THINKING OUTSIDE THE DOX: THE FIRST AMENDMENT AND THE RIGHT TO DISCLOSE PERSONAL INFORMATION

Frank D. LoMonte* and Paola Fiku**

I. INTRODUCTION

During a hard-fought 2021 mayoral race in New York City, an unanticipated issue fixated the attention of local journalists and threatened to derail the frontrunning campaign of Democrat Eric Adams: it wasn't clear that Adams actually *lived* in New York.[1]

Reporters used publicly available records to sleuth out indicators that Adams' primary residence was not, as he claimed, in the Bedford-Stuyvesant neighborhood of Brooklyn.[2] Rather, it appeared that Adams, a retired police officer, was living either in his municipal office as Brooklyn borough president or in an apartment he co-owned across the Hudson River in New Jersey.[3] Adams only invigorated the speculation with what one reporter described as a "surreal" tour of his putative Brooklyn home that, it seemed apparent, was primarily occupied by his twenty-five-year-old son.[4] The scrutiny intensified after Adams' tax records showed that he disclaimed living at the Brooklyn home for tax purposes and characterized the home as investment property—which, after reporters questioned the apparent inconsistency, Adams chalked up to an accountant's mistake.[5] Journalists' persistent questioning raised doubts not just about Adams' commitment to the city he was seeking to lead, but about his

* Professor & Director of the Joseph L. Brechner Center for Freedom of Information at the University of Florida in Gainesville, Fla. B.A., 1992, Political Science, Georgia State University; J.D. (Order of the Coif), 2000, University of Georgia School of Law.

** Law Clerk, Joseph L. Brechner Center for Freedom of Information. B.A., 2018, Political Science & Criminology, University of Florida; J.D., 2022 (anticipated), University of Florida Levin College of Law.

[1] Katie Glueck et al., *Where Does Eric Adams Live? Rivals Question His Residency and Ethics*, N.Y. TIMES, https://www.nytimes.com/2021/06/09/nyregion/eric-adams-maya-wiley-endorsement-jumaane.html (Sept. 23, 2021).

[2] *See* Sally Goldenberg & Joe Anuta, *Mayoral Candidate Eric Adams Lived in His Government Office During the Pandemic. He May Have Never Left*., POLITICO (June 9, 2021, 11:01 AM), https://www.politico.com/news/2021/06/09/eric-adams-government-office-home-492497; *see also* Elizabeth Kim & Gwynne Hogan, *Facing Questions About Where He Lives, Eric Adams Invites Reporters to Brooklyn Home*, GOTHAMIST (June 9, 2021), https://gothamist.com/news/where-does-eric-adams-live.

[3] Goldenberg & Anuta, *supra* note 2; Kim & Hogan, *supra* note 2.

[4] *See* Kim & Hogan, *supra* note 2.

[5] Greg B. Smith & Yoav Gonen, *Eric Adams' Townhouse Trouble: Tax Filing 'Mistake' and Blown-Off Buildings Inspector*, THE CITY (Sept. 19, 2021, 7:17 PM), https://www.thecity.nyc/2021/9/19/22683164/eric-adams-townhouse-trouble-tax-filing-buildings-inspector.

candor and trustworthiness[6]—though he ended up victorious in a July 2021 free-for-all primary anyway.[7]

As the controversy unfolded, journalists pulled information from a variety of publicly accessible sources—campaign disclosure reports, tax filings, citation notices—to document Adams' whereabouts. At times, news accounts included the addresses of Adams' properties and photos of the buildings or linked to public records containing that information.[8] The controversy may have been accurately described as surreal, but the reporting was standard Journalism 101: gather the records, then publish the records.

A disclosure that a leading candidate for a powerful elected office may have misled the electorate about his residency would be considered, by most, an example of investigative reporting in service of the public good. But *some* privacy advocates also might call it "doxing"—publicizing home address information gathered from little-read sources, which might enable angry people to locate and harass the homeowner.

As the Adams experience demonstrates, there are times when personal information about prominent people becomes a matter of intense public concern. The First Amendment has long been understood to secure the freedom to publish information of public interest—even highly sensitive and unflattering information that has been kept secret.[9] But the reach and durability of online publishing, and particularly the nearly non-existent barriers to entry provided by social media platforms, is causing policymakers to rethink some First Amendment absolutes.[10] Among these is the legally protected right to reveal information about public figures without fear of being prosecuted.

---

[6] Glueck et al., *supra* note 1.

[7] Karen Matthews, *Eric Adams Wins Democratic Primary in NYC's Mayoral Race*, ASSOCIATED PRESS (July 6, 2021), https://apnews.com/article/eric-adams-wins-nyc-democratic-mayoral-primary-9c564828a29831747f9c2e6f52daf55e.

[8] *See, e.g.*, Yoav Gonen & Greg B. Smith, *New Evidence Eric Adams Retained Brooklyn Co-op Long After He Says Gave It to His 'Good Friend'*, THE CITY (June 21, 2021, 3:55 AM), https://www.thecity.nyc/2021/6/21/22542834/eric-adams-kept-brooklyn-coop-long-after-alleged-gift-friend; *see also* Greg B. Smith & Yoav Gonen, *Eric Adams Failed to Disclose Co-Ownership of Brooklyn Co-op He Says He Gave Away to a Friend*, THE CITY (June 16, 2021, 4:00 AM), https://www.thecity.nyc/2021/6/16/22536241/eric-adams-failed-to-disclose-brooklyn-coop-ownership.

[9] *See* Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 104-06 (1979) (striking down indictment of two newspapers for violating a state statute forbidding publication of the name of any youth charged as a juvenile offender); *see also* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496-97 (1975) (finding that television stations cannot be held liable for civil damages for broadcasting name of a rape-murder victim that was lawfully obtained from courthouse records); *see also* Okla. Publ'g Co. v. Dist. Ct. for Okla. Cnty., 430 U.S. 308, 311-12 (1977) (invalidating pretrial order directing news media to refrain, under threat of sanction, from using name or image of 11-year-old charged in fatal shooting, where information was gathered as part of open court proceeding).

[10] *See* Adam Liptak, *Two Justices Say Supreme Court Should Reconsider Landmark Libel Decision*, N.Y. TIMES (July 2, 2021) (reporting that, in dissenting from the Supreme Court's refusal to grant certiorari in a 2021 defamation case, Justices Clarence Thomas and Neil Gorsuch suggested revisiting the Court's venerable *New York Times v. Sullivan*, 376 U.S. 254 (1964), which for decades has set a demanding standard for libel suits against the news media by public figures).

As of the end of 2021, seven states—Arizona, Colorado, Florida, Kentucky, Minnesota, Oklahoma, and Oregon—had enacted laws explicitly targeting the practice of "doxing,"[11] which lawmakers have generally defined as involuntarily disseminating home contact information about police officers and others with sensitive jobs who might be targets of vengeful people. In none of these states is there any significant evidence that lawmakers debated the First Amendment implications of making it a crime to publish lawfully obtained information about government employees. That debate is overdue. This Article attempts to provide cautionary guidance about both the constitutional risks and the practical trade-offs that policymakers should take into account before following the lead of the early adopters and creating a new "information crime" of doxing.

Part II explains how doxing entered the popular lexicon a decade ago and how its meaning has become so malleable that, on occasion, the term has been "defined down" to encompass routine acts of news reporting or political advocacy. Part III explores how courts have worked to reconcile two competing and deeply cherished American values—the right of a free press to disclose information, and the personal privacy of those who prefer to keep information about themselves confidential. It explains how courts have fashioned constitutional workarounds enabling legislators to criminalize, and prosecutors and judges to punish, threatening and harassing behavior even though some expression is incidentally curtailed. Part IV analyzes the first generation of doxing legislation, flagging in particular a newly enacted—but little-noticed—Florida statutory provision that treads especially close to the danger zone of criminalizing ordinary acts of newsgathering and commentary. It assesses those statutes against the handful of documented facial challenges to "doxing-like" statutes; every one of which has resulted in a finding of unconstitutionality. Finally, Part V suggests a cautious approach to creating additional criminal codes that might be weaponized to deter or punish discussion of issues of public concern. The authors conclude that existing statutes already provide a remedy for most harmful doxing behaviors, and that enacting broad additional remedies for speech that does *not* rise to the level of punishable threats or harassment would be constitutionally questionable, impracticable to effectively enforce, and likely to embolden retaliatory arrests of law enforcement critics.

II. DOXING DEFINED

A. No Consensus on a Meaning—or Even a Spelling

What we now know as "doxing" first emerged in the 1990s in the world of online hackers, in which people operated through anonymized screen names.[12] If a feud broke out among hackers, or a member of a hacking group was

---

[11] *See infra* Part IV (describing qualities of each anti-doxing statute).

[12] Natalia Homchick, Note, *Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries*, 76 WASH. & LEE L. REV. 1307, 1309 (2019).

perceived as having violated group norms, a squealer would "drop docs" on the perceived wrongdoer by exposing the person's true offline identity.[13] Eventually, "docs" became "dox," lost the "drop," and evolved as a verb, sometimes written with an extra "x" as "doxxing."

The understood meaning of doxing has since expanded beyond the world of hackers to include the weaponizing of any type of personal information.[14] Today's doxers reveal information such as home addresses, employers, criminal history, private correspondence, and other such details about their targets.[15] The motives behind doxing range from intimidating or humiliating victims, causing a loss of employment, breaking off relationships, or even making the target a victim of physical assault.[16] Some commentators have adopted such a broad understanding of what it means to "dox" that the definition—the mere act of publishing personally identifying information without consent, regardless of the publisher's intent—would encompass all manner of routine acts of news reporting or database stewardship.[17] Notably, the common understanding of doxing invariably refers to *online* publishing, suggesting that there is something especially invidious about sharing personal information in an online publication that is not true of other mediums.[18]

The public policy arguments in favor of taking steps to deter and/or punish doxing, especially when vulnerable private citizens are targeted, are obvious and appealing. As one commentator has argued, "Freedom of speech is undoubtedly a bedrock principle in our constitutional democracy; but it should not be interpreted in a way that protects speech that causes severe emotional harms, undermines equality, and decreases meaningful public discourse."[19] In

---

[13] *See* Anna Schaverien, *Colorado Makes Doxxing Public Health Workers Illegal*, N.Y. TIMES (May 19, 2021), https://www.nytimes.com/2021/05/19/us/colorado-doxxing-law.html ("The term doxxing comes from internet slang that hackers would use to describe collecting and posting private documents, or 'docs,' about an individual, usually a rival.").

[14] *See* Alexander J. Lindvall, *Political Hacktivism: Doxing & The First Amendment*, 53 CREIGHTON L. REV. 1, 2 (2019) ("Doxing is a form of cyber-harassment that involves the public release of personal information that can be used to identify or locate an individual, such as the person's home address, email address, phone number, or other contact information.") (internal quotes omitted).

[15] Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2453 (2017).

[16] *See* Andy Greenberg, *Anonymous Hackers Target Alleged WikiLeaker Bradley Manning's Jailers*, FORBES (Mar. 7, 2011, 6:34 AM), https://www.forbes.com/sites/andygreenberg/2011/03/07/anonymous-hackers-target-alleged-wikileaker-bradley-mannings-jailers/?sh=49c386927c0e.

[17] *See* Elizabeth Leonard, Comment, *Daniel v. Armslist: A "Bad Samaritan" Case Study*, 36 WIS. J.L. GENDER & SOC'Y 85, 108 (2021) ("Doxxing is the act of posting a person's real-world address or personal information without their permission."); Homchick, *supra* note 12, at 1308 (defining doxing as "the act of releasing personal information on the internet without consent"); Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting,* 70 FED. COMM'S L.J. 317, 318 (2018) ("Doxing is when someone's personal information is shared on the Internet without their consent . . . .").

[18] *See* Michal Buchhandler-Raphael, *Overcriminalizing Speech*, 36 CARDOZO L. REV. 1667, 1676 (2015) ("The overcriminalization of speech has been greatly exacerbated over the last two decades due to the unprecedented rise in the use of the Internet as the dominant form of communication.").

[19] Lindvall, *supra* note 14, at 3.

this view, protecting the act of doxing on free-speech grounds arguably results in a net *diminution* of speech because intimidation may cause speakers to mute what they say online or leave the forum entirely. Besides the intimidating effect of doxing, if the disclosures are sufficiently sensitive—such as Social Security number, date of birth, or bank account number—they may enable bad actors to commit fraud, identity theft, or other financial crimes.[20]

Mainstream media first picked up on the concept of doxing in 2011, in reference to the activities of a shadowy group of digital vigilantes (known simply as "Anonymous") that published information identifying the jailers guarding military leaker Chelsea (then known as Bradley) Manning.[21] In common contemporary usage, however, doxing is distinguishable from the work of hacker groups like Anonymous in that doxing does not generally depend on gaining unauthorized access to secured data (which is already illegal under a variety of computer fraud and abuse laws).[22] Rather, doxing typically relies on information gleaned from publicly accessible sources, making it, in the words of one commentator, "like hacking, but legal."[23]

In the popular lexicon, "doxing" has become a somewhat elastic term subject to selective and opportunistic use. A Seattle journalist covering protests against police violence complained that the head of the police union had engaged in "doxing" when he made a joke expressing his distaste for the media by posting a picture of the journalist's press pass on Twitter, even though the tweet merely showed the journalist's name, face, and media affiliation[24]—the same information routinely displayed on news organizations' own websites. The conservative commentary magazine, *National Review*, accused U.S. Representative Joaquin Castro, D-Tex., of "doxing" because he used Twitter to disseminate the names of donors who had given the legal maximum to Donald Trump's re-election campaign, which were gleaned from reports that campaigns are legally obligated to make public.[25] The commentator, a former Republican appointee to the Federal Elections Commission, claimed that Castro must have intended "to put a target on the backs of" Trump contributors.[26] Another conservative commentator accused Pulitzer Prize-winning journalist, Nikole Hannah-Jones, of "doxing" a blogger who contacted her seeking a quote for a

---

[20] *See* Homchick, *supra* note 12, at 1311-12 ("Doxing's harms include harassment, physical harm, and financial harm. Doxing victims are also at an increased risk of identity theft.").
[21] *See* Greenberg, *supra* note 16.
[22] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (making it a federal crime to gain unauthorized access to a computer system); Stored Communications Act, 18 U.S.C. § 2701 (making it a federal offense to gain unauthorized access to a cloud storage system or other repository of digital data).
[23] Samantha H. Scheller, *A Picture Is Worth a Thousand Words: The Legal Implications of Revenge Porn*, 93 N.C. L. REV. 551, 594 (2015).
[24] *See* Jonathan Choe, *Reporter's Lost Press Pass Spurs Complaints Against Seattle Police Union President,* KOMO NEWS (Sept. 10, 2020), https://komonews.com/news/local/reporters-lost-press-pass-linked-to-complaints-against-seattle-police-union-president.
[25] Bradley A. Smith, *Doxing Trump Donors Is Just the Beginning*, NAT'L REV. (Aug. 9, 2019, 12:46 PM), https://www.nationalreview.com/2019/08/doxxing-trump-donors-is-just-the-beginning/.
[26] *Id.*

column he was writing—even though the "dox" consisted entirely of republishing professional email correspondence in which the blogger's name, email address, and phone number could be seen.[27] "Doxing" has even been applied to describe the leak of then-President Trump's long-hidden personal income tax returns to *The New York Times* and to the shaming of racist police officers by the Black Lives Matter movement.[28]

A Cleveland newspaper's decision to expose potentially disqualifying information about the judge in a high-profile murder case has been characterized as "doxxing."[29] Reporters from *The Plain Dealer* decided to investigate the source of online comments that a *Plain Dealer* reader posted in response to news stories about a 2010 murder trial, which contained a level of detail suggesting the commenter had inside knowledge of the trial. By gaining access to the newspaper's (normally nonpublic) reader account data, the reporters traced the comments to the trial judge's personal email account.[30] The *Plain Dealer* article mentioned that the judge accessed the comment section of the online newspaper using a personal email address, but it did not disclose that address or any other information that would enable or encourage anyone to harm the judge.[31] More to the point, the article was widely considered to be a public service, as it raised questions about the judge's impartiality; one of the comments attributed to the judge's account was harshly critical of the defense attorney in the ongoing murder trial, resulting in her disqualification from the case.[32] While the newspaper might legitimately be criticized for making a questionable ethical choice, or even held to have breached its promise of anonymity to contributors using its website comment feature,[33] one would be hard-pressed to argue that reporting on unprofessional behavior by an elected judge should be a crime.

---

[27] C. Douglas Golden, Commentary, *'1619 Project' Creator Scrubs Twitter After Getting Blasted for Doxing Reporter*, W. J. (Feb. 10, 2021, 9:18 AM), https://www.westernjournal.com/1619-project-creator-scrubs-twitter-getting-blasted-doxing-reporter/.

[28] MacAllister, *supra* note 15, at 2460.

[29] Jasmine McNealy, *Readers React Negatively to Disclosure of Poster's Identity*, 38 NEWSPAPER RSCH. J. 282, 286-88 (2017).

[30] James F. McCarty, *Anonymous Online Comments Are Linked to the Personal E-mail Account of Cuyahoga County Common Pleas Judge Shirley Strickland Saffold*, CLEVELAND PLAIN DEALER, https://www.cleveland.com/metro/2010/03/post_258.html (Mar. 25, 2010, 12:00 PM).

[31] *Id.*

[32] In re Disqualification of Saffold, 981 N.E.2d 869, 871 (Ohio 2010).

[33] Henry J. Gomez, *Plain Dealer Sparks Ethical Debate by Unmasking Anonymous Cleveland.com Poster*, CLEVELAND.COM, https://www.cleveland.com/metro/2010/03/plain_dealer_sparks_ethical_de.html (Mar. 26, 2010, 12:00 PM) (quoting journalism ethics expert questioning decision to use access to commenter's email addresses for newsgathering purposes and citing other news company executives who say news reporters are walled off from knowing identities of comment authors). The judge and her daughter—who took responsibility for authoring at least some of the comments originating from the judge's internet account—sued the newspaper and its parent publishing company, alleging that they breached their promise to protect commenters' anonymity. Brennan McCord & Eamon McNiff, *Judge Saffold Files $50M Suit Against Cleveland Newspaper Over Online Comments*, ABC NEWS (Apr. 6, 2010, 7:46 PM), https://abcnews.go.com/TheLaw/cleveland-judge-denies-making-online-comments/story?id=10304420. The case concluded at the end of 2010 with an undisclosed

"Doxing" has even been applied to disclosures of mundane information about public officials. U.S. Senator John Cornyn, R-Tex., a former Texas Supreme Court justice and state attorney general, accused activists opposed to then-President Trump of committing the crime of "doxing" when they published lists of White House staffers in hopes that employers might hesitate to hire people associated with Trump.[34] However, the sum total of the information disclosed—name and employer—is nothing more than what would appear on a résumé or a LinkedIn profile. While there is no genuine indication that the anti-Trump activist group Lincoln Project came anywhere close to violating a criminal statute with its disclosures about Trump staffers, the fact that a highly accomplished attorney could insist that such a crime exists reflects how "doxing" has been distorted and weaponized in contemporary political discourse.

B. Is There Such a Thing as "Virtuous Doxing?"

If doxing is understood to mean disclosing personal information in a way that is intended to cause harm to befall the target, is it always categorically proscribable? Should it be? In one of the earliest references to "doxing" in academic literature, law professor, Lenese C. Herbert, spoke admiringly of the doxing skills of "Occupy Wall Street" protesters who used their hacking prowess to expose information about police officers they believed to be responsible for violating civil liberties.[35] So, the public has had a love-hate relationship with the concept of doxing, depending on whether the target appears to deserve public shaming.

Internet researcher danah boyd captured this fraught relationship in one of the earliest mainstream media explorations of doxing in her opinion article for *Wired*, in which she described how a journalist exposed the identity of a prolific author of hateful posts on the popular discussion site, Reddit.[36] Noting that "[m]any celebrated this public shaming, ecstatic to see a notorious troll grovel," boyd used the unmasking episode to illustrate how doxing can function as a tool to impose consequences on antisocial behavior within online communities—but also, how it can misfire and undeservedly harm people who are misidentified.[37]

---

settlement. *Saffolds Dismiss Lawsuit Against Plain Dealer, Settle with Advance Internet*, CLEVELAND PLAIN DEALER, https://www.cleveland.com/metro/2010/12/saffolds_dismiss_lawsuit_again.html (Dec. 31, 2010, 12:00 PM).

[34] *See* John Cornyn (@JohnCornyn), TWITTER (Jan. 13, 2021, 8:05 AM), https://twitter.com/JohnCornyn/status/1349357019015352320 ("Doxing is illegal. These guys better check with their lawyers unless they want to spend their windfall gains on criminal defense lawyers: The Lincoln Project, a well-funded political group, wants to make it easier to cancel Trump alumni.").

[35] Lenese C. Herbert, *O.P.P.: How "Occupy's" Race-Based Privilege May Improve Fourth Amendment Jurisprudence for All*, 35 SEATTLE U. L. REV. 727, 745 n.97 (2012).

[36] danah boyd, Opinion, *Truth, Lies, and 'Doxxing': The Real Moral of the Gawker/Reddit Story*, WIRED (Oct. 29, 2012, 6:30 AM), https://www.wired.com/2012/10/truth-lies-doxxing-internet-vigilanteism/.

[37] *Id.* This infamously happened in the case of University of Arkansas professor Kyle Quinn, who experienced hateful calls and messages after being misidentified as a participant in a white

Contemporary doxing has jumped the fence of the online world and become a method of holding people with noxious political views or behaviors accountable. For instance, after white nationalist torchbearers marched through Charlottesville, Virginia, in August 2017, culminating in the intentional hit-and-run killing of counter-protester Heather Heyer, online crusaders took to social media to identify the marchers and alert their schools and workplaces that they were harboring white supremacists.[38] More recently, amateur online sleuths worked alongside law enforcement to identify insurgents who ransacked the U.S. Capitol building on January 6, 2021, in an attempt to disrupt the certification of electoral votes formalizing Joe Biden's presidential victory.[39] Concerned citizens scrutinized social media images of the rioters to expose and publicize their identities, in hopes that those who participated in violence would be prosecuted, fired, or otherwise made to pay consequences.[40]

Journalists and activists have been applauded for exposing violent racists on police forces throughout the country, including revealing the real names behind anonymized accounts and the authors' workplaces.[41] Reporters from the blog *Injustice Watch* won a national ethics award for a 2019 article describing how researchers found hundreds of posts on Facebook accounts traceable to current or retired police officers, in which the officers used racial slurs or joked

---

supremacist march by way of a photo circulated on social media. Laura Sydell, *Kyle Quinn Hid at a Friend's House After Being Misidentified on Twitter as a Racist*, NAT'L PUB. RADIO (Aug. 17, 2017, 12:32 PM), https://www.npr.org/sections/alltechconsidered/2017/08/17/543980653/kyle-quinn-hid-at-a-friend-s-house-after-being-misidentified-on-twitter-as-a-rac.

[38] *See Charlottesville White Nationalist Marchers Face Backlash*, BRIT. BROAD. CO. (Aug. 14, 2017), https://www.bbc.com/news/world-us-canada-40922698 (reporting that demonstrators "are now facing an online backlash, as Twitter users identify and denounce them. Calls have been made to have them kicked out of universities and sacked from their jobs."); Patrick May, *How Berkeley Top Dog Employee at Charlottesville Rally Got Outed on Twitter*, MERCURY NEWS, https://www.mercurynews.com/2017/08/14/how-berkeley-top-dog-employee-at-charlottesville-rally-got-outed-on-twitter/ (Aug. 15, 2017, 2:29 PM) (describing how a Twitter user known by the screen name @YesYoureRacist circulated photos of Charlottesville protesters, leading Twitter followers to identify a California hotdog vendor whose employer promptly fired him).

[39] *See* Tim Mak, *The FBI Keeps Using Clues from Volunteer Sleuths to Find the Jan. 6 Capitol Rioters*, NAT'L PUB. RADIO (Aug. 18, 2021, 5:01 AM), https://www.npr.org/2021/08/18/1028527768/the-fbi-keeps-using-clues-from-volunteer-sleuths-to-find-the-jan-6-capitol-riote (reporting that "the FBI is relying on crowdsourced tips from an ad hoc community of amateur investigators sifting through that pile of content for clues" in the Jan. 6 attack).

[40] *See* Sara Murray, *Meet the Internet Sleuths Tracking Down the January 6 Insurrectionists*, CABLE NEWS NETWORK (June 11, 2021, 7:37 PM), https://www.cnn.com/2021/06/11/politics/internet-sleuths-january-6-insurrectionists/index.html.

[41] *See, e.g.*, A.C. Thompson, *Inside the Secret Border Patrol Facebook Group Where Agents Joke About Migrant Deaths and Post Sexist Memes*, PROPUBLICA (July 1, 2019, 10:55 AM), https://www.propublica.org/article/secret-border-patrol-facebook-group-agents-joke-about-migrant-deaths-post-sexist-memes (reporting that some 9,500 people, many of them current or former federal law enforcement agents, belonged to a private Facebook group where racist and misogynistic comments, including jokes about doing violence to immigrants crossing the border, were regularly shared). At least four agents were fired for sharing offensive posts to the group. Molly O'Toole, *Border Agency Fires 4 for Secret Facebook Groups with Violent, Bigoted Posts*, L.A. TIMES (July 16, 2020, 3:35 PM), https://www.latimes.com/politics/story/2020-07-16/border-patrol-fired-for-secret-facebook-group-with-violent-sexist-posts.

about brutalizing arrestees or protesters.[42] In Minnesota, a police watchdog blew the whistle on a Facebook comment author who used a pseudonymous account to encourage motorists to run down Black Lives Matter protesters—and turned out to be a St. Paul police officer.[43] After activists discovered that the same author had been posting insulting messages about Black activists in other Facebook groups, the officer agreed to resign.[44]

A mini-genre of online activism exists to amplify offensive social media posts in hopes that their authors will lose their jobs or suffer other adverse consequences.[45] The advocacy goes well beyond the police and others with sensitive public service jobs, and even extends to the youngest social media users.[46] Actress Skai Jackson has been widely lauded for her online crusading to identify and expose people, including other teenagers, who use racially offensive language on social media platforms, such as Twitter and Instagram, leading some of them to incur school discipline or the loss of college admission.[47] When then-President Barack Obama was re-elected in 2012, reporters with a celebrity news blog combed Twitter for posts by teenagers using racial slurs in reference to the President and then contacted their schools in hopes of seeing the students punished.[48]

Professor Hadar Aviram coined the term "progressive punitivism" to refer to the political left's selective enthusiasm for public humiliation and criminalization only when distasteful people are on the receiving end.[49] Aviram

---

[42] *See* Emily Hoerner & Rick Tulsky, *Cops Across the US Have Been Exposed Posting Racist and Violent Things on Facebook. Here's the Proof.*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/emilyhoerner/police-facebook-racist-violent-posts-comments-philadelphia (July 23, 2019, 3:32 PM).

[43] Mara H. Gottfried, *St. Paul Police Officer Who Posted 'Run Them Over' Resigns*, PIONEER PRESS, https://www.twincities.com/2016/02/17/st-paul-police-run-them-over-black-lives-matter-resigns/ (Feb. 28, 2016, 12:16 PM).

[44] Mara H. Gottfried, *St. Paul Cop's 'Run Them Over' Post Not His First, Activists Say*, PIONEER PRESS, https://www.twincities.com/2016/01/22/st-paul-cops-run-them-over-post-not-his-first-activists-say/ (June 28, 2016, 8:26 AM).

[45] *See* Soraya Nadia McDonald, *'Racists Getting Fired' Exposes Weaknesses of Internet Vigilantism, No Matter How Well-Intentione*d, WASH. POST (Dec. 2, 2014, 5:30 AM), https://www.washingtonpost.com/news/morning-mix/wp/2014/12/02/racists-getting-fired-exposes-weaknesses-of-internet-vigilantism-no-matter-how-well-intentioned/ (describing how "Racists Getting Fired" blog "adds consequences" to offensive online speech by recruiting volunteers to lodge complaints with the workplaces of people who post racist remarks on social media).

[46] *See* Taylor Lorenz & Katherine Rosman, *High School Students and Alumni Are Using Social Media to Expose Racism*, N.Y. TIMES (June 16, 2020), https://www.nytimes.com/2020/06/16/style/blm-accounts-social-media-high-school.html (explaining that, during a period of nationwide outrage and protest over excessive use of deadly police force against Black people, "high school students have leveraged every social media platform to call out their peers for racist behavior").

[47] De Elizabeth, *Skai Jackson Is Using Her Twitter to Expose Racist Behavior*, TEEN VOGUE (June 6, 2020), https://www.teenvogue.com/story/skai-jackson-twitter-expose-racist-behavior.

[48] Tracie Egan Morrissey, *Racist Teens Forced to Answer for Tweets About the 'Nigger' President*, JEZEBEL (Nov. 9, 2012, 12:30 PM), https://jezebel.com/racist-teens-forced-to-answer-for-tweets-about-the-nigg-5958993.

[49] *See* Hadar Aviram, *Progressive Punitivism: Notes on the Use of Punitive Social Control to Advance Social Justice Ends*, 68 BUFF. L. REV. 199, 204 (2020) ("Progressive punitive initiatives seek to

questions the ends-justifies-the-means rationalizations of those who, in their zeal for social justice, adopt the tactics of the carceral state against which they would otherwise be disposed to rebel.[50]

The Anti-Defamation League (ADL), one of the nation's most respected human rights organizations, has a complicated relationship with the concept of doxing. The ADL has called for legislation to outlaw the release of information with intent to cause harassment, while also supporting the unmasking of white supremacists and other wrongdoers. In a blog post setting forth its position, the ADL explained:

> [U]nlawful doxing is different from the work that activists and researchers—including those at ADL—are now engaging in to identify extremists and help law enforcement agencies investigate the rioters who violently stormed the Capitol. These activists and researchers are not operating with a criminal mental state. The same goes for journalists who break important stories, people who take on powerful institutions and interests by disclosing information (for example about the source of political donations), and people who report abuses of power or otherwise act as whistleblowers.[51]

In short, if "doxing" is understood to mean circulating personally identifiable information online in anticipation of inflicting injury on the targeted individual—humiliation, loss of employment, severe emotional distress—then doxing subsumes quite a bit of conduct that contemporary society regards as holding wrongdoers accountable. The question, then, becomes whether the legal system is equipped to distinguish between "good doxing" and "bad doxing" in a way that clearly protects societally beneficial disclosures.

III. THE "RIGHT TO DOX?"

A. When Free Speech and Personal Privacy Collide

For decades, bedrock First Amendment principles have protected the right to publish lawfully obtained information about matters of public concern, even when those who are the subject of the publication find the disclosures highly unwelcome. The government, including the judiciary, may neither enjoin the publication of news, nor impose after-the-fact punitive consequences absent

---

identify the powerful people who have long been served by the oppressive legal apparatus, and subject them to formal or informal social control . . . .").

[50] *See id.* at 213-14 (stating that "shaming, punitivism, and online endangerment raise particular difficulties when employed by a political constituency invested in criminal justice reform"); *see also id.* at 245 (remarking that "it is important to bring . . . nonpunitive perspectives into public discourse and encourage progressive activists, as well as progressive voters, to expand their imagination beyond punishment").

[51] *Doxing Should Be Illegal. Reporting Extremists Should Not.*, ANTI-DEFAMATION LEAGUE (Jan. 15, 2021), https://www.adl.org/blog/doxing-should-be-illegal-reporting-extremists-should-not.

extraordinary circumstances.[52] Any statute making it a punishable offense to publish information based on its content will be viewed skeptically and will be found unconstitutional unless it is the least restrictive means to achieve a compelling government objective and is narrowly tailored to penalize no more speech than necessary to accomplish that objective.[53] Courts particularly disfavor overly broad statutory prohibitions and will invalidate a speech-restrictive statute if it sweeps in substantially more speech than can legitimately be proscribed.[54] Because criminalizing speech runs the risk of inhibiting speakers into silencing themselves (referred to as the "chilling effect"), federal courts have relaxed ordinary principles of standing to make it easier to challenge speech-punitive statutes.[55]

Time and again, journalists have prevailed when facing either civil or criminal consequences for publishing lawfully obtained information that pertains to matters of public concern, regardless of whether the information is highly intimate or embarrassing. The Supreme Court has even found that news organizations have a constitutionally protected right to publish a rape victim's full name,[56] or the name of a child charged with a serious crime,[57] if those disclosures are newsworthy. The right to publish newsworthy information is so deeply ingrained in First Amendment jurisprudence that it even extends to material that a journalist's source committed a crime to obtain, so long as the journalist was not a participant.[58]

---

[52] *See* Near v. Minnesota, 283 U.S. 697, 716 (1931) (asserting that "liberty of the press, historically considered and taken up by the Federal Constitution, has meant, principally although not exclusively, immunity from previous restraints or censorship").

[53] Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

[54] *See, e.g.*, United States v. Miselis, 972 F.3d 518, 530 (4th Cir. 2020) (explaining that a prohibition on speech will be held overbroad even if it could constitutionally be applied in some situations, if "a substantial number of its applications" are invalid as compared with the universe of speech that can constitutionally be proscribed); Commonwealth v. Ashcraft, 691 S.W.2d 229, 232 (Ky. Ct. App. 1985) ("A challenge to a statute on the basis that it is overbroad is essentially an argument that in an effort to control impermissible conduct, the statute also prohibits conduct which is constitutionally permissible.").

[55] *See* Gooding v. Wilson, 405 U.S. 518, 521 (1972) (stating that a broader concept of standing to challenge speech-punitive statutes "is deemed necessary because persons whose expression is constitutionally protected may well refrain from exercising their rights for fear of criminal sanctions provided by a statute susceptible of application to protected expression").

[56] *See* Fla. Star v. B.J.F., 491 U.S. 524 (1989) (invalidating civil judgment against newspaper that printed unredacted police report about rape case, under Florida statute that outlawed publishing the name of a sex crime victim); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (finding that the First Amendment would not permit imposing civil damages on news organization that aired name of murdered rape victim, which was discussed openly in court).

[57] *See* Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979) (finding that news organization could not constitutionally be prosecuted for disclosing name of 14-year-old indicted in the shooting death of a classmate obtained from court records); Okla. Publ'g Co. v. Dist. Ct. for Okla. Cnty., 430 U.S. 308 (1977) (vacating trial court's order that forbade journalists from using name and photo of 11-year-old charged in shooting death, which were gathered from open court proceedings).

[58] *See* Bartnicki v. Vopper, 532 U.S. 514 (2001) (holding that radio news host had a First Amendment right to publish the contents of an illegally intercepted phone conversation furnished by a source that contained newsworthy information about a labor dispute); N.Y. Times Co. v. United States, 403 U.S.

Although the right appears nowhere explicitly within the Constitution, federal courts widely recognize a right to personal privacy that encompasses "informational privacy"—that is, the right to control when, where, and how one's personal information is disclosed.[59] But constitutional rights are enforceable almost exclusively against government agencies and employees.[60] Only in rare instances have courts found that a constitutional claim could lie against a private entity, such as when a news media organization works hand-in-glove with law enforcement agents in jointly raiding a home.[61]

The right to publish news regularly collides with the privacy interests of those targeted for coverage. But the universally recognized remedy