (i.e., yes or no) assessment of whether the plaintiff has presented a prima facie case, but if that assessment is made in the affirmative, also that the court evaluate the *strength* of the prima facie case.[88]

It is also important to note that certain—though not all—claims underlying unmasking requests require a mental state analysis. For example, to prove defamation, a plaintiff must demonstrate that the defendant acted negligently or (if the defendant is a public figure) with actual malice.[89] However, as emphasized in *Cahill*, plaintiffs charged with making a prima facie showing to support their unmasking requests are not required to prove their "case as a matter of undisputed fact"[90]—instead, they have to present sufficient evidence "for all elements of a defamation claim *within plaintiff's control*."[91] This is because courts recognize that before discovery, plaintiffs may not have access to information that would allow them to prove the defendant's mental state since the defendant's identity is unknown.[92] If the court grants the unmasking request, the

87. *Id.* at 767–68 ("[P]laintiff should establish to the Court's satisfaction that plaintiff's suit against defendant *could* withstand a motion to dismiss." (emphasis added) (quoting Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 579 (N.D. Cal. 1999)).

88. *Id.* at 760–61.

89. New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964).

90. Best W. Int'l, Inc. v. Doe, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at *4 (D. Ariz. July 25, 2006).

91. Doe v. Cahill, 884 A.2d 451, 463 (Del. 2005) (emphasis in original).

92. *Best W. Int'l, Inc.,* 2006 WL 2091695, at *5 ("[A] plaintiff at an early stage of the litigation may not possess information about the role played by particular defendants or other evidence that normally would be obtained through discovery. But . . . [the] plaintiff must produce such evidence as it has to establish a *prima facie* case of the claims asserted in its complaint."). A recent case illustrates how an anonymous speaker's mental state may be evaluated without knowledge of his or her identity. In *Kennedy v. Kos Media*, Senator

plaintiff can then engage in discovery to seek the evidence necessary to prove the mental state element of the claim.[93]

3. The Evolution of Unmasking Standards

When unmasking requests for online content started becoming more common in the early days of widespread internet adoption, courts initially adopted approaches that were highly deferential to the parties seeking disclosure. *Seescandy.com* and *America Online* were some of the earliest cases to consider this issue. Adopting the motion to dismiss[94] and good faith standards[95] respectively, these courts allowed plaintiffs to prevail on their unmasking requests without having to make any evidentiary showing of the strength of their underlying claims.[96]

Following (though not necessarily as a direct result of) the *America Online* ruling, the Virginia state legislature signed an

---

Robert F. Kennedy Jr. filed a petition for pre-action disclosure against a news site seeking to unmask an anonymous blogger who posted on the site about Kennedy's appearance at a rally in Germany. Motion to Quash at 8, Nos. 2021-0370 & 2021-04476 (N.Y. App. Div. Dept. 2), https://mkus3lurbh3lbztg254fzode-wpengine.netdna-ssl.com/wp-content/uploads/Motion-to-quash-memo-decls-8-9-final-version.pdf. Kennedy sought the blogger's identity so that he could pursue a defamation claim. *Id.* The blogger moved to quash, arguing that Kennedy could not show that any factual statements at issue were false and could not provide clear and convincing evidence of actual malice. *Id.* at 20. The blogger contended that a showing of actual malice was necessary in this case since Kennedy was, at least, a limited purpose public figure, and that such a showing could be "predicated on proving that the blog post [at issue] was so far different from what various sources in the mainstream media were saying about the protest that [the blogger] must have known that the blog post was wrong." *Id.* at 25.

93. There may be instances when, based on publicly available information, a plaintiff can prove the defendant's mental state without knowing their identity. For instance, consider a Twitter user who tweets an intention to knowingly spread false information via Twitter—and who then proceeds a few days later to do exactly that.

94. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 580–81 (N.D. Cal. 1999).

95. *In re* Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 2000 WL 1210372, at *8 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds*, 542 S.E.2d. 377 (Va. 2001).

96. It is important to note that, while the motion to dismiss standard established by the *Seescandy.com* court requires no evidentiary showing, in the case itself the court actually did consider evidence offered by the plaintiff. *Seecandy.com*, 185 F.R.D. at 579–80.

unmasking bill into law in April of 2002.[97] The Virginia unmasking statute is even more plaintiff-friendly than *America Online*. It provides that a plaintiff can meet the requirements for unmasking by either showing he or she has "a legitimate, good faith basis to contend" that he or she is a "victim of conduct actionable" or by showing communications that "may be tortious or illegal."[98] This is a hurdle so low that it is hardly a hurdle at all. The statute is arguably[99] constitutionally suspect, as it confers to plaintiffs the power to unmask defendants using a threshold that is insufficiently protective of the right to anonymous speech.

While the Virginia statute remains on the books, courts in other jurisdictions have generally concluded that the judicially created good faith and motion to dismiss standards were

---

97. H.D. 819, 2002 Leg., Reg. Sess. (Va. 2002). The summary of the bill states that it "[p]rovides a procedure governing certain subpoenas in civil proceedings where it is alleged that an anonymous individual has engaged in tortious Internet communications. This bill is a recommendation of the Study on the Discovery of Electronic Data and has been endorsed by the Judicial Council." *2002 Session: H819 Identity of Persons Communicating Anonymously Over the Internet*, VA.'S LEGIS. INFO. SYS., https://lis.virginia.gov/cgi-bin/legp604.exe?021+sum+HB819S (last visited Oct. 21, 2021).

98. VA. CODE ANN. § 8.01-407.1 (2002): This statute was at the center of a 2015 Virginia Supreme Court case considering a subpoena served on Yelp by a business owner alleging defamation. Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., 770 S.E.2d 440 (Va. 2015). The court held that the "circuit court was not empowered to enforce the subpoena duces tecum against Yelp[.]" *Id*. at 441.

99. There are important and as yet unresolved legal questions of whether the government violates the Constitution when it creates a statute authorizing a private party to take an action that, if taken by the government, would be unconstitutional. The Supreme Court has explained that "[w]hether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities." Skinner v. Railway Lab. Execs. Ass'n, 489 U.S. 602, 614 (1989). An analogous line of reasoning would presumably apply to the First Amendment. With regard to unmasking under the Virginia statute, it could be argued that the government is not a participant at all (because the litigation is between private parties), or, alternatively, that the government is very much a participant (through having created a process that directly undermines the ability to speak anonymously). The issue of the constitutionality of laws authorizing private actions also arose in 2021 in *United States v. Texas*, a Supreme Court case considering a Texas law permitting private citizens to sue (and if successful, recover damages from) anyone who "aids or abets the performance or inducement of an abortion." S.B. 8, 87th Leg., Reg. Sess. (Tex. 2021) (to be codified as Tex. Health & Safety Code §§ 171.203(b), 171.204(a)).

inadequate in light of First Amendment concerns, and have instead formulated more stringent approaches. For example, in *Dendrite*,[100] a New Jersey appellate court created what one legal scholar has described as "the first test that maintained national traction."[101] The *Dendrite* standard requires a plaintiff to: (1) provide notice to the defendant, (2) identify the allegedly actionable statements, (3) establish a claim sufficient to survive a motion to dismiss, and (4) produce evidence sufficient to establish a prima facie cause of action.[102] An additional key aspect of the *Dendrite* standard relates to what occurs once the plaintiff has satisfied the four prongs above: The court must balance the interests of the anonymous speaker and the strength of the plaintiff's case to determine whether unmasking is proper.[103]

In *Cahill*, the Delaware Supreme Court adopted a modified version of *Dendrite*.[104] This standard still requires the plaintiff to attempt to notify the defendant and to provide evidence sufficient to satisfy the "prima facie or 'summary judgment standard.'"[105] However, the court found the second *Dendrite* prong (the identification of actionable statements) to be "subsumed in the summary judgment inquiry" and also concluded that the separate balancing analysis is unnecessary since, in the view of the *Cahill* court, "the summary judgment test is itself the balance."[106] Courts have varied in their application of *Dendrite* and *Cahill*, with some adopting *Dendrite*'s express balancing step[107] and others following *Cahill*'s process.[108] Courts and scholars have expressed differing

---

100. Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

101. Plemons, *supra* note 14, at 196.

102. *Dendrite*, 775 A.2d at 760–61.

103. *Id.*

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

105. *Id.* at 460 (quoting *Dendrite*, 775 A.2d at 769).

106. *Id.* at 461.

107. *See In re* Ind. Newspapers, Inc., 963 N.E.2d 534, 552 (Ind. Ct. App. 2012); Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 456–57 (Md. 2009); Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

108. *See* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 245–46 (Cal. Ct. App. 2008); *In re* Does 1–10, 242 S.W.3d 805, 821 (Tex. Ct. App. 2007).

views about whether *Cahill* or *Dendrite* is more demanding and protective of speech.[109]

While *Dendrite* and *Cahill* have been used extensively,[110] some courts have adopted other approaches. For example, in *Doe v. 2TheMart.com, Inc.* (2001)[111] a federal district court in Washington State created a four-part test for evaluating whether to grant a civil subpoena to unmask an anonymous poster who was not a party to the litigation.[112] The court explained that "non-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker."[113] *Highfields*[114] is another important case in the unmasking landscape, having established what is essentially the Northern District of California's slimmed down version of *Dendrite*: a two-part prima facie standard that requires the party seeking unmasking to make a strong evidentiary showing and the court to balance the strength of the claim with First Amendment interests.

---

109. *Compare In re* PGS Home Co. Ltd., No. 19-mc-80139-JCS, 2019 WL 6311407, at *6 (N.D. Cal. Nov. 25, 2019) (asserting that *Cahill* created "the most exacting standard" for unmasking), *and* Doe I v. Individuals, 561 F. Supp. 2d 249, 255–56 (D. Conn. 2008) (noting that *Cahill* is "difficult for a plaintiff to satisfy" and opting to use the prima facie standard adopted by *Dendrite* and other courts because it "strikes the most appropriate balance" between the parties), *and* McMallman, *supra* note 12, at 247 (explaining that *Cahill* is more defendant-friendly than *Dendrite*), *with* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 243 (Cal. Ct. App. 2008) (explaining that the *Cahill* court felt that "[t]he *Dendrite* test . . . required too much"), *and* Plemons, *supra* note 14, at 209 ("[C]ourts that utilize the *Cahill* approach are far more likely to grant discovery into the speaker's identity than those that implement *Dendrite*.").

110. *See* Plemons, *supra* note 14, at 196 ("[J]urisdictions typically adopt one of two approaches: either the *Dendrite* or *Cahill* test."); Kelly Waldo, *Signature Mgm't Team LLC v. Doe: The Right to Anonymous Speech Post-Judgment*, 19 N.C. J.L. & TECH. 253, 267 (2018) (citing *Dendrite* and *Cahill* as examples of prominent cases in which courts have expanded upon the "pioneering test from *Seescandy.com*").

111. 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

112. *Id.* at 1095–97.

113. *Id.* at 1095; *see also In re* Anonymous Online Speakers, 661 F.3d 1168, 1176 (explaining that the *2TheMart.com* court "drew from *seescandy.com* and *America Online*, but recognized that a higher standard should apply when a subpoena seeks the identity of an anonymous Internet user who is not a party to the underlying litigation").

114. 385 F. Supp. 2d 969 (N.D. Cal. 2005).

In 2011, the Ninth Circuit became one of the earliest federal appellate courts[115] to address online unmasking,[116] but its decision created more questions than answers. In *Anonymous Speakers*,[117] the Ninth Circuit rejected a broad application of *Cahill* after cataloguing the various unmasking standards and stating that "*Cahill*'s bar extends too far."[118] The court wrote that instead of uniformly applying the *Cahill* standard, "the nature of the speech should be a driving force in choosing a standard by which to balance the right of anonymous speakers in discovery disputes,"[119] with commercial speech getting less First Amendment protection than literary, religious, or political speech.[120] Since *Anonymous Speakers*, there remains little clarity about what unmasking standard is appropriate for what type of speech.

B. UNMASKING IN CRIMINAL PROCEEDINGS

Far less attention has been paid to unmasking in the criminal context, and more particularly to unmasking in relation to grand jury investigations.[121] This may be because subpoenas

---

115. The prior year, in 2010, the Second Circuit considered unmasking in a case addressing mass downloading. *See Arista Records v. Doe 3*, 604 F.3d 110, 119 (2d. Cir. 2010).

116. Philip L. Gordon & Christopher M. Leh, *Ninth Circuit Provides Some Relief for Employers and Executives Anonymously Trashed on the Web*, LITTLER (July 23, 2010), https://www.littler.com/publication-press/publication/ninth-circuit-provides-some-relief-employers-and-executives.

117. *In re* Anonymous Online Speakers, 661 F.3d 1168 (9th Cir. 2011).

118. *Id.* at 1177.

119. *Id.*

120. *Id.*

121. While the discussion herein focuses on grand jury proceedings, unmasking also arises in relation to criminal investigations. For instance, in *In re* Facebook, Inc. v. U.S., a Washington D.C. court authorized search warrants for two individual Facebook accounts and one Facebook page that the government had probable cause to believe contained evidence regarding unrest in Washington on the day of President Trump's inauguration. Order, Nos. 17 CSW-658, 659, 660 (2017), https://www.citizen.org/wp-content/uploads/facebookwarrantfinalorder_0.pdf (last accessed Nov. 18, 2021). These warrants would permit the government to obtain the identifying information and private communications of both the accountholders and innocent third parties associated with the accounts. *Id.* at 13–15. The account holders moved to intervene and challenge the warrants. *Id.* at 2. Acknowledging that these warrants threatened to undermine associational privacy and anonymous speech rights, the court created procedural safeguards to narrow their scope. *Id.* at 9, 12. Some of these safeguards included requiring the government to

requesting the identity of an online speaker issued during the course of grand jury investigations would generally be kept confidential, making it impossible to know how commonly it occurs. There are currently few cases in the public record specifically addressing this point.[122]

Federal grand jury proceedings are generally required to be kept secret.[123] State grand jury proceedings generally are as well, although laws vary about the extent of this

---

submit its search protocol to the court for review, redact identifying information of third parties who communicated on Facebook Messenger with the accounts or pages in question, and delete any data obtained during the search that did not fall within the scope of the warrant. *Id.* at 13–15.

122. In addition to *Glassdoor* discussed herein, *see In re* Grand Jury Subpoena No. 11116275, 846 F. Supp. 2d 1, 3 (D.D.C. 2012) (denying a motion to quash a government subpoena to unmask a Twitter user who threated to "engage in sadomasochistic activities" with then-presidential candidate Michele Bachmann); *In re* Grand Jury Subpoena Issued to Twitter, Inc., No. 3:17-MC-40-M-BN, 2017 WL 9485553, at *1 (N.D. Tex. Nov. 7, 2017), *report and recommendation adopted*, No. 3:17-MC-40-M-BN, 2018 WL 2421867 (N.D. Tex. May 3, 2018) (recommending that the court grant in part and deny in part Twitter's motion to quash an unmasking subpoena seeking the identity of five users who the government suspected were either involved in cyberstalking or had information relevant to the government's investigation of a cyberstalking suspect). In addition, a 2012 California district court case dealt with a motion to quash a subpoena from the SEC to Google to identify the owner of an anonymous Gmail account. Doe v. United States Secs. & Exch. Comm'n, No. MC 11-80184 CRB, 2012 WL 78586, at *1 (N.D. Cal. Jan. 10, 2012). The owner of the account moved for a protective order or stay of the subpoena pending his appeal, and the court denied the motion. *Id.* at *1, *6. This is a civil case (since the SEC is an administrative agency, it cannot bring criminal charges on its own). However, the SEC often partners with the FBI in related criminal investigations, raising an evidentiary question about whether the information obtained during the SEC investigation could later be used by the government in a related criminal case.

123. *See* SARA SUN BEALE ET AL., GRAND JURY LAW AND PRACTICE § 1:6 (2d ed. 2020) ("The traditional principle of grand jury secrecy is still generally observed in federal proceedings . . . .").

requirement.[124,125] Thus, it might be argued that the secret nature of grand jury proceedings is protective of the right to anonymous speech of people whom a grand jury seeks to unmask. After all, unmasking the identity of a formerly anonymous speaker only to members of a grand jury is certainly less invasive of privacy than unmasking the speaker to the public.

But that argument misses the point that *any* unmasking, even to a limited group, removes anonymity and creates a risk of more widespread disclosure, whether inadvertent (e.g., if documents that were supposed to remain under seal are compromised via human error or a cybersecurity flaw) or intentional (e.g., if the unmasked speaker is a witness who is subsequently compelled to testify in open court at a trial). While grand juries are not ubiquitous, they are a common feature of the landscape at both the federal and state level.[126]

Some state criminal courts have grappled with the issue of anonymous online speech outside of grand jury proceedings. But in contrast with civil litigation, where a plaintiff typically seeks the identity of an anonymous online speaker, state criminal courts have often considered the issue in the inverse, when a

---

124. For example, California Penal Code § 938.1 permits grand jury testimony to be revealed if a defendant is indicted. CAL. PEN. CODE § 938.1(a) (West 2003). The transcript of the testimony becomes accessible to the public 10 days after it has been delivered to the defendant or the defendant's attorney. CAL. PEN. CODE § 938.1(b). Missouri's Sunshine Law authorizes records related to a law enforcement investigation to become public once the investigation is inactive. MO. ANN. STAT. § 610.100 (West 2020). Although Missouri has multiple statutes requiring grand jury proceedings to be kept secret, none of them explicitly exempt the proceedings from the Sunshine Law's requirements. MO. REV. STAT. §§ 540.310, 540.320, 540.110, 540.120; *see also* Joseph E. Martineau et al., *Grand Jury Records–Can the Public Get Them?*, LEWIS RICE (Aug. 21, 2015), https://www.lewisrice.com/publications/grand-jury-records-can-the-public-get-them/ ("While Missouri, like most other states, has statutes creating secrecy in grand jury proceedings, nothing in the grand jury statutes in Missouri changes the Sunshine Law's presumption of openness, even for the portions of the investigative files presented to the grand jury.").

125. The right to a grand jury has not been incorporated. *See* Hurtado v. California, 110 U.S. 516 (1884) (holding the right to indictment by a grand jury has not been incorporated against the states).

126. Nicole Smith Futrell, *Visibly (Un)just: The Optics of Grand Jury Secrecy and Police Violence*, 123 DICK. L. REV. 1, 22 (2018) ("While 'nearly all state constitutions provided for indictment by grand jury in the early nineteenth century,' not all states actually make use of grand juries." (footnotes omitted) (citations omitted)).

litigant already known to the court seeks to challenge an affirmative *prohibition* on anonymous online activity. Such prohibitions can arise through requirements for sex offender registries[127] or through laws addressing computer crimes.[128]

Thus, state criminal cases have often focused not on articulating a procedure for unmasking, but rather on questions such as whether context-specific prohibitions on anonymous online activity are constitutional. There are also federal and state criminal proceedings that include unmasking of the identity of online speakers who are unambiguously engaging in unprotected speech—a circumstance that raises no need for any sort of balancing test. For instance, in November 2015, several people used the anonymity-conferring social networking app Yik Yak to issue threats of imminent, racially-targeted violence at the University of Missouri.[129] They were quickly unmasked and arrested.[130]

Another potential reason for the paucity of federal criminal cases in the public record dealing with unmasking requests may be the Stored Communications Act (SCA).[131] The SCA, which

---

127. Multiple state criminal courts have considered the constitutionality of statutes requiring convicted sex offenders to provide identifying information like their email addresses and usernames on particular sites to government registries, just as they are required to provide information like their phone numbers and home addresses. *See, e.g.*, People v. Minnis, 67 N.E.3d 272, 279, 291 (Ill. 2016) (holding that Illinois' Sex Offender Registration Act requiring "sex offenders to disclose and periodically update information regarding their Internet identities and websites" survives intermediate scrutiny); *Ex parte* Odom, 570 S.W.3d 900, 905–16 (Tex. App. 2018) (affirming that the "Texas Sex Offender Registration Program's requirement that convicted sex offenders register [their] internet identifiers . . . does not burden substantially more speech than is necessary to further the State's legitimate interests").

128. *See, e.g.*, Jaynes v. Commonwealth, 276 Va. 443 (Va. 2008) (detailing a Virginia Supreme Court decision involving a defendant convicted of violating a provision of Virginia's Computer Crimes Act for providing false routing information when disseminating unsolicited bulk emails).

129. Sarah Larimer, *University of Missouri police arrest suspect in social media death threats*, WASH. POST (Nov. 11, 2015), https://www.washingtonpost.com/news/grade-point/wp/2015/11/11/universityof-missouri-police-arrest-suspect-in-social-media-death-threats/.

130. *Id.*

131. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). The ECPA included the SCA, which was codified at 18 U.S.C. §§ 2701–12.

was enacted in 1986 and is now widely viewed as outdated,[132] provides the government with mechanisms to access both "records concerning"[133] (i.e., metadata of) electronic communications as well as the "contents of"[134] those communications. Unmasking inquiries will typically target the metadata, since the goal will often be to identify the person who posted one or more messages for which the contents are already public.

Unmasking in criminal cases implicates both First and Fourth Amendment issues. While the Supreme Court in *Carpenter v. United States*[135] found the SCA provision with respect to *warrantless* access to metadata to be unconstitutional, that holding was extremely narrow, applying only to metadata in the form of cell site location information.[136] In any case, *Carpenter* left intact the portion of the SCA that allows law enforcement to obtain this information with a warrant.[137] Thus, before a grand jury investigation even begins, law enforcement investigators can (with a warrant as needed) use the SCA to identify an anonymous speaker, and then bring that information to a grand jury. Of course, this raises a separate question of whether the SCA is constitutionally problematic with respect to the First Amendment when used for this purpose. The upshot is that the jurisprudence is far sparser with respect to unmasking in criminal cases than in civil litigation. This is why *Glassdoor* is such an important—and we believe, concerning—precedent.

1. Glassdoor

Glassdoor is a website that provides a platform for individuals to post anonymous reviews about their employers.[138] Glassdoor requires people wishing to post reviews to register their e-mail addresses with the site, though there is no

---

132. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 291 (6th Cir. 2010) (finding unconstitutional the portions of the SCA permitting the government to access the contents of electronic communications without a warrant).

133. 18 U.S.C. § 2703(c).

134. 18 U.S.C. § 2703(a).

135. 138 S. Ct. 2206 (2018).

136. *Id.* at 2220.

137. *Id.* at 2220–23.

138. United States v. Glassdoor, Inc., 875 F.3d 1179, 1182 (9th Cir. 2017).

requirement that the e-mail address convey the name of the person who controls it.[139]

In March 2017, the government subpoenaed Glassdoor, ordering it to unmask over 100 users who had posted anonymous reviews of a government contractor under investigation by an Arizona federal grand jury for wire fraud and misuse of government funds.[140] Glassdoor objected, invoking its users' First Amendment rights.[141] In response, the government narrowed its request to eight users[142] who the government considered "witnesses to certain business practices" pertinent to the investigation.[143] Glassdoor filed a motion to quash, arguing that the government had not met its burden under the compelling interest test articulated in *Bursey v. United States*,[144] a 1972 Ninth Circuit decision in which the court partially quashed a grand jury subpoena to identify the anonymous publishers of a Black Panther Party newspaper that was critical of the United States government.[145] By contrast, the government

---

139. *See id.* ("[T]o post reviews, users must first provide Glassdoor with their e-mail addresses . . . .").

140. *Id.* at 1182–83. The name of the company was redacted in the published opinion. *Id.*

141. *Id.* at 1183.

142. *Id.*

143. *Id*; *see also In re* Grand Jury Subpoena, No. 16-03-217, at 2 (D. Ariz. May 10, 2017) (on file with author). This order has since been sealed, so is inaccessible on legal databases but has been circulated online.

144. 466 F.2d 1059 (9th Cir. 1972). In *Bursey*, the Ninth Circuit established a three-part test that the government must satisfy when seeking information that implicates First Amendment rights in the course of a grand jury investigation. *Id.* at 1083. This test requires the government to establish that (1) its "interest in the subject matter of the investigation is 'immediate, substantial, and subordinating;'" (2) a "substantial connection" exists "between the information [the government] seeks . . . and the overriding governmental interest in the subject matter of the investigation;" and that (3) its "means of obtaining the information" are "not more drastic than necessary to forward the asserted governmental interest." *Id.* Notably, the court emphasized that while the "grand jury is an arm of the judiciary, rather than an appendage of other branches of Government" it is "bound by the Constitution" just as much as "its governmental coordinates[.]" *Id.* at 1082. Accordingly, "it would be anomalous for courts to protect First Amendment rights from infringement by other branches of Government, while providing no such protection from the acts of judicial agencies over which the courts have supervisory as well as constitutional powers." *Id.*

145. *Glassdoor*, 875 F.3d at 1182, 1187–88. *See generally Bursey*, 466 F.2d 1059.

contended that under *Branzburg v. Hayes*,[146] Glassdoor was obligated to comply with the subpoena unless it could demonstrate that the government acted in bad faith when making the request.[147]

After the district court denied Glassdoor's motion to quash the subpoena, Glassdoor appealed to the Ninth Circuit, which affirmed the district court's decision.[148] The Ninth Circuit's analysis focused on two questions: first, whether the Glassdoor users in question had a right to associational privacy, and second, whether the statements made in the reviews were protected speech, and if so, whether that status was sufficient to block a grand jury subpoena.[149]

The court found the associational privacy argument to be "tenuous," stating that this right did not protect those "who happen to use a common platform to anonymously express their individual views" and that "Glassdoor's users are necessarily strangers to each other, because they are anonymous."[150] Having (improperly in our view, as discussed later herein)[151] rejected the associational privacy claim, the Ninth Circuit then turned to the question of whether the reviews were protected speech.[152] The court answered this question in the affirmative, but then went on to find *Branzburg* controlling—i.e., because there was no evidence that the government requested the subpoenaed information in bad faith, Glassdoor had to comply.[153]

The court found that subjecting the government to the more stringent compelling interest test from *Bursey* would burden

---

146. 408 U.S. 665 (1972). The Supreme Court held in *Branzburg* that reporters have "no First Amendment privilege to refuse to answer the relevant and material questions asked during a good-faith grand jury investigation." *Id.* at 708. It found "no basis for holding that the public interest in law enforcement and in ensuring effective grand jury proceedings is insufficient to override the consequential, but uncertain, burden on news gathering that is said to result from insisting that reporters, like other citizens, respond to relevant questions" during a "valid grand jury investigation or criminal trial"—even if this means revealing the criminal conduct, or evidence thereof, of the reporter's source. *Id.* at 690–92.

147. *Glassdoor*, 875 F.3d at 1182. *See generally Branzburg*, 408 U.S. 665.

148. *Glassdoor*, 875 F.3d at 1182–83.

149. *Id.* at 1183.

150. *Id.* at 1184.

151. *Infra* Part IV.A.2.

152. *Glassdoor*, 875 F.3d at 1184.

153. *Id.* at 1189–90.

grand jury proceedings, concluding that even if the compelling interest test applied, "[a]ny incidental infringement on Glassdoor's users' First Amendment rights is no more drastic than necessary to vindicate those compelling interests."[154] But despite articulating such a lopsided, government-friendly approach for unmasking in the course of grand jury investigations, *Glassdoor* has generated surprisingly little commentary.[155]

2. Grand Juries and Unmasking

What are the implications of *Glassdoor* for anonymous online speech of interest in grand jury proceedings? To answer that question, it is helpful to briefly provide context regarding the role of grand juries more generally. While grand juries are not used in all federal criminal cases, they are used in relation to charges for crimes for which the consequences for conviction are particularly severe[156]—or, in the language of the Fifth Amendment, "infamous."[157]

As Gabriel J. Chin and John Ormonde explain in a 2018 law review article, "[u]nder the current rules, felonies must be

154. *Id.* at 1189–91.

155. Only a handful of law review articles to date cite *Glassdoor*, and all of them mention it only in passing. Evan Caminker, in an article on the long-term implications of *Carpenter v. U.S*, 138 S. Ct. 2206 (2018) on modern privacy doctrine and digital privacy protections, mentions *Glassdoor* as an example of how "[c]ourts moved to protect personal privacy interests implicated by subpoenas issued to corporations" will "do so, if at all, by ensuring the information is requested in good faith or tightening the required showing of relevance—not by requiring a showing of anything approaching probable cause." Evan H. Caminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, SUP. CT. REV. 411, 477 n.312 (2019). Madeline Lamo and Ryan Calo note in an article about why society should act cautiously when regulating bot speech that "[w]hile the Ninth Circuit's *Glassdoor* ruling has already been the subject of extensive criticism by First Amendment advocates for its failure to take the unique qualities of online speech into account . . . it remains to be seen whether the Supreme Court will intervene." Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. REV. 988, 1022 n.215 (2019). And Barry Stricke, in an article on California's online bot disclosure act, mentions *Glassdoor* as an example of when a third-party publisher was unable to resist a subpoena to protect its users' anonymity. Barry Stricke, *People v. Robots: A Roadmap for Enforcing California's New Online Bot Disclosure Act*, 22 VAND. J. ENT. & TECH. L. 839, 891 (2020).

156. Gabriel J. Chin & John Ormonde, *Infamous Misdemeanors and the Grand Jury Clause*, 102 MINN. L. REV. 1911, 1911–12 (2018).

157. U.S. CONST. amend. V.

prosecuted by grand jury indictment, but a misdemeanor may be based on a charge in a prosecutor's information or even a ticket issued by a law-enforcement officer with no further review."[158] Thus, many federal crimes are charged without a grand jury indictment.

As the grand jury clause of the Fifth Amendment has never been incorporated against the states,[159] states have adopted a patchwork of different approaches. As described by LeFave et al., as of 2020, eighteen states guaranteed those accused of serious crimes the right to an indictment by a grand jury.[160] Four other states were considered "limited indictment jurisdictions," where prosecution by indictment is guaranteed only in cases involving "the most severely punished felonies"— those punishable by life imprisonment or the death penalty.[161] In contrast, twenty-eight states allowed for felony prosecutions by information rather than grand jury indictment.[162] These "information states" technically leave open the option to

---

158. Chin & Ormonde, *supra* note 156, at 1911–12 (internal citations omitted). Chin and Ormonde further argue that the felony/misdemeanor distinction is the wrong place to draw the line, as "many misdemeanors are infamous because they authorize imprisonment or carry stigmatizing consequences" and that using the felony/misdemeanor categorization for determining whether a crime is "infamous" undermines defendants. *Id*. at 1949.

159. *See* McDonald v. City of Chicago, 561 U.S. 742, 765 n.13 (2010) (listing "the Fifth Amendment's grand jury indictment requirement" as one of "the only rights not fully incorporated"); *see also* 2 SUSAN W. BRENNER & LORI E. SHAW, FED. GRAND JURY: A GUIDE TO LAW AND PRACTICE § 24:1 (2d ed. 2020) (explaining that "States are . . . free (i) to rely solely on the grand jury, (ii) to reject it for charges initiated by a prosecutor and preliminary hearings to determine probable cause," which is also called prosecution by information, "or (iii) to rely on a combination of both").

160. 4 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 15.1(d) (4th ed. 2020). While these "indictment states" differ "in their description of the offenses as to which a defendant may insist upon a grand jury accusation," all of these descriptions "add up to requiring a grand jury charge for offenses meeting the traditional definition of felonies." *Id*. Furthermore, on these jurisdictions, if a defendant is prosecuted on information, convicted, and timely raises an objection, the conviction will automatically be reversed. *Id*.

161. *Id.* § 15.1(e). In Louisiana and Rhode Island, the accused has a right to indictment by a grand jury when charged with offenses punishable by life imprisonment or the death penalty. *Id.* Florida guarantees the right to an indictment by a grand jury only in capital cases, and Minnesota, having abolished the death penalty, guarantees the right only in cases involving charges that could result in life imprisonment. *Id.*

162. *Id.* § 15.1(g).

prosecute by a grand jury indictment, but in many states "this option is entirely or largely theoretical."[163] Other information states generally only impanel indicting grand juries for major investigations.[164] And in the remaining information states, whether such indictments actually occur depends heavily on prosecutorial discretion and accordingly varies not just by state but by "prosecution district . . . within the same state."[165]

It is also important to underscore that grand juries actually perform two tasks[166] that potentially interact differently with the unmasking question. First, a grand jury *investigates* crimes and identifies person(s) suspected of committing them.[167] Second, a grand jury determines whether there is sufficient evidence to *indict* the accused.[168] This dual function of the grand jury has been referred to "as both shield and sword."[169]

---

163. *Id*. For example, Nebraska only authorizes an indicting grand jury if requested by citizen petition or in cases involving death caused by law enforcement. *Id.* at n.356.30. Pennsylvania allows individual counties to eliminate the indicting grand jury by petitioning the Pennsylvania Supreme Court "to approve a system of prosecution by information in that court." *See* BEALE ET AL., *supra* note 123, § 1:5. And Connecticut has eliminated the indicting grand jury altogether. *See* CHRISTOPHER REINHART, CONN. GEN. ASSEMB., OLR RESEARCH REPORT: CONNECTICUT GRAND JURIES (Sept. 3, 1998), https://www.cga.ct.gov/PS98/rpt%5Colr%5Chtm/98-R-1101.htm ("On November 24, 1982, Connecticut adopted a constitutional amendment to repeal the requirement of a grand jury indictment before a person can be tried for any crime punishable by death or life imprisonment, and to require, instead, a probable cause hearing.").

164. *See* BEALE ET AL., *supra* note 123, § 1:5.

165. *See* LAFAVE ET AL., *supra* note 160, § 15.1(g).

166. *See, e.g.*, BEALE ET AL., *supra* note 123, § 1:7 (noting that grand juries perform "two interrelated but distinct functions").

167. *Id.* Investigative grand juries are still relied on in information states, though infrequently. *See* LAFAVE ET AL., *supra* note 160, § 14.2(d) n.47.50 ("Even when the grand jury continues to be used for investigations, that use may be so infrequent as to have gaps of more than a decade between grand juries.").

168. *See* LAFAVE ET AL., *supra* note 160, § 14.2(d) n.47.50. This determination is made (or rejected) after a prosecuting authority has "made a definite accusation of criminal conduct against a particular person." BEALE ET AL., *supra* note 123, § 1:7.

169. *See, e.g.*, BEALE ET AL., *supra* note 123, § 1:7 ("A colorful metaphor is used to describe these dual functions: the grand jury acts as both shield and sword.").

In its investigative capacity, a grand jury has broad powers.[170] The Supreme Court explained in *United States v. Real Enterprises* in 1991 that a grand jury is free to "investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[171] Indeed, a grand jury investigation is only complete when "every available clue has been run down and all witnesses [have been] examined in every proper way to find if a crime has been committed."[172] The rules of evidence do not apply to grand jury proceedings—even unlawfully obtained evidence can be used.[173] The grand jury's power, however, is not limitless. While "[i]t may consider incompetent evidence . . . it may not itself violate a valid privilege, whether established by the Constitution, statutes, or the common law."[174]

Furthermore, the power of the grand jury to issue subpoenas and compel the production of evidence is broad, and can be enforced through contempt proceedings.[175] Grand jury subpoenas to produce documents are rarely struck down for irrelevance,[176] no doubt in part because subpoenaed parties are

---

170. *See, e.g.,* Eugene R. Scheiman, *Grand Jury Subpoenas and First Amendment Privileges*, 446 ANNALS AM. ACAD. POL. & SOC. SCI. 106, 108 (1979) (explaining that a grand jury has "almost unfettered powers").

171. 498 U.S. 292, 297 (1991) (internal quotations and citations omitted). The *R. Enterprises* Court also wrote that such investigations are "not fully carried out until every available clue has been run down and all witnesses examined in every proper way to find if a crime has been committed." *Id.* (internal quotations omitted).

172. *Id.* (internal quotations omitted).

173. United States v. Calandra, 414 U.S. 338, 346 (1974).

174. *Id.*

175. See BEALE ET AL., *supra* note 123, § 1:7 (explaining that grand jury subpoenas are "subject to few restrictions, and if a witness refuses to testify or produce evidence, the grand jury may invoke the court's contempt power to compel compliance with its subpoena.").

176. *See* 1 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 104 (4th ed. 2021) ("In U.S. v. R. Enterprises, the Supreme Court said that while grand juries may not engage in fishing expeditions, 'the law presumes, absent a strong showing to the contrary, that a grand jury acts within the legitimate scope of its authority,' and that therefore, 'a grand jury subpoena issued through normal channels is presumed to be reasonable, and the burden of showing unreasonableness must be on the recipient who seeks to avoid compliance." (internal quotations and citations omitted)).

not provided with contextual information that would allow them to evaluate the relevance of the information being sought.[177]

In contrast with investigations, which provide few protections (thus the "sword" in the "sword and shield" metaphor mentioned above), an indicting grand jury[178] exists, at least in theory, to protect the due process rights of those under investigation, ensuring that citizens vote on whether or not to bring charges, rather than allowing the government to unilaterally make such decisions.[179]

3. *Glassdoor*'s Overreliance on *Branzburg*

By providing a precedent that is binding in the Ninth Circuit and will likely be highly influential elsewhere, *Glassdoor* is concerning for multiple reasons. First, the Ninth Circuit relied on *Branzburg*—a 1972 decision that focused on limits on the rights of journalists to protect their sources and is only partially analogous to *Glassdoor*.[180] As was made evident by the information conveyed in the news articles that attracted the government's attention in *Branzburg*, the reporters' sources whom the government sought to identify were by definition people with highly specific knowledge bearing on the alleged crimes the government was investigating.[181]

---

177. *See id.* ("In considering whether a motion to quash a subpoena satisfies the R Enterprises test, at least one court has said that the district judge may only look to the categories of information sought in the subpoena itself; it is improper to make a document-by-document evaluation of relevancy. Given the secrecy of the grand jury's proceedings, it will be the rare case that a subpoena recipient will be able to make such a showing.").

178. A single grand jury will often both investigate and indict, but will be called an investigatory or indicting grand jury depending on what function it is serving. *See generally* BEALE ET AL., *supra* note 123, § 1:7 (explaining that when a grand jury is "investigating whether crimes have been committed and, if so, who committed them" it "is often referred to as an investigative grand jury," and when a grand jury is determining "whether there is sufficient evidentiary support to justify holding the accused for trial on each charge . . . [it] is called an indicting grand jury").

179. Beale et al. explain that this enables a grand jury to "shield the accused from criminal charges even though there is an adequate evidentiary basis if . . . [it] conclude[s] that the charges are improperly motivated or unjust." BEALE ET AL., *supra* note 123, § 1:7.

180. *See* United States v. Glassdoor, 875 F.3d 1179, 1185–91 (9th Cir. 2017) (applying Branzburg v. Hayes, 408 U.S. 665 (1972)).

181. *See Branzburg*, 408 U.S. at 667–70 (describing two instances where a reporter published articles that included details of anonymous drug users).

By contrast, the speakers in *Glassdoor* were engaged in casual online conversations that left far more uncertainty regarding how much they actually knew of the alleged crimes, and how much of that knowledge might have been based on hearsay.[182] This is an important difference, as any balancing test weighing the interests of the government against those of the people it seeks to unmask surely should favor the anonymous speakers more heavily when there is such a high degree of uncertainty regarding the value of the information the government would obtain through the unmasking.

Furthermore, *Branzburg* focused on whether the First Amendment protects a journalist's newsgathering activities, which is related to but distinguishable from the right of a journalist's confidential sources to speak anonymously. In *Branzburg*, the reporters had actively sought out and published information from confidential sources relevant to a specific criminal investigation. In contrast, Glassdoor merely provides a platform for users to post all types of information related to their employment experiences. Accordingly, the Ninth Circuit should have focused on the First Amendment protections afforded to the anonymous speakers in *Glassdoor*, not on whether the platform itself was or was not entitled to something analogous to a reporter's privilege. As the D.C. District Court noted in 2009 in *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, the *Branzburg* Court concluded that the First Amendment rights of the journalists were not implicated by the subpoenas at issue, and accordingly it did not consider "whether the substantial relationship [test] would be the appropriate standard of review for a subpoena implicating First Amendment interests."[183]

Second, by relying on *Branzburg* and simply requiring that the government act in good faith, the Ninth Circuit makes it far too easy to successfully subpoena any internet service to obtain identifying information about its users. Online speakers are more likely to be hesitant to post anonymously if they know that

---

182. *See Glassdoor*, 875 F.3d at 1182–83 ("As of March 2017, current and former employees of the subject company had posted 125 reviews on Glassdoor.com. Many of the reviews criticize the subject's management and business practices.").

183. In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq., 706 F. Supp. 2d 11, 19 (D.D.C. 2009).

the government will be able to unmask them if anything they say later becomes even loosely related to a criminal investigation. And, as explained above, the secrecy of grand jury proceedings can sometimes be temporary. The public sometimes gains access to transcripts of federal[184] and state grand jury proceedings after the proceedings themselves have concluded.[185]

IV. RECOMMENDATIONS

A. GRAND JURIES AND UNMASKING

The *Glassdoor* court's choice to base its decision solely on *Branzburg* is highly concerning. A more appropriate approach would view *Branzburg* as a non-dispositive minimum hurdle to be cleared. It is certainly the case that as the *Branzburg* Court concluded, grand juries that are operating in good faith deserve a degree of deference in their activities. However, the fact that an investigation is being done in good faith should not remove constitutional protections from people whose activities come under scrutiny.

What should be done to ensure that the free expression rights of anonymous speakers, who are not typically aware of a grand jury's desire to unmask them,[186] are given appropriate weight? Making the burden too high would run afoul of the *Real Enterprises* Court's admonition that "[a]ny holding that would saddle a grand jury with minitrials and preliminary showings would assuredly impede its investigation and frustrate the public's interest in the fair and expeditious administration of the

---

184. Federal Rule of Criminal Procedure 6(e)(3) outlines circumstances under which a court may disclose federal grand jury matters to those not involved in the proceeding. For example, a court may authorize the disclosure of a grand jury matter in connection with a judicial proceeding. FED. R. CRIM. P. 6(e)(3)(E)(i).

185. *See, e.g.*, N.Y. CRIM. PROC. Law § 190.25 (McKinney) ("Grand jury proceedings are secret, and no grand juror, or other person specified in subdivision three of this section or section 215.70 of the penal law, may, except in the lawful discharge of his duties or upon written order of the court, disclose the nature or substance of any grand jury testimony, evidence, or any decision, result or other matter attending a grand jury proceeding.").

186. It is also possible to imagine circumstances in which anonymous users might be made aware of attempts to unmask them. As noted earlier this occurred, for example, in *Cahill* in which a defendant was notified of the unmasking demand and filed a motion aimed at preventing it. Doe v. Cahill, 884 A.2d 451, 455 (Del. 2005).

criminal laws."[187] But a burden that fails to consider the rights of the anonymous online speakers is also insufficient. Just as a grand jury is, as the Supreme Court has written, "without power to invade a legitimate privacy interest protected by the Fourth Amendment,"[188] it should similarly be powerless to invade legitimate First Amendment interests.

It is important to highlight the *Branzburg* concurrence from Justice Powell—whose vote was indispensable to the majority[189]—which emphasized "the limited nature of the Court's holding."[190] He explained that if a journalist subpoenaed to reveal confidential source information believes that the information is only remotely related to the investigation or that law enforcement has no "legitimate need" for the source's identity, the journalist can seek a protective order from the court or file a motion to quash.[191] Justice Powell further stressed that decisions about whether to compel disclosure should be determined on a case-by-case basis that balances each citizen's duty to testify in a criminal investigation with First Amendment interests.[192]

Justice Powell's concurrence has been influential,[193] although mostly in the context of civil, not criminal cases**.** Faced

---

187. United States v. Real Enters., 498 U.S. at 298–99 (citing United States v. Dionisio, 410 U.S. 1, 17 (1973)).

188. United States v. Calandra, 414 U.S. 338, 346 (1974).

189. *See* Carey v. Hume, 492 F.2d 631, 636 (D.C. Cir. 1974) ("[T]he Branzburg result appears to have been controlled by the vote of Justice Powell."); Dalitz v. Penthouse Int'l, Ltd., 168 Cal. App. 3d 468, 473 (Cal. Ct. App. 1985) ("It is the view of this court that Branzburg v. Hayes . . . cannot legitimately be read without regard to the concurring opinion of Mr. Justice Powell . . . as his vote was necessary to that decision.").

190. Branzburg v. Hayes, 408 U.S. 665, 709–10 (1972) (Powell, J., concurring) (emphasizing the court's ruling does not seek to deprive subpoenaed newsmen of their constitutional rights "with respect to the gathering of news or in safeguarding their sources").

191. *Id.*

192. *Id.* ("The asserted claim to privilege should be judged on its facts by the striking of a proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct.").

193. Laura R. Handman, *Protection of Confidential Sources: A Moral, Legal, and Civic Duty*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 573, 577 (2005) ("Many courts interpreting *Branzburg* have held that Justice Powell's opinion, prescribing a balance of First Amendment and law enforcement interests, is controlling."); *see also* Reps. Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1084 (D.C. Cir. 1978) (Wright, Chief J., dissenting) ("[C]ourts

with motions to compel disclosure in civil cases, multiple circuits have adopted a three-part balancing test based on his proposition, which requires courts to consider: (1) whether the information the reporter is seeking to protect is relevant, (2) whether the information can be obtained through alternative means, and (3) whether there is a compelling interest in the information.[194] Notably, while this test has mostly been applied only in the civil context, the Second Circuit requires a moving party in both civil suits and criminal prosecutions to make a showing that the information sought by a subpoena is "highly material and relevant, necessary or critical to the maintenance of the claim, and not obtainable from other available sources."[195] Some courts, however, have interpreted *Branzburg* as explicitly denying any qualified privilege to reporters subpoenaed in a grand jury investigation.[196]

1. Limiting Subpoenas to Protect First Amendment Rights

A Western District of Wisconsin case illustrates how courts can fashion solutions that balance the government's need to obtain information relevant to an investigation while still protecting First Amendment rights. In *In re Grand Jury Subpoena to Amazon.com Dated 7, 2006* (*"Amazon"*), Amazon was subpoenaed by a grand jury to provide the names of 24,000

---

have consistently read Branzburg as recognizing the First Amendment interests of reporters in confidentiality and as requiring a judicial balancing before disclosure is ordered."); LaRouche v. Nat'l Broad. Co., 780 F.2d 1134, 1139 (4th Cir. 1986) (citing Justice Powell's concurrence to explain that the court must "balance the interest involved" in order to determine "whether the journalist's privilege will protect the source in a given situation"); *In re* Shain, 978 F.2d 850, 854 (4th Cir. 1992) (Wilkinson, J., concurring) (citing Justice Powell's concurrence when stating that "courts traditionally have balanced the competing interests of press and prosecution in ruling on a reporter's motion to quash").

194. *See, e.g.*, *LaRouche*, 780 F.2d at 1139; Ashcraft v. Conoco, Inc., 218 F.3d 282, 287 (4th Cir. 2000); Miller v. Transamerican Press, Inc., 621 F.2d 721, 726 (5th Cir.1980); United States v. Cuthbertson, 630 F.2d 139, 145 (3d Cir. 1980).

195. United States v. Burke, 700 F.2d 70, 77 (2d Cir. 1983).

196. *See, e.g.*, *In re* Shain, 978 F.2d 850, 852–53 (4th Cir. 1992) ("[A]bsent evidence of governmental harassment or bad faith, the reporters have no privilege different from that of any other citizen not to testify about knowledge relevant to a criminal prosecution."); Bursey v. United States, 466 F.2d 1059, 1090–92 (9th Cir. 1972); McKevitt v. Pallasch, 339 F.3d 530, 531–32 (7th Cir. 2003); Storer Communs. v. Giovan, 810 F.2d 580, 584–85 (6th Cir. 1987); Lee v. United States Dept. of Justice, 287 F. Supp. 2d 15, 17–18 (D.D.C. 2003).

users who had purchased books from a seller that was being investigated for wire fraud and tax evasion.[197] Amazon filed a motion to quash, asserting the First Amendment rights of its users to not reveal their private reading choices.[198] The Western District of Wisconsin court found these concerns legitimate, explaining that while the grand jury was not actually interested in the individual reading habits of the users,

> [I]t is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens when hunting for evidence against somebody else . . . . [R]ational book buyers would have a non-speculative basis to fear that federal prosecutors and law enforcement agents have a secondary political agenda that could come into play when an opportunity presented itself.[199]

This fear, the court stressed, could make people less likely to purchase online books, thereby ensuring that their reading choices did not end up in government databases.[200]

While acknowledging that there is no precedent requiring the government to prove that it has a compelling interest in the information or that the information is substantially related to the investigation,[201] the *Amazon* court also noted that the customers who bought books from the bookseller targeted by the investigation had First Amendment rights in their private reading choices.[202] After considering both the First Amendment rights of the customers and the grand jury's needs, the court fashioned an alternative to the initial subpoena that better balanced the interests of the parties.[203]

The court denied the motion to quash the subpoena, but it also greatly limited the subpoena's power and scope by creating a "filtering mechanism"[204] requiring Amazon to send a letter to a subset of the purchase group, informing them of the

---

197. *In re* Grand Jury Subpoena to Amazon.com, 246 F.R.D. 570, 571 (W.D. Wis. 2007).

198. *Id.*

199. *Id.* at 572.

200. *Id.* ("[A] measurable percentage of people . . . would abandon online book purchases in order to avoid the possibility of ending up on some sort of perceived 'enemies list.'").

201. *Id.* at 573.

202. *Id.* at 572–73.

203. *Id.* at 573–74.

204. *Id.* at 573.

investigation and the limited extent of the customers' and Amazon's responsibilities.[205] The letter asked for volunteers to interview with the government, ensuring that those who chose not to participate would be left alone and would not have their identities revealed.[206]

There are clear parallels between *Amazon* and *Glassdoor*, despite the vastly larger number of individuals the government was seeking to unmask in *Amazon*. The *Amazon* court stressed that the government was "not entitled to unfettered access to the identities of even a small sample" of the "group of book buyers without each book buyer's permission."[207] And, in both cases, the government was seeking to identify users who were suspected of no wrongdoing and were engaging in activities protected by the First Amendment. Accordingly, the approach used by the Western District of Wisconsin in *Amazon*, which provides government access while also protecting users of online services from intrusion is instructive for how courts may think about addressing subpoena challenges in similar cases.

2. Online Associational Privacy Rights

The Ninth Circuit's assertion that Glassdoor users have no right to associational privacy is problematic, as it incorrectly implies that people who wish not to be identified to one another lack associational privacy rights. One can imagine any number of scenarios where people would have an interest in associating without revealing their identities, especially online, where anonymous association is particularly easy to engage in. Consider a social media group for people who have a particular medical condition that they do not wish to publicize. They might find a sense of community as well as useful information by communicating with similarly situated people—and there is no good reason, either constitutionally or logically, to require that

---

205. *Id.*

206. *Id.* at 573–74. In a case raising similar questions, the government subpoenaed a bookstore for a list of Monica Lewinsky's purchases as part of its investigation into her relationship with President Bill Clinton. *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, Nos. 98–MC–135–NHJ, 26 Med. L. Rptr. 1599, 1600 (D.D.C. Apr. 6, 1998). The D.C. District Court recognized the First Amendment interests that Lewinsky had in her reading choices and thus required the government to make an in camera showing that its need for this purchase list was compelling. *Id.*

207. *Id.* at 573.

they unmask themselves in order to obtain the benefits of that sort of online association.

Similarly, on Glassdoor, users gather to share their employment experiences with others who have either worked at the same company or who may be interested in applying. The fact that they have a shared connection to this company brings them together. Rather than assume, as the *Glassdoor* court did, that users who are anonymous to each other of necessity lack a right to associational privacy, a better approach is to make that inquiry on a case-by-case basis, considering the nature of the platform and the relationship of the users to each other.

Proper recognition of the associational privacy rights of an online group of people interacting anonymously is important because those rights are intertwined with their right to speak anonymously. There will be many instances (including when posting to Glassdoor, or when participating in the online community of people who share a particular medical condition in the example above) in which people will be willing to associate only because they are able to do so without revealing their identities. Improperly stripping someone of the right to speak anonymously can also have the effect of preventing them from engaging in certain online associations. Put simply, in the online context, unmasking—including fear of future unmasking—implicates not only the freedom of expression but also the freedom of association.

B. UNMASKING IN CIVIL LITIGATION

In our view, both the good faith and motion to dismiss standards provide too little protection for anonymous speakers, and therefore should not be used. That leaves the two more stringent standards: the motion for summary judgment standard (from *Cahill*) and the prima facie standard (from *Dendrite*). As noted earlier, a key difference between *Dendrite* and *Cahill* is that the former includes a separate balancing prong that requires the court, after a prima facie showing has been made, to weigh the interests of the parties, while the latter does not.[208] Paul Alan Levy contends—and we agree—that the balancing stage is "an important one precisely because it enables courts to apply the test to a wide range of circumstances while

208. *See supra* Part III.A.1.

taking the individualized circumstances of each case into account."[209] This express balancing step, when properly applied, ultimately makes *Dendrite* more protective of anonymous speech.[210]

The separate balancing prong under *Dendrite* allows for a more thorough inquiry into the reasons for and against unmasking than what is possible under *Cahill*'s motion for summary judgment analysis. When evaluating a motion for summary judgment, a court draws all inferences in favor of the nonmoving party—in other words, the court must weigh the evidence presented to determine whether "a reasonable jury could return a verdict for the nonmoving party."[211] There is some balancing inherent in that analysis, but not as much as under *Dendrite*, in which a court considers not only "the strength of the prima facie case,"[212] but also "the necessity for disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed"[213] and "the defendant's First Amendment right of anonymous free speech."[214] Accordingly, the *Dendrite* standard still requires a strong evidentiary showing—like that required under *Cahill*—but goes further to ensure that the court weighs the interests of both parties, not just in terms of whether there is a genuine dispute of material fact that is appropriate for trial, but also in terms of the potential harms caused by granting or denying an unmasking request.

There is also the question of what specific factors a court should consider when performing the balancing test. This is an area in which no specific court opinion (including *Dendrite*) provides broadly applicable guidance. Indeed, a Maryland Court of Appeals[215] judge wrote that balancing, at least in the defamation context, invites "lower courts to apply, on an ad hoc

---

209. Paul Alan Levy, *Developments in Dendrite*, 14 FLA. COASTAL L. REV. 1, 15 (2012).

210. *See* Plemons, *supra* note 14, at 209 ("[C]ourts that utilize the *Cahill* approach are far more likely to grant discovery into the speaker's identity than those that implement *Dendrite*.").

211. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986).

212. Dendrite Int'l, Inc. v. Doe No. 3775, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

213. *Id.* at 760–61.

214. *Id.* at 760.

215. The Maryland Court of Appeals is Maryland's highest court.

basis, a 'superlaw' of Internet defamation that can trump the well-established defamation law,"[216] and therefore may be "an obstacle to pursuit of legitimate causes of action."[217] However, the proper response to this concern is not to dispense with a balancing test altogether but rather to give it structure and consistency.

Considering the case law in the aggregate, for unmasking demands arising during discovery,[218] we believe that the following three factors should be analyzed in the balancing test: (1) the type of anonymous speech at issue, (2) whether the speaker is a party to the underlying litigation, and (3) the extent and comparative degree of harm to the parties if the wrong unmasking decision is made. We explore each of these in turn.[219]

---

216. Indep. Newspapers, Inc. v. Brodie, 996 A.2d 432, 460 (Md. 2009) (Adkins, J., concurring).

217. *Id.* ("The balancing test adopted by the majority accords to a trial court the authority to decide that a plaintiff's cause of action for defamation shall not go forward, even though it meets, on a *prima facie* basis, all of the common law requirements, because the court has decided that the defendant's interests are greater, on balance, than the plaintiff's. But the majority grants judges that discretion.").

218. Unmasking requests post-judgment can also arise, though they are uncommon. However, if an unmasking request does arise post-judgement, the standard established by the Sixth Circuit in *Signature Management* is a good model as it fairly balances the interests of the parties. Under *Signature Management*, a presumption in favor of unmasking exists "when judgment has been entered for a plaintiff" similarly to the "general presumption of open judicial records." Signature Mgmt. Team v. Doe, 876 F.3d. 831, 837 (6th Cir. 2017). The Sixth Circuit explained that it is important to consider the public's interests in the speaker's identity and the plaintiff's need to know the speaker's identity in order to obtain relief. *Id.* However, if the anonymous party has "willingly participated litigation and complied with all relief ordered," this weighs against unmasking. *Id.*

219. An analogy can be drawn between the approach recommended here and that courts are statutorily required to follow when performing a fair use inquiry in copyright law. Under the Copyright Act, when evaluating whether the use of a copyrighted work is a fair use, courts must evaluate "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." 17 U.S.C. §107. While requiring courts to consider all of these factors, and in the end to make a binary decision (i.e., is the use fair or not?), the statute leaves courts substantial flexibility in the analysis. Free Speech Sys., LLC v. Menzel, 390 F. Supp. 3d 1162, 1174 (N.D. Cal. 2019) ("The doctrine of fair use allows courts flexibility to interpret the copyright

1. Type of Anonymous Speech

Courts have long recognized that type of anonymous expression can impact the level of First Amendment protection it receives. As noted earlier, in 1995 the Supreme Court in *McIntyre v. Ohio Elections Commission* wrote that "when a law burdens core political speech" courts must apply "exacting scrutiny" and "uphold the restriction only if it is narrowly tailored to serve an overriding state interest."[220] The *McIntyre* Court explained that in upholding the decision to punish the petitioner for posting unsigned leaflets regarding an election, lower courts had failed to give proper deference to the importance of anonymous speech on political issues.[221] The Ninth Circuit has also recognized that the scope of the right to expression is context dependent, writing in 2011 in *In re Anonymous Speakers* that "[t]he right to speak, whether anonymously or otherwise, is not unlimited . . . and the degree of scrutiny varies depending on the circumstances and the type of speech at issue."[222] The Ninth Circuit concluded that political speech receives "the highest level of protection."[223] The Fourth Circuit has explained that anonymous literary and religious speech also merit high levels of protection.[224]

Unmasking challenges in relation to online speech also often involve questions of whether and to what extent the speech in question is commercial. It is well settled that, as the Supreme Court explained in a 1980 decision, "[t]he Constitution . . . accords a lesser protection to commercial

---

statute when its strict application would restrict the kind of creativity the statute intended to encourage.").

220. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995).

221. *Id.*

222. *In re* Anonymous Online Speakers, 661 F.3d 1168, 1173 (9th Cir. 2011).

223. *Id.*

224. *See* Lefkoe v. Jos. A. Bank Clothiers, Inc., 577 F.3d 240, 248 (4th Cir. 2009) ("Courts have typically protected anonymity under the First Amendment when claimed in connection with literary, religious, or political speech."); *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150 (2002) (holding that a municipal ordinance requiring local residents to register with the mayor before engaging in canvassing "violated the First Amendment as it applies to religious proselytizing, anonymous political speech, and the distribution of handbills"); Buckley v. Am. Const. L. Found., Inc., 525 U.S. 182, 186 (1999) (explaining that a state statute requiring citizens to "wear an identification badge" when circulating ballot petitions violated the First Amendment's right to free speech).

speech than to other constitutionally guaranteed expression."[225] But there can be divergent views regarding what constitutes "commercial" speech.

The *In re Anonymous Speakers* court categorized the contested speech in the case—a series of online posts about the plaintiff company that may or may not have been made by the employees of a rival company—as commercial, but its reasoning was unclear.[226] As Paul Alan Levy argued in a 2012 law review article, "[p]recedent in the Ninth Circuit and elsewhere squarely rejects the argument that commercial speech includes criticism of a company, even criticism that someone intends the company's customers to see and to harm the company's business."[227] Approximately six months after the initial ruling, the Ninth Circuit issued a revised opinion in which it omitted its explanation for why it considered the speech commercial, without providing any additional explanation.[228]

Lack of clarity regarding what constitutes *commercial* online anonymous speech is found in decisions from other courts as well. In fact, different courts can categorize the same type of speech differently. In *In re PGS Home Co. Ltd* (2019),[229] a Northern District of California court considered tweets alleging that the company did its work poorly, did not complete the work the customer had paid it to do, and did not deal "decently" with customers.[230] The court concluded that the tweets constituted commercial speech.[231] In contrast, in *Yelp, Inc. v. Superior Court*,[232] a California appellate court concluded that anonymous Yelp posts in which a customer criticized a company for the

---

225. Cent. Hudson Gas v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562–63 (1980).

226. *In re* Anonymous Online Speakers, 611 F.3d 653, 657 (9th Cir. 2010), *opinion withdrawn and superseded*, *In re* Anonymous Online Speakers (Anonymous II), 661 F.3d 1168 (9th Cir. 2011). "The Internet postings and video at issue in the petition and cross-petition are best described as types of "expression related solely to the economic interests of the speaker and its audience" and are thus properly categorized as commercial speech." *Id.*

227. Levy, *supra* note 209, at 23.

228. *In re* Anonymous Online Speakers (Anonymous II), 661 F.3d 1168 (9th Cir. 2011).

229. No. 19-mc-80139-JCS, 2019 WL 6311407 (N.D. Cal. Nov. 25, 2019).

230. *Id.* at 2.

231. *Id.* at 9.

232. 224 Cal. Rptr. 3d 887 (Cal. Ct. Ap.2017).

allegedly poor services it provided did *not* constitute commercial speech. The *Yelp* court explained that "the type of 'commercial speech' that is accorded less First Amendment protection is comprised largely of statements made *by* those engaged in commerce relating to their business—not statements made *about* them to consumers."[233] This illustrates that a category-based approach to choosing unmasking standards can be frustrated by inconsistencies in how courts categorize speech.

There is also a circular logic problem that arises in tailoring unmasking approaches to whether or not the speech in question is commercial, since answering that question may require knowing who is doing the speaking. The Ninth Circuit considered this question in *SI03, Inc. v. Bodybuilding.com, LLC*,[234] vacating and remanding a district court's denial of a motion to compel unmasking because the district court had "assessed . . . [the] motion without knowledge of the speakers' identities" and thus could not accurately categorize the contested speech.[235] The Ninth Circuit proposed a problematic, paradoxical, and procedurally burdensome alternative involving proceeding with the unmasking first, sharing the resulting information with plaintiff's counsel, and then performing an inquiry to determine if that information should be further made available; e.g., to the plaintiff and the public record.[236] Given the spotty record that courts have of maintaining the confidentiality of supposedly sealed filings and the risk that some plaintiff's attorneys, confidentiality obligations notwithstanding, might convey or suggest the identity of the defendant to their clients, such an approach would chill online anonymous speech if widely adopted.[237]

---

233. *Id.* at 896 (emphasis in original).

234. 441 F. App'x 431 (9th Cir. 2011).

235. *Id.* at 432.

236. *Id.* The court wrote that some further disclosure may be necessary "in order to resolve the underlying issue of the speakers' relationship to [the plaintiff] and the corresponding nature of their speech." *Id.* at 432 n.1. The court instructed the trial court to fashion procedural safeguards (e.g., only revealing the identity of the anonymous speaker to the plaintiff's attorney) in order to ostensibly protect the anonymous speaker while allowing the case to move forward. *Id.*

237. It is also worth noting that some types of speech (e.g., copyright infringement) receive no protection at all. But even here there can be circularity challenges if there is some question regarding whether the speech is really

In light of the above, the type of speech should weigh against unmasking if the speech is political, literary, or religious, and in favor of unmasking if the speech is commercial. However, considering the potential difficulty of ascertaining the nature of the speech without knowing the identity of the speaker, and the general inconsistencies with how speech is categorized, courts should err on the side of caution when making determinations about the nature of speech. Thus, this factor should weigh against unmasking if there is uncertainty or if determining the nature of the speech would itself require identifying the speaker.

2. Party or Nonparty

The next factor considers whether the speaker whose identity is sought is a party to the litigation. Unmasking a non-party may be critical to resolving a case—for example, if the non-party's testimony would be important in proving (or disproving) the allegations at issue. Consider the following example: Person A posts under a pseudonym on social media that he went to lunch at a particular restaurant and got serious food poisoning that started almost immediately after the meal. Person B responds to Person A's post, also under a pseudonym, saying "He's not telling the truth—I was with him for hours after that meal and he was fine." The restaurant owner believes Person A is lying and files a defamation complaint.

This a case where the testimony of Person B could be vital to fact-finding, and where the unmasking to allow that to occur—and that the plaintiff would certainly seek—would need to be of someone not a party to the litigation. Despite the potential importance of Person B's testimony, our view is that, as a non-party not accused of any wrongdoing, Person B should benefit from a higher hurdle to unmasking than Person A.

Some courts[238] facing plaintiff demands to unmask a non-party have followed the *Doe v. 2TheMart* approach—which

---

unprotected. For instance, a person who posts copyrighted content in a manner protected by fair use has a right to make the posting anonymously. But a defendant might find it hard to convince a court that the posting qualifies as fair use without providing identifying information that would amount to unmasking.

238. *See, e.g.*, Rich v. Butowsky, No. 20-mc-80081-DMR, 2020 WL 5910069 (N.D. Cal. Oct. 6, 2020) ("The court finds *2TheMart.com* persuasive for this issue and will refer to it for guidance."); Sedersten v. Taylor, No. 09-3031-CV-S-GAF,

requires that the identifying information is sought in good faith, "relates to and is directly and materially relevant to the claim or defense," and is unavailable elsewhere.[239] However, this sets the bar too low, as it permits unmasking of an anonymous speaker whose testimony might be "directly and materially relevant," but not necessary, to fact-finding (even information that is unavailable elsewhere may not be *necessary* to prove the asserted claim). When deciding whether to order unmasking, a better approach is for courts to examine the potential role of the anonymous non-party's testimony in light of the other evidentiary information, as well as the chilling effect and resulting broader harms that might result from the unmasking. This analysis will be highly context-dependent. For instance, unmasking an anonymous online speaker whose statements support an accusation regarding a claim of relatively minor harm might then disincentivize future speakers from speaking anonymously and whose later testimony might prove vital to resolving accusations of major harms.

3. Comparative Harms

The third factor examines the comparative potential harms to a party if an improper unmasking decision is made. This can occur if a court declines to allow unmasking of a defendant who engaged in tortious conduct, as well as if a court allows unmasking of a defendant who did not engage in tortious conduct. Consider, for example, a restaurant owner who files a defamation claim against an anonymous Yelp reviewer who claims that he or she was dramatically overcharged for a recent meal. If, as alleged by the restaurant owner, the reviewer's claims are false, then a court decision to deny unmasking will leave the restaurant owner with little recourse—unable to get the defamatory post(s) removed or to seek monetary damages. The most the owner can do is to respond to the post and hope that prospective customers will believe the owner's side of the

---

2009 WL 4802567 (W.D. Mo. Dec. 9, 2009) (relying on the *2TheMart.com* test to quash plaintiff's motion to compel); Enterline v. Pocono Med. Ctr., No. 3:08-CV-1934, 2008 WL 5192386 (M.D. Pa. Dec. 11, 2008) (applying the *2TheMart.com* test to deny plaintiff's motion to compel on the grounds that information was available from alternate sources); Solers, Inc. v. Doe, 977 A.2d 941, 952 (D.C. 2009) (applying *2TheMart*.com test).

239. Doe v. 2TheMart.com, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001) (outlining the standard a party must meet to compel the unmasking of an anonymous speaker who is not a party to the litigation).

story. On the other hand, a court decision to unmask a reviewer whose claims are accurate would violate that reviewer's constitutional right to speak anonymously.

While both types of wrong unmasking decision are problematic, they might cause different relative levels of harm. To explore this, consider two scenarios. First, if the restaurant has a long history of many complaints regarding overcharging from many different reviewers, the marginal harm to the restaurant owner of the defendant's review is lower regardless of its accuracy. In this scenario, a court might conclude that the potential harm to the defendant that would arise through an incorrect decision in favor of unmasking (i.e., allowing unmasking and then finding that the review was accurate) is higher than the potential harm to the plaintiff arising from an incorrect decision denying the unmasking demand.

For the second scenario, suppose that, other than from the anonymous reviewer named as the defendant, the restaurant has a history of receiving exclusively glowing reviews. In this scenario, a court might allocate heightened importance to determining the accuracy of the review(s) cited in the complaint, and proceed to authorize the unmasking. While the potential harm of an incorrect decision for the plaintiff might be the same regardless of whether the overcharging accusations in an accurate negative review were consistent with other reviews of the restaurant, the potential harm to the *defendant* of failing to authorize the unmasking is much higher. Thus, in a relative sense, this second scenario would weigh more heavily in favor of unmasking than the first.

V. CONCLUSIONS

With anonymous online postings now a major component of the digital ecosystem, the issue of unmasking will arise with increasing frequency in both civil litigation and criminal investigations and prosecutions. With respect to civil litigation, this Article has argued that the current patchwork of caselaw is inconsistent, provides insufficiently clear guidance, and often fails to adequately consider the expression rights of anonymous online speakers.

The Article thus proposes an approach that adopts the prima facie burden of *Dendrite* with respect to the requisite evidentiary showing by a party seeking unmasking, but also goes further in articulating a specific balancing test including

three factors: (1) the type of anonymous speech at issue, (2) whether the speaker is a party to the underlying litigation, and (3) the extent and comparative degree of harm to the parties if the wrong unmasking decision is made. This framework offers the advantage of being flexible and adaptable, and avoids the challenge of attempting to create a one-size-fits-all standard that will inevitably prove inadequate given the tremendous variety of factual circumstances encountered in unmasking cases.

The Article has also considered unmasking in grand jury investigations, arguing that the Ninth Circuit's *Glassdoor* decision—which requires only that a grand jury investigation be carried out in good faith when determining whether to unmask online speakers who have published statements of interest to the grand jury—sets too low a bar. Establishing that a grand jury is acting in good faith should be a necessary but not sufficient condition in relation to unmasking. Additionally, the *Glassdoor* decision incorrectly failed to recognize that online users can have associational privacy rights despite being anonymous to one another. In combination, these factors indicate that courts should follow the Western District of Wisconsin's approach in *Amazon* by fashioning subpoenas in such a way that gives grand juries access to information necessary for their investigations while still protecting the First Amendment rights of the anonymous online speakers these grand juries seek to unmask.