The Construction of Doxxing in Judicial Opinions

EMMA LURIE, University of Pennsylvania

Doxxing—the unauthorized online publication of personal information with intent for third parties to engage in harassment—has prompted fourteen U.S. states to enact anti-doxxing legislation since 2018. Yet policy debates lack empirical grounding in how courts interpret this phenomenon. This paper conducts a content analysis of fourteen state anti-doxxing statutes and eighty-two judicial opinions, revealing how legal institutions actively construct doxxing as a sociotechnical harm. Courts encounter doxxing across four contexts: First Amendment challenges, personal jurisdiction disputes, judicial transparency questions, and evidence of harassment patterns. These contexts shape which harms become legally cognizable and which victims receive protection. The analysis identifies two bottlenecks: personal jurisdiction doctrine incompatible with online platforms' geographic reach, and judicial risk assessment that undervalues women and minorities' experiences. This work demonstrates why addressing doxxing requires interdisciplinary collaboration, as it demonstrates the necessity of legal reform informed by technical constraints, and technical design shaped by legal doctrine and empirical research.

Additional Key Words and Phrases: doxxing, privacy, law, judicial opinions

ACM Reference Format:
Emma Lurie. 2026. The Construction of Doxxing in Judicial Opinions. In *Proceedings of ACM Conference on Computers and the Law (CS+Law '26).* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

On August 12, 2017, as white nationalists clashed with protesters in Charlottesville, Virginia, a gray Dodge Challenger plowed into a crowd, killing Heather Heyer and injuring nineteen others. As police searched for the driver, 4Chan users began their own investigation, discovering a similar vehicle had been registered to Jerome Vangheluwe of Michigan. Without verification, *GotNews* published an article identifying Jerome's son Joel as the killer. Twitter users posted the family's address and vehicle identification number: a practice known as doxxing. Neither Jerome nor Joel had any connection to the attack. As the Vangheluwes hosted a wedding at their Michigan home, they became overwhelmed with threats. Clients severed business relationships and police warned the family to leave their home.

Two years later, a Michigan court had to decide not whether the doxxing harmed the Vangheluwes, but whether the court had jurisdiction over the case. *Vangheluwe v. Got News* (2019) illustrates how courts don't simply apply law but regulate who can be held responsible for sociotechnical harms.[1]

This paper defines doxxing as the unauthorized online publication of personal information with intent for third parties to engage in harassment. Doxxing is rising and causes significant harm [9, 27, 36]. Fourteen states have enacted anti-doxxing laws in the past six years. Yet like other technology-mediated harassment, victims struggle to make their harm legally legible [3]. Lawsuits are prohibitively expensive, legal gaps exist, and law enforcement remains skeptical of online harassment's seriousness [3, 24].

[1] *Vangheluwe v. Got News, LLC*, 365 F. Supp. 3d 850 (E.D. Mich. 2019).

Author's Contact Information: Emma Lurie, University of Pennsylvania, ewlurie@seas.upenn.edu.

Manuscript submitted to ACM

Scholars have proposed various responses to doxxing: additional penalties [22, 23, 30], protections for law enforcement [13], or raised concerns about weaponization against journalists [20]. Over a dozen states have passed anti-doxxing laws [6, 20]. However, current debates are not grounded in how courts are already handling doxxing.

This paper fills that empirical gap. As courts interpret doxxing and craft remedies, they shape society's understanding of the act and related harms, which influences how individuals experience it as perpetrators and victims, and how legislators respond. Courts are not passive recipients of technology but through language, theories, and analogies determine its social meaning and the distribution of rights and responsibilities [2, 16]. Through their interpretive work, legal actors draw boundaries for the sociotechnical governance of online harms, establishing precedents that influence how platforms, users, and stakeholders understand their obligations.

This paper conducts a content analysis of fourteen state anti-doxxing statutes and eighty-two judicial opinions that explicitly reference doxxing. The analysis reveals courts encounter doxxing across four contexts: (1) First Amendment challenges, (2) personal jurisdiction clashes, (3) balancing judicial transparency against doxxing risks, and (4) evidence of harassment patterns. These contexts shape which harms become legally cognizable, which victims receive protection, and which regulatory interventions become possible.

This paper identifies two bottlenecks that illustrate why doxxing demands interdisciplinary analysis. First, personal jurisdiction doctrine filters victims out of federal court based on geographic requirements incompatible with how online platforms operate. Second, judicial risk assessment systematically undervalues women and minorities' experiences, ignoring empirical harassment research. These bottlenecks show that doxxing cannot be addressed through law or computer science alone: technical systems enable the harm's geographic reach, while legal institutions define available remedies. This paper contributes to interdisciplinary scholarship by revealing how judicial construction of doxxing creates implicit content moderation requirements while failing to account for technical realities that make internet personal jurisdiction doctrine insufficient and social scientific evidence that should inform judges' risk models. Addressing these gaps requires interdisciplinary collaboration—legal reform informed by technical constraints, and technical design shaped by legal doctrine and empirical research.

2 Related Research

Doxxing, the unauthorized online publication of personal information that occurs with the intent for third parties to engage in harassment or other abuse, is theoretically situated within the wider phenomenon of digital vigilantism. Digital vigilantism involves online actions taken by individuals or groups to enforce perceived social norms or exact informal justice when formal legal institutions appear inadequate or unresponsive [33].

Scholars like Loveluck locate doxxing within broader digital vigilantism typologies, describing it specifically as a tactic of "hounding," where sustained harassment and public humiliation are central objectives [21]. In this framing, digital vigilantism functions as an informal but powerful mode of social control that often challenges traditional legal and media institutions tasked with norm enforcement and accountability [21].

Online harassment, including doxxing, is now widely recognized as a pervasive social problem that disproportionately affects women and people of color [17, 34]. Researchers across disciplines, including law [3], computer science [14], and other social sciences [1], have documented the far-reaching psychological, economic, and physical consequences of such harassment [4]. These scholars have called attention to the way online harassment replicates and amplifies offline power imbalances, shaping both access to online spaces and the participation of marginalized groups [3]. This body of research demonstrates that online harassment like doxxing represents a paradigmatic sociotechnical harm that emerges not from isolated technical failures or legal oversights, but from the entangled interactions of platform design and regulatory structures [10, 26].

Doxxing originally emerged from hacker communities in the 1990s as a method of revenge by revealing anonymous individuals' identities, doxxing has evolved significantly in scope and method, prompting ongoing debates about its definition and impact [12, 20]. The definitional boundaries of doxxing remain contested, reflecting the practice's complex and multifaceted nature. Some formulations view it as a "complex, gendered communicative process" in which personal identifying information is disclosed without consent, exposing targets to heightened vulnerability and harm [9]. Others focus more on the context and intent of dissemination, emphasizing that the act becomes doxxing when personal information is shared before an audience expected to be hostile to the subject [7]. A narrower interpretation limits doxxing to disclosures involving residential addresses or legally protected sensitive information, drawing a line between general online shaming and the more severe breaches of informational privacy [15].

Danielle Citron and Daniel Solove highlight that doxxing involves both tangible physical risks and psychological trauma, with effects that can persist due to the perpetual availability of personal information online [4]. They advocate for recognizing psychological harms, often undervalued by the legal system, urging stronger and more responsive legal frameworks.

Applying Helen Nissenbaum's theory of contextual integrity provides further analytical clarity, suggesting that privacy harms from doxxing stem from violations of contextual norms around information sharing rather than simply the nature of the disclosed information itself [25]. Thus, even ostensibly "non-sensitive" data like home addresses or employment details can constitute significant harm when shared inappropriately [4, 5].

Legal responses to doxxing have been piecemeal and inconsistent. Individual states have enacted anti-doxxing laws with substantial variations in scope, types of protected information, and the levels of culpability required for prosecution [20]. These legislative differences highlight ongoing challenges and tensions, including concerns over free speech implications and effectiveness in addressing doxxing harms.

The First Amendment poses a significant constraint on legal responses to doxxing, particularly when the disclosed information is already publicly available or when the act is framed as political speech. In their review of seven state anti-doxxing laws, LoMonte and Fiku caution that broadly written anti-doxxing statutes may criminalize constitutionally protected activities such as journalism, whistleblowing, or public-interest advocacy [20]. Courts are reluctant to suppress speech absent a clear showing of intent to incite imminent harm, and overly expansive laws risk being struck down as unconstitutionally vague or overbroad [19]. This constitutional backdrop complicates legislative efforts, as any attempt to curb harmful disclosures must be carefully tailored to avoid infringing on the First Amendment.

Legal scholars have also proposed a range of reforms to address doxxing more directly. Some advocate for the creation of a federal anti-doxxing statute, while others suggest expanding existing tort doctrines, such as intentional infliction of emotional distress or public disclosure of private facts, to encompass doxxing [22, 23, 30]. While these proposals vary in scope and feasibility, they reflect a growing consensus that existing legal doctrine is inadequate to address the harms caused by doxxing.

This paper studies how judicial actors conceptualize and contest the nature and harms of doxxing. Answering this question bridges existing academic research on the social and privacy-related dimensions of doxxing with practical legal applications, offering insights for future legal reforms aimed at balancing a safe online environment for marginalized individuals while protecting freedom of expression.

3 Methods

This paper employs the qualitative research method of content analysis [18] focusing on two two corpora of documents. The first are state anti-doxxing statutes drafted by policymakers, specifically state legislators. The second corpus is comprised of eighty-two judicial opinions that explicitly mention doxxing. This methodological approach enables the tracing of patterns in legal reasoning across different institutional contexts while maintaining attention to the specific ways that expert knowledge shapes regulation [11].

Content analysis emerged from social science and has gained traction in empirical legal scholarship due to its capacity to systematically categorize and interpret qualitative textual data. Unlike quantitative approaches that might count case outcomes or measure variables, content analysis allows researchers to examine the underlying reasoning, values, and conceptual frameworks that structure legal decision-making [11].

3.1 Methods: State Anti-Doxxing Laws

There are over a dozzen state anti-doxxing laws [6, 20]. Identifying relevant state anti-doxxing legislation presented an initial challenge, as most of the laws characterized as "anti-doxxing laws" do not use the term "doxxing" in the title or text of the statute, even if the legislative history suggests that the purpose was to address doxxing. To identify anti-doxxing statutes, this paper follows the definitional criteria established by LoMonte and Fiku in their analysis [20]. They define an anti-doxxing law as legislation that specifically penalizes the publication of personally identifying information with the intent to expose individuals to harassment or violence by third parties. This definition helpfully distinguishes anti-doxxing laws from broader privacy statutes, traditional stalking or harassment laws.

There were fourteen state anti-doxxing laws enacted between 2010 and 2024 across Arizona, Arkansas, California, Colorado, Connecticut, Florida, Kentucky, Minnesota, Missouri, Nevada, Oklahoma, Oregon, Utah, and Virginia. Notably, only Arkansas explicitly uses the term "doxxing" in its statute title, while the remaining thirteen states regulate similar underlying behaviors through different phrases.

For each statute, the authors coded across four dimensions that capture how state legislators construct doxxing as a legal phenomenon:

Penalty Structure: The authors categorized whether each law creates criminal penalties, civil remedies, or both, and classified criminal penalties by severity (misdemeanor vs. felony). This analysis reveals how seriously different states view doxxing and what enforcement mechanisms they prioritize. Twelve of the fourteen laws create criminal penalties, with most classified as misdemeanors, though several states impose enhanced penalties for doxxing of particular classes like law enforcement officers.

Covered persons: The authors determined whether statutes provide universal protection or limit coverage to specific categories like minors, law enforcement officers, healthcare workers, or other "protected careers." This dimension reveals assumptions about who deserves protection from doxxing and reflects different theories about the relative harms and risks faced by various groups. For example, Minnesota's law protects only law enforcement officials, while California's law provides broader coverage.

Personal Information Categories: The authors analyzed what types of information each statute covers as the information disclosed in the doxxing, ranging from broad definitions encompassing "any personally identifiable information" to narrow approaches limited to specific categories like home addresses or photographs. This analysis reveals different theories about which information disclosures create actionable harm and how privacy violations should be conceptualized.

First Amendment Considerations: The authors determined whether statutes include explicit First Amendment carve-outs or acknowledgments of constitutional speech protections. Only Arizona and Nevada include such provisions.

3.2 Methods: Judicial Opinions

This paper relies on content analysis to code eighty-two judicial opinions. It is important to note that judicial opinions are collaborative texts that reflect multiple forms of legal expertise [2]. While judges author these opinions (often with assistance from law clerks), they do not generate analysis from a blank slate. The parties litigating, represented by lawyers in most cases in this corpus, submit written briefs and make oral arguments that shape judicial reasoning. Courts frequently quote directly from party briefings, incorporate arguments from legal counsel, and respond to specific framing choices made by litigants.

This paper details the results of a content analysis of the eighty-two judicial opinions that explicitly reference doxxing. To create the corpus, the authors queried Westlaw, an online legal research database for judicial opinions that contained the term "dox," "doxx," "doxing," or "doxxing" and then manually reviewed the use of the relevant term to see if the case was related to a controversy involving an online dispute, harassment, or disclosure of online information. There were eighty-nine unique citations, but seven of those were duplicative with regard to the parties and content of the opinion. Therefore, the authors were left with eighty-two unique judicial opinions from November 2015 to February 2024.

Through multiple rounds of coding, the authors identified patterns in judicial reasoning that coalesced into the four primary legal contexts: (1) First Amendment challenges, (2) personal jurisdiction clashes, (3) balancing judicial transparency, and (4) evidence of patterns of harassment. Each round of coding involved returning to previously coded opinions to test category stability and identify cases that didn't fit existing frameworks.

The analysis also incorporates deductive elements drawn from the legal construction of technology framework [16]. This framework provided analytical concepts: values, targets of regulation, and objects of regulation. The legal construction of technology framework proved particularly valuable for understanding variation within the inductively derived categories. For example, while multiple cases involve First Amendment challenges to doxxing, courts apply different values frameworks (marketplace of ideas versus dignity-based approaches), focus on different regulatory targets (speaker intent versus audience response), and reach different conclusions about constitutional protection. The framework helped reveal these deeper patterns in judicial reasoning.

For each opinion, the authors coded four dimensions that capture both the legal reasoning and the regulatory implications:

Definitional Sources and Meaning: How courts define or characterize doxxing, including whether they provide explicit definitions, rely on dictionary sources, focus on information categories, or leave the term undefined. This dimension reveals assumptions about what constitutes doxxing and which aspects courts view as legally significant. Courts adopt four main definitional sources: general dictionary definitions (most common), malicious intent requirements (typically in cases skeptical of doxxing harms), information-type focused definitions (emphasizing home addresses or images), and implicit definitions through context.

Analogical Reasoning: What legal concepts, doctrines, or phenomena courts compare doxxing to, such as traditional harassment, cyberstalking, true threats, defamation, or invasion of privacy. This dimension illuminates how courts translate novel technological practices into familiar legal categories. The analogies courts choose shape their analysis—comparing doxxing to true threats emphasizes speaker intent and audience fear, while comparing it to invasion of privacy focuses on information sensitivity and disclosure norms.

Values and Interests: What competing values (e.g., free speech vs. safety, transparency vs. privacy, individual autonomy vs. collective security) courts explicitly or implicitly balance when addressing doxxing. This coding captures both values that courts explicitly articulate and those revealed through their reasoning patterns. The salience of different values varies across the four legal contexts, with First Amendment cases emphasizing speech values, jurisdiction cases focusing on fairness and state sovereignty, and transparency cases balancing openness against safety.

Regulatory Targets: What specific aspects of doxxing behavior courts focus on for potential regulation—the content of disclosed information, the platforms enabling distribution, the motivations of doxxers, the responses of third parties, or the broader social context. This dimension reveals what courts view as the appropriate objects of legal intervention. Some courts focus narrowly on the disclosure itself, while others examine the broader sociotechnical system that enables doxxing harms.

3.3 Methods: Limitations

This methodology has several limitations. First, the focus on published judicial opinions means that many doxxing-related legal disputes, particularly those resolved through settlement, plea agreements, or unpublished decisions, are not captured in this analysis. This may skew the sample toward cases that present novel legal questions or involve higher-stakes disputes. Second, the keyword search approach may miss cases where courts address doxxing-like behavior without using the specific terminology. However, the focus of this article is precisely on how courts make sense of the concept of "doxxing" as it has emerged in legal discourse, making this limitation less problematic for this project. Third, the analysis of state statutes is necessarily limited by the availability of enforcement data. Many anti-doxxing laws are relatively recent, and data on their implementation and effectiveness may not yet be available. Despite these limitations, this methodological approach provides a foundation for examining how legal expertise constructs doxxing in legislation and judicial opinions, revealing patterns that would not be visible through analysis of individual cases or an analysis of a particular doctrinal context.

4 Findings: Statute Analysis

The review of the fourteen state statutes[2] finds substantial differences in states' choice of enforcement mechanisms and covered populations (see Table 1 in the Appendix).

There is a clear preference by state legislatures to criminalize doxxing. Twelve of fourteen states employ criminal penalties as the remedy to doxxing, with only Oregon and Nevada relying exclusively on civil causes of action. Most of the criminal anti-doxxing statutes establish misdemeanor-level baseline penalties, though several states create escalation mechanisms to charge doxxing as a felony. Kentucky and Arkansas allow penalties to increase to based on actual harm caused (physical injury, death, or monetary loss), while Missouri and Virginia escalate penalties based on the status of the target (law enforcement officers, judges). These distinct approaches reveal competing theories about what makes doxxing particularly harmful whether it is the actual consequences that flow from information disclosure or the inherent vulnerability of certain classes of individuals.

Seven states provide enhanced protections for specific categories of individuals, with law enforcement officers receiving the most extensive coverage (five of the fourteen states). This pattern likely reflects political realities about which groups have sufficient influence to secure special legislative protections and policy judgments about differential

[2] Ariz. Rev. Stat. Ann. § 13-2916, Ark. Code Ann. § 5-27-610, Cal. Penal Code § 653.2, Colo. Rev. Stat. § 18-9-313, Conn. Gen. Stat. § 53a-181d, Fla. Stat. § 836.115, Ky. Rev. Stat. Ann. § 525.085, Minn. Stat. § 609.5151, Mo. Rev. Stat. § 565.240, Nev. Rev. Stat. § 41.1347, Okla. Stat. tit. 21, § 1176, Or. Rev. Stat. § 30.835, Utah Code Ann. § 76-9-201, Va. Code Ann. § 18.2-186.4

vulnerability to doxxing harms. The prominence of law enforcement protection likely stems from concerns about officer safety.

Colorado represents the broadest approach to providing differential protection for particular professions, extending enhanced protections to educators, healthcare workers, human services workers, judges, prosecutors, and public safety personnel. This broad coverage suggests a policy judgment that public servants generally face elevated doxxing risks due to their professional roles.

Conversely, there is an absence of dedicated protection for commonly identified vulnerable populations: only Arkansas' statute specifically protects minors.

States employ diverse intent standards, ranging from specific malicious intent requirements (Oregon, Kentucky, Virginia) to more objective "imminent and serious threat" standards (Minnesota, Colorado). California and Arizona impose the most complex requirements, demanding both intent to cause fear and intent that third parties will take harmful action. This variation creates substantial differences in prosecutorial burden and the likely case outcomes across jurisdictions.

Only three states (Nevada, Arizona, Connecticut) include explicit First Amendment protections. They make explicit that speech covered by the First Amendment should be charged under the law. The importance of such carve-outs is unclear. Presumably, no law is enforced in violation of the First Amendment, but perhaps the call-out of First Amendment protections provides insight into the legislatures' concern over anti-doxxing laws infringing on First Amendment protections.

5 Findings: Judicial Opinions

The eighty-two judicial opinions in this corpus reveal doxxing's emergence in legal discourse over the past decade. Prior to 2019, fewer than five judicial opinions per year referenced doxxing terminology. Since 2019, there has been steady growth in judicial attention to doxxing, with mentions increasing from seventeen cases in 2022 to twenty-six cases in 2023. This timeline suggests that doxxing has moved from a relatively obscure internet phenomenon to a recognized legal concern requiring judicial attention.

The corpus comprises seventy-four federal cases and eight state cases, with doxxing references appearing across all federal circuits except the Eighth Circuit. The Ninth Circuit accounts for the highest number of doxxing references, reflecting both the Circuit's large population and its jurisdiction over technology-heavy regions like California. This geographic distribution indicates that doxxing has become a nationwide legal phenomenon rather than being concentrated in particular jurisdictions. The factual scenarios underlying these cases include both from highly publicized national controversies to local disputes. High-profile cases include January 6th prosecutions, disputes over 2020 election fraud claims, cases involving Alabama Senate candidate Roy Moore, and proceedings related to President Trump. However, the corpus also includes cases that received no media attention, involving college sexual assault allegations, police brutality claims, and disputes with school officials. This range suggests that doxxing has become a common enough phenomenon to appear across the full spectrum of civil and criminal litigation.

5.1 First Amendment Challenges

When courts frame doxxing as a type of speech or ask whether doxxing is covered by the First Amendment, the court orients the analysis of doxxing towards particular values, logics, and analogies. When framed as a type of speech, the legal analysis focuses on First Amendment protection. The First Amendment states that "Congress shall make no law...

abridging the freedom of speech."[3] Among its other goals, First Amendment doctrine looks to protect matters of public concern and limit chilling effects [29, 35]. First Amendment values prioritize a robust marketplace of ideas and the implicit belief that words alone generally do not cause a legally cognizable injury [31].

However, not all speech receives constitutional protection. Under First Amendment doctrine, not all speech is protected from regulation. Courts must determine whether or not doxxing falls into categories of "low-value speech" such as true threats, incitement, or defamation that remain outside First Amendment coverage [19]. Characterizing doxxing as speech allows courts to make comparisons and analogies to these established categories of unprotected expression.

Take for example, *United States v. Cook* (2020), where a man indicted on cyberstalking charges relating to his doxxing of a law enforcement officer's address and names of family members had stated: "God willing I'm going to take them out."[4] The court found that his posts did not rise to the level of specificity necessary to constitute a true threat. Therefore, his stalking charges were dismissed. The Court in *Cook* was skeptical that doxxing individuals using otherwise available information could ever constitute a true threat:

> "[No cases] of the Fifth Circuit cases discuss a situation in which a person's information, such as address or family members' names, is shared publicly; a phenomenon sometimes referred to a "doxing" or "doxxing". Certainly, sharing public information, while potentially offensive and disagreeable, does not rise to the level of a true threat."[5]

In contrast, in *D.S. v. T.M.* (2023), a woman appealed a harassment prevention order issued against her on the grounds that her doxxing and other harassment of the plaintiff were protected speech.[6] The defendant had posted a video on social media that filmed the plaintiff and his home where she announced the plaintiff's name and address and called him racist and a perpetrator of sexual harassment. She did this after "incessantly" contacting the plaintiff. The court found it was reasonable to find that the defendant's intent was to cause the plaintiff fear and rose to the level of a true threats. The court found that her conduct, "specifically, posting the video of the plaintiff and his home on social media" constituted unprotected speech and the harassment prevention order was affirmed.[7]

One difference between the two cases is the breadth of the context courts adopt to understand doxxing. In *Cook*, the court examines doxxing as speech in isolation from additional context. In this approach, doxxing is considered the text on the "page" (most frequently a social media post) and disconnected from subsequent harms. As such, courts look to the words of the doxxer's message to determine the value of the speech. In *D.S. v. T.M.*, the court views doxxing as part of a wider pattern of speech and other non-expressive conduct. In this second approach, doxxing is viewed as part of a wider set of speech acts where doxxing is one speech act in a pattern of behaviors. This wider view of behavior and other context often allows courts to make some kind of claim about whether under an objective standard, the listener had a reasonable basis to fear for their safety.

An additional important example in this category is *DeHart v. Tofte*, where elected school board officials sued parents of students under the Oregon anti-doxxing statute for improper disclosure of private information, alleging that the officials suffered severe emotional distress via the parent's doxxing of officials in a private Facebook group.[8] The court found that the parent's doxxing of school officials was protected speech in connection with the public interest and

[3] Amendment I to the Constitution of the United States.
[4] *United States v. Cook*, 472 F. Supp. 3d 326 (N.D. Miss. 2020).
[5] *Id.* at 335.
[6] *D.S. v. T.M.*, 102 Mass. App. Ct. 1106, 203 N.E.3d 1173 (2023).
[7] *Id.* at 4.
[8] *DeHart v. Tofte*, 326 Or. App. 720, 533 P.3d 829, review denied, 371 Or. 715, 539 P.3d 787 (2023).

that reasonable people in the school board official's positions would not suffer severe emotional distress because of the particular types of information disclosed. A theme among this category of cases is the importance of matters of public concern. While the Court has long struggled to provide a clear definition of matters of public concern, but the underlying principle—that speech that implicate core First Amendment topics—particularly speech that implicates public affairs—is deserving of the utmost legal protection. The concept of "matters of public interest or concern" is widely used in the law while also widely acknowledge to be ambiguous and contested.

One way that states legislatures have codified the importance of preserving speech about matters of public concern is via anti-SLAPP ("Strategic Lawsuits Against Public Participation") laws. The purpose of anti-SLAPP laws is to be speech protective via limiting chilling effects, such that speakers or others considering futures speech are not deterred by the threat of a frivolous lawsuit [28].

Nine of the eighty-nine cases in the corpus invoke anti-SLAPP laws, with eight of the nine anti-SLAPP actions arising out of California's anti-SLAPP law. The purpose of anti-SLAPP laws (which 33 U.S. states have) is to prevent nuisance lawsuits that are meant to chill speech. When a case is brought—perhaps alleging defamation or libel, anti-SLAPP laws can be used to dismiss the claims and force the plaintiff to cover the defendant's attorney fees. A key part of the legal standard for dismissing cases under anti-SLAPP laws is establishing that the speech, in this case, doxxing, touched on a matter of public interest or social importance.

5.2 Personal Jurisdiction Clashes

The law of personal jurisdiction, which governs whether a court has the authority to require a party to appear, has struggled to adapt to technology and globalization. The doctrine of personal jurisdiction has traditionally been closely linked to physical location and geographical boundaries, with jurisdictional authority often depending on the defendant's physical presence within a specific state. However, the internet has blurred these boundaries, creating scenarios where individuals and entities can have a substantial impact in jurisdictions without ever physically entering them.

Courts have struggled to evaluate their jurisdiction when the case involves online activities, ranging from commerce to doxxing. The Supreme Court has repeatedly declined addressing questions of when internet conduct constitutes sufficient contacts for personal jurisdiction, most recently in *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.* (2021).[9] The cases in the corpus about personal jurisdiction ask whether the defendant has sufficiently targeted the forum.

When a federal court adjudicates a civil dispute between parties who are citizens of different states, it may exercise jurisdiction, if the defendant has sufficient "minimum contacts" with the forum state. Minimum contacts analysis balances the defendant's rights against the forum state's interest in protecting its residents and ensuring access to justice. The issue is frequently discussed in the judicial opinions in the corpus, with seventeen of the eighty-two cases engaging in a minimum contacts analysis. The framing of doxxing as a question of personal jurisdiction doctrine brings up different values, logics, and analogies.

For example, courts rely on the constitutional principle of due process to evaluate minimum contacts. Due process requires that an out-of-state defendant have "minimum contacts" with the forum state sufficient to comport with "traditional notions of fair play and substantial justice."[10] The principle is based on the idea that the defendant must "purposefully avail[ ] [herself] of the privilege of conducting activities within the forum State, thus invoking the benefits

[9] *Ford Motor Co. v. Montana Eighth Judicial Dist.*, 592 US 351 (2021),

[10] *International Shoe Co. v. State of Washington, Office of Unemployment Compensation and Placement*, 326 U.S. 310 (1945).

and protections of its laws," which "ensures that a defendant will not be hauled into a jurisdiction solely as a result of 'random,' 'fortuitous,' or 'attenuated' contacts."[11]

For example, in *Vangheluwe v. Got News, LLC* (2019), the case detailed in the introduction to this paper, a Michigan resident sued out-of-state internet users for defamation. These users, including a news publisher, mistakenly identified him as a murderer on Twitter and doxxed him by revealing his home address and license plate number. The users challenged the jurisdiction of the Michigan court, citing insufficient contacts with the forum state of Michigan. The court found sufficient contacts between the defendant and forum state to survive the jurisdictional challenge.

Contrast that with *Blessing v. Chandrasekhar* (2021), where Kentucky high school students sued out-of-state internet users for civil harassment, menacing, invasion of privacy, and aiding and abetting.[12] Internet users had engaged in a viral doxxing and harassment campaign after video footage emerged ostensibly showing the Kentucky high schoolers harassing Native American activists at the Lincoln Memorial. The out-of-state internet users challenged the jurisdiction of the Kentucky court. The court dismissed the case for lack of personal jurisdiction.

As a result of a minimum contacts analysis, doxxing is evaluated based on the physical presence of the doxxer in relation to the doxxed. This is somewhat counter-intuitive to the nature of doxxing, as the physical proximity of the doxxer to the doxxed in no way bears on the physical danger or other consequences the target of the doxxing faces from third-parties motivated by the doxxer. But, as *Blessing* makes clear, the Supreme Court has "consistently rejected attempts to satisfy the defendant-focused 'minimum contacts' inquiry by demonstrating contacts between ... third parties[ ] and the forum state." For personal jurisdiction purposes, the focus of the minimum contacts analysis must be between the defendant and the forum state.

5.3 Balancing Judicial Transparency

This category reflects doxxing emerging as a risk through litigation. In these cases, a party has typically made a motion to litigate under a pseudonym, redact or seal personally identifiable information, or add stipulations to protect the confidentiality of their identity or home address. The posture of these cases are different as these cases are not about seeking remedies for harms of doxxing but rather seeking protection against the possibility of doxxing.

For example, in *Cancino Castellar v. Mayorkas*, the court granted Custom and Border Patrol agents' motion to redact their names, non-public email addresses, and phone number. The agents were able to overcome a strong presumption the open access of judicial records, by demonstrating "some likelihood" of the specific harm via "doxxing, which imposes 'a direct safety concern for Agents and their family members.'"

In *Allen v. City of Graham*, protestors sought early discovery in their suit against local law enforcement after allegedly being improperly sprayed with tear gas. Many of the officers remained unnamed defendants and the protestors sought early discovery to uncover the identity of the officers who were party to the suit. The court explained that the disclosure of the officer's personal information could cause "irreparable harm" if distributed via doxxing, which would make the officer's "tantalizing targets of vigilante justice."[13]

Courts do not always take the governments arguments at face value. In *Club v. Sierra Club* (2020), where the court found the Environmental Protection Agency (EPA) could not claw back documents it had failed to properly redact when producing relevant material to an environmental advocacy group's Freedom of Information Act (FOIA) request.

[11] *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985).
[12] *Blessing v. Chandrasekhar*, 988 F.3d 889 (6th Cir. 2021).
[13] *Allen v. City of Graham*, No. 1:20CV997, 2021 WL 2037983, at *9-10 (M.D.N.C. May 21, 2021).

The court found that the EPA had "presented no evidence" of doxxing or other coordinated harassment in this instance beyond "pure speculation" given that no past lobbyists on EPA emails had been doxxed or harassed in this way. While cases that weigh the potential doxxing of litigants as a future risk are governed by different legal rules or standards, the values underlying the court's balancing are relatively constant. Courts are balancing a presumption of judicial transparency and openness to the public against the privacy interest of litigants.[14]

The values of judicial access and openness stand for the proposition that the public has the right to access judicial records. The idea is that the public should know what is happening in a court room. The presumption of access provides the public with a way of ensuring an accountable judiciary and confidence in the administration of justice. This presumption of openness is understood to be grounded as a listener-oriented First Amendment principle, that allows members of the public and press to hear and learn about what happens in the court room, given their close relationship to matters of public concern.

The court weighs the default presumption of judicial openness against what it describes as the privacy interest of litigants. The privacy interest here is "not conceptualized as the right to be let alone," or an analysis based on the sensitivity of the disclosed data categories; rather, it is formulated as the risk of harm to litigants by disclosure of the data. What seems to be the most persuasive to courts is litigants citing examples of past doxxing of similarly positioned individuals or entities. Potential physical danger is the most often cited harm flowing from the violation of the litigant's privacy interest. However, the amount of evidence required to convince the court of potential physical danger seems to vary by court and the profession of the litigant.

5.4 Evidence of Patterns of Harassment

In these cases, doxxing is cited as an example of behavior or conduct, among other examples of allegedly problematic behaviors. Doxxing is often listed in a series with other offenses like harassment or threats, but these offenses are not the causes of action or underlying claims at issue. Rather, plaintiffs in their complaint (excerpted in the opinion) or judges in their opinions are raising doxxing as evidence of the defendant's conduct that may broadly speak to the allegedly illegal behavior at the heart of the case or motion.

In *United States v. Trader*, a man was convicted of charges including enticing a minor to produce sexually explicit video. In an appeal of the conviction, the court recounted facts from the trial, including that an expert witness "admitted that he was not aware that [defendant] continued molesting his daughters and downloading child pornography while on probation and bond, that he had over 100 victims, or that he threatened to dox his young victims if they did not continue sending him images."[15] The conviction was affirmed by the court. Here doxxing is discussed as a way to further illustrate the deeply disturbing conduct of the defendant.

Doxxing in these cases is often provided as an example of bad conduct. Even though doxxing itself may only be tangentially related to the allegedly illegal conduct, it provides some amount of supporting entity that this person should be legally liable. Courts are weighing the value of justice, as it reflects what the plaintiff sees as a just outcome. The object being regulated in this category of cases is often broader than in other conceptualizations of doxxing. Doxxing is used as an example of the kind of conduct the defendant participates in or threatens to participate in. As such, definitions or intent standards are less important in the conceptualization of doxxing. Rather, doxxing, when it occurs alongside other types of problematic conduct, provides just another reason to think poorly of the defendant.

[14] *Club v. Sierra Club*, 505 F. Supp. 3d 982, 985 (N.D. Cal. 2020).

[15] *United States v. Trader*, 981 F.3d 961, 966 (11th Cir. 2020).

6 Analysis

The empirical findings reveal disconnects between the academic framings of doxxing and how courts encounter this concept in practice. While legal scholarship has focused primarily on doxxing as a First Amendment problem requiring careful balancing between free speech and cyber civil rights concerns, this analysis demonstrates that First Amendment challenges represent only one frame where courts grapple with doxxing. This framing has obscured other important ways that legal institutions construct and regulate doxxing. The diverse contexts in which doxxing surfaces in judicial opinions, extend beyond a single cause of action or stage of litigation. This underscores the need for scholars and policymakers to adopt a broader lens when examining the range of legal responses to doxxing.

6.1 Internet Personal Jurisdiction Revisited

Personal jurisdiction determines whether a court has the authority to require a defendant to appear in court and be bound by the court's judgment. As introduced above, courts use a 'minimum contacts' test rooted in due process to determine whether they can hear cases involving out-of-state defendants. This doctrine has proved a barrier to address the geographically agnostic nature of of doxxing harms.

Personal jurisdiction doctrine presents a significant structural barrier to legal remedies for doxxing victims in federal civil cases. Seventeen of the eighty-two cases involve minimum contacts analysis. The different outcomes in *Vangheluwe v. Got News* and *Blessing v. Chandrasekhar* illustrates this breakdown. In both cases, out-of-state defendants engaged in similar behavior: publishing names, addresses, and inciting the harassment of forum state residents, yet the courts reached different outcomes.

The law of personal jurisdiction has traditionally been closely linked to physical location and geographical boundaries, with jurisdiction often depending on the defendant's physical presence within a specific state. However, the internet has blurred these boundaries, creating scenarios where individuals can have substantial impact in jurisdictions without ever physically entering them. Courts have struggled to evaluate online activities, ranging from commerce to doxxing [32, 37] The Supreme Court has repeatedly declined addressing questions of when internet conduct constitutes sufficient contacts for personal jurisdiction.[16] This jurisdictional filtering operates as a form of institutional gatekeeping that systematically excludes certain doxxing victims from accessing civil legal remedies. The legal requirement that minimum contacts analysis focus exclusively on defendant-forum relationships, rather than harm to forum residents, is particularly vexatious for doxxing cases. Unlike traditional tort scenarios where defendant conduct and victim harm occur in the same physical space, doxxing enables remote actors to cause localized harm without establishing the purposeful forum contacts that personal jurisdiction doctrine requires. The geographical mismatch becomes more problematic when considering that doxxing harms often manifest precisely through local third-party responses: harassment at work, threats from community members, or physical stalking near the victim's residence. Yet courts cannot consider these forum-centered harms when evaluating whether non-resident doxxers have insufficient contacts with the jurisdiction. The outcome is a regulatory gap where the most harmful forms of doxxing may be the least accessible to legal intervention.

Courts should approach the question of personal jurisdiction in doxxing cases not by drawing bright-line rules based on the specific types of information disclosed, but rather by adapting the standard laid out in *Vangheluwe*. This standard asks whether doxxing was intended to cause some action in the forum state or was intended to target citizens of the forum state. If either of these criteria is satisfied, it should weigh strongly in favor of finding personal jurisdiction. This

[16] *Ford Motor Co. v. Montana Eighth Judicial Dist.*, 592 US 351 (2021),

approach aligns with the perspective of doxxing scholars who do not differentiate between the types of information disclosed when assessing the magnitude of harm caused by doxxing [1, 4, 8]. By focusing on the intent and impact of the doxxing rather than the specific nature of the information disclosed, courts can develop a more comprehensive and equitable framework for addressing personal jurisdiction in these cases.

The proposed *Vangheluwe* standard offers advantages over current approaches. First, it recognizes that doxxing's harm stems not from the sensitivity of disclosed information, but from location-agnostic ability to mobilize third-party harassment within specific geographic communities. An employment address disclosed to encourage workplace harassment, or a home address shared to facilitate local stalking, both satisfy the forum-targeting criterion regardless of whether such information appears in public directories elsewhere. Second, this standard captures the deliberately targeted nature of most doxxing campaigns, which typically aim to leverage local social networks, employers, or community members to inflict reputational and social harm. Third, while a somewhat flexible standard, looking at the intent to geographically target individuals is still workable and allows for consistent outcomes. By adopting this approach, courts would better fulfill personal jurisdiction's fundamental purpose of ensuring defendants can reasonably anticipate being brought into court, while preserving due process protections against unforeseeable forum contacts.

6.2 Doxxing as a Litigation Risk

Courts' exploration of doxxing as a risk resulting from legal action reveals how legal institutions construct assess risk and construct models that determine what creates it and who warrants protection. This empirical analysis demonstrates that courts are increasingly asked to consider the risk of doxxing before it has occurred rather than evaluating whether a particular instance of doxxing should be punished after the fact. When doxxing is evaluated as an ex ante risk of litigation, courts weigh the privacy interests of litigants against the principle of judicial openness. The privacy interest is formulated as the risk of harm to litigants due to the unauthorized disclosure of their personal information. Courts find it most persuasive when litigants cite examples of past doxxing of similarly positioned individuals or entities, with potential physical danger being the most frequently cited harm \cite{volokh2022law}.

These cases demonstrate that courts often accept doxxing risk arguments when made by law enforcement officers while sometimes requiring more evidence when other litigants raise similar concerns. This pattern extends beyond judicial opinions to state anti-doxxing legislation, where five of fourteen states provide enhanced protection specifically for law enforcement. However, in the sample, courts were sympathetic to privacy concerns in college sexual assault cases, granting pseudonym use and sealed proceedings based on arguments about reputational harm and the sensitive nature of sexual misconduct allegations.

In general, the approach to risk assessment reflects broader institutional assumptions about whose safety concerns deserve legal protection. The prominence of law enforcement protection in both statutes and judicial opinions suggests that doxxing regulation has failed to been shaped by empirical assessment of who is at risk from doxxing. While scholarship often focuses on doxxing as a gendered phenomenon and a form of harassment against women, there is little discussion or understanding of doxxing as a gendered form of abuse in the law. A quantitative analysis of pseudonym success rates across different litigant categories would provide valuable empirical evidence for understanding how these hierarchies of protection operate in practice.

This analytical gap reflects broader problems with how legal institutions understand online harassment. Courts often approach doxxing through individualized harm frameworks that obscure its function as a mechanism for enforcing social hierarchies and excluding marginalized voices from public discourse. When judicial analysis ignores the systematic targeting of women and minorities, it fails to capture how doxxing operates as both individual harm and collective silencing mechanism.

6.3 Anti-SLAPP Laws as a Helpful Tool

Anti-SLAPP laws (Strategic Lawsuits Against Public Participation) are designed to protect defendants from frivolous lawsuits intended to chill speech. If successful, anti-SLAPP motions not only dismiss the lawsuit but also require the plaintiff to pay the defendant's attorney fees. A core part of the legal standard for dismissing cases under anti-SLAPP laws is establishing that the speech, in this case doxxing, touched on a matter of public interest or social importance [28].

Nine cases in the corpus involve anti-SLAPP motions, representing a significant proportion of the First Amendment challenges to doxxing claims. The cases typically involved claims by local officials (e.g., school boards) that they had been doxxed by constituents. The doxxing at issue commonly involved the sharing of phone numbers and contact information for the local representatives. The majority of these cases were dismissed at an early procedural stage on anti-SLAPP grounds. This pattern reveals that anti-SLAPP laws may be a partial solution to resolving the tensions a tension between protecting legitimate speech about matters of public concern and preventing the weaponization of doxxing regulation against grassroots organizing or accountability.

We argue that that states that pair anti-doxxing legislation with robust anti-SLAPP protections will be better positioned to protect both doxxing victims and legitimate speech about public affairs. This suggests that effective doxxing regulation requires careful attention to how these laws interact with broader speech protection frameworks, rather than treating doxxing as an isolated regulatory problem.

6.4 Inconsistencies in State Legislative and Judicial Responses

State anti-doxxing laws vary dramatically in coverage, penalties, and enforcement mechanisms, creating a patchwork of protection that depends more on the location of the person being doxxed than principled policy differences. Meanwhile, federal courts encounter doxxing primarily through procedural challenges rather than substantive legal questions, limiting their ability to develop coherent doctrinal approaches.

Within the diverse set of cases that discuss doxxing, claims under state anti-doxxing laws are sparse, with only two of the eighty-two cases in the dataset involving such laws. This scarcity could be attributed to either the corpus not capturing the full extent of anti-doxxing litigation or the rarity of cases being brought under anti-doxxing laws. There is reason to believe there is more litigation using anti-doxxing laws than is revealed in this corpus of judicial opinions. State trial courts do not publish opinions due to the large volume of cases on their docket and the non-binding nature of state trial court opinions for precedent. Consequently, cases involving anti-doxxing laws would only surface in this search if they were brought up on appeal or if federal courts applied state law.

The cases where doxxing is the central cause of action are predominantly civil in nature, such as defamation or other speech torts, rather than criminal. This stands in contrast to the state anti-doxxing laws, where twelve out of fourteen have criminal penalties. The discrepancy highlights a gap between how state legislators, as an institution, are conceptualizing the appropriate remedies for doxxing (primarily as misdemeanors) and how claims related to doxxing (mostly as civil matters) are structured. This difference may suggest that prosecutors may not be bringing certain kinds of criminal claims related to doxxing, despite the existence of criminal anti-doxxing laws.

7 Conclusion

This paper examines how courts conceptualize and contest doxxing, a sociotechnical harm, revealing significant disconnects between academic framings of online harassment and how legal institutions actually encounter and regulate this phenomenon. Through content analysis of eighty-two judicial opinions and fourteen state anti-doxxing statutes, this research demonstrates that doxxing emerges in legal discourse across multiple contexts that shape which harms become legally cognizable and which victims receive protection.

This paper contributes to broader understandings of sociotechnical governance by demonstrating how legal institutions actively shape the meaning and regulation of online harms rather than passively responding to technological developments [16]. The four legal contexts where courts encounter doxxing: First Amendment challenges, personal jurisdiction disputes, judicial transparency questions, and evidence of harassment patterns, reveals the posture of litigation may matter more than substantive legal issues in determining outcomes for doxxing victims. The analysis suggests that effective doxxing regulation requires attention to how different regulatory modalities interact rather than treating legal responses as isolated interventions. States that pair anti-doxxing legislation with robust anti-SLAPP protections may be better positioned to protect both harassment victims and legitimate speech about matters of political concern. Similarly, courts that adopt the approach outlined in *Vangheluwe*: focusing on whether doxxing was intended to cause action in the forum state rather than bright-line rules about information categories, can develop more equitable frameworks for evaluating personal jurisdiction in online harassment cases.

References

[1] Briony Anderson and Mark A Wood. 2022. Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing. *International Journal for Crime, Justice and Social Democracy* 11, 1 (2022), 196–209.

[2] Haig A. Bosmajian. 1992. *Metaphor and Reason in Judicial Opinions.* SIU Press.

[3] Danielle Keats Citron. 2014. *Hate Crimes in Cyberspace.* Harvard University Press.

[4] Danielle Keats Citron and Daniel J Solove. 2022. Privacy harms. *BUL Rev.* 102 (2022), 793.

[5] Julie E Cohen. 2019. *Between truth and power.* Oxford University Press.

[6] David Cremins. 2024. Defending the Public Quad: Doxxing, Campus Speech Policies, and the First Amendment. *Stanford Law Review* 76 (2024), 1813.

[7] Katherine Cross. 2019. Toward a formal sociology of online harassment. *Human Technology* 15, 3 (2019), 326–346.

[8] David M. Douglas. 2016. Doxing: a conceptual analysis. *Ethics and Information Technology* 18, 3 (2016), 199–210.

[9] Stine Eckert and Jade Metzger-Riftkin. 2020. Doxxing. In *The International Encyclopedia of Gender, Media, and Communication*, Karen Ross, Ingrid Bachmann, Valentina Cardo, Sujata Moorti, and Marco Scarcelli (Eds.). Wiley, 1–5.

[10] Tarleton Gillespie. 2018. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.

[11] Mark A Hall and Ronald F Wright. 2008. Systematic content analysis of judicial opinions. *Calif. L. Rev.* 96 (2008), 63.

[12] Mat Honan. 2014. What Is Doxing? Wired.

[13] Laura Huey, Lorna Ferguson, and Zachary Towns. 2025. "Cops Need Doxxed": Releasing Personal Information of Police Officers as a Tool of Political Harassment. *Crime & Delinquency* 71, 3 (2025), 714–739.

[14] Jane Im, Sarita Schoenebeck, Marilyn Iriarte, Gabriel Grill, Daricia Wilkinson, Amna Batool, Rahaf Alharbi, Audrey Funwie, Tergel Gankhuu, Eric Gilbert, and Mustafa Naseem. 2022. Women's Perspectives on Harm and Justice after Online Harassment. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (2022), 355:1–355:23.

[15] Sarah Jeong. 2015. Stop Diluting the Definition of "Dox". https://sarahjeong.net/2015/07/08/stop-diluting-the-definition-of-dox/ Blog post.

[16] Margot E Kaminski and Meg Leta Jones. 2023. Constructing AI speech. *Yale LJF* 133 (2023), 1212.

[17] Beth Kolko, Lisa Nakamura, and Gilbert Rodman. 2013. *Race in cyberspace.* Routledge.

[18] Klaus Krippendorff. 2018. *Content analysis: An introduction to its methodology.* Sage publications.

[19] Genevieve Lakier. 2014. The Invention of Low-Value Speech. *Harvard Law Review* 128, 8 (2014), 2166–2233.

[20] Frank D LoMonte and Paola Fiku. 2022. Thinking Outside the Dox: The First Amendment and the Right to Disclose Personal Information. *UMKC L. Rev.* 91 (2022), 1.

[21] Benjamin Loveluck. 2020. The many shades of digital vigilantism. A typology of online self-justice. *Global Crime* 21, 3-4 (2020), 213–241.

[22] Julia M. MacAllister. 2016. The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information. *Fordham Law Review* 85 (2016), 2451.

[23] Victoria McIntyre. 2016. "Do (x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent. *Tul. J. Tech. & Intell. Prop.* 19 (2016), 111.

[24] Anna Merlan. 2015. The Cops Don't Care About Violent Online Threats. What Do We Do Now?

[25] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[26] Jessica A. Pater, Moon K. Kim, Elizabeth D. Mynatt, and Casey Fiesler. 2016. Characterizations of Online Harassment: Comparing Policies Across Social Media Platforms. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work*. Association for Computing Machinery, 369–374.

[27] Kathleen Perricone. 2013. UPDATED: Kim Kardashian, Beyonce, Ashton Kutcher Among Those Targeted in 'Doxxing' Hacker Scheme. *Yahoo News* (2013).

[28] George William Pring and Penelope Canan. 1996. *SLAPPs: Getting sued for speaking out.* Temple University Press.

[29] Frederick Schauer. 1978. Fear, Risk and the First Amendment: Unraveling the Chilling Effect. *Boston University Law Review* 58, 5 (1978), 685–732.

[30] Hannah Shankman. 2022. How to Close Pandora's Dox: A Case for the Federal Regulation of Doxing. *University of Florida Journal of Law and Public Policy* 33 (2022), 273.

[31] Rodney A Smolla. 2019. The meaning of the "marketplace of ideas" in First Amendment Law. *Communication Law and Policy* 24, 4 (2019), 437–475.

[32] Alan M. Trammell and Derek E. Bambauer. 2014. Personal Jurisdiction and the Interwebs. *Cornell Law Review* 100, 5 (2014), 1129–1190.

[33] Daniel Trottier. 2017. Digital vigilantism as weaponisation of visibility. *Philosophy & Technology* 30 (2017), 55–72.

[34] Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. 2017. Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Association for Computing Machinery, 1231–1245.

[35] R George Wright. 1987. Speech on Matters of Public Interest and Concern. *DePaul L. Rev.* 37 (1987), 27.

[36] Brianna Wu. 2015. Doxxed: Impact of online threats on women including private details being exposed and "swatting". *Index on Censorship* 44, 3 (2015), 46–49.

[37] Gretchen Yelmini. 2023. Internet Jurisdiction and the 21st Century: Zippo, Calder, and the Metaverse. *Connecticut Law Review Online* 55 (2023), 1–28.

Table 1. State Anti-Doxxing Laws: Legal Framework and Penalties

State	Type	Covered Individuals/Roles	Information Scope	Intent Requirement	Penalties
AZ	Criminal	General (anyone OR anyone through their family)	PII (home/work address, phone, email, contact info, images of person)	Without consent and for purpose of imminently causing unwanted physical contact/injury/harassment	Misdemeanor
AR	Criminal	Minors only	PII with an emphasis on social media	Purpose to frighten, coerce, intimidate, threaten, abuse, or harass	Misdemeanor - Felony
CA	Criminal	General	PII, images, and messages of harassing nature	Intent to place in reasonable fear AND for purpose of imminently causing unwanted physical contact/injury/harassment	Misdemeanor
CO	Criminal	Educators, health workers, human services, judges, peace officers, public defenders/prosecutors	Home address, phone numbers, personal email, directions to home, photos of person/home/vehicle	Knowingly make available where disclosure poses imminent and serious threat	Misdemeanor
CT	Criminal	General	Name, SSN, DOB, address, phone, biometric, medical/education/financial records	For no legitimate purpose and with intent to harass, terrorize or alarm	Misdemeanor

Table 1. State Anti-Doxxing Laws: Legal Framework and Penalties (continued)

State	**Type**	**Covered Individuals/Roles**	**Information Scope**	**Intent Requirement**	**Penalties**
FL	Criminal	General	Personal identification information (cross-references other statutes)	Intent to incite violence/commit crime OR intent to threaten/harass	Misdemeanor
KY	Criminal	General	SSN, DOB, home address, email, phone, financial accounts, biometric/health data, school/employment	Intent to intimidate, abuse, threaten, harass, or frighten	Misdemeanor - Felony
MN	Criminal	Law enforcement OR their family	Home address, directions to home, photographs of home (limited scope)	Knowingly and without consent, where disclosure poses imminent and serious threat	Misdemeanor
MO	Criminal	Law enforcement, judges, prosecutors OR their family	Name, home address, SSN, phone, personally identifiable information	Intent to cause great bodily harm or death, or threatening to cause great bodily harm or death	Misdemeanor - Felony
NV	Civil	General	Personal identifying info + sensitive info (sexual orientation, gender transition, HIV status)	Intent to aid criminal activity OR intent to cause harm with reckless disregard	Damages; attorney fees, injunctive relief
OK	Criminal	Peace officer, public officials, medical providers, crime victims	PII (e.g., home/work address, SSN, phone, email, contact info)	Intent to threaten, intimidate or harass OR facilitate another to do so	Misdemeanor
OR	Civil	General	Home address, email, phone, SSN, employer contact, family contact, photos of children, children's schools	Intent to stalk, harass, or injure	Damages; attorney fees injunctive relief
UT	Criminal	General	PII	Intent to abuse, threaten, or disrupt electronic communication AND without permission	Misdemeanor
VA	Criminal	General + heightened penalties for law enforcement and judges	Name, photograph of person, home address or other PII	Intent to coerce/intimidate/harass	Misdemeanor - felony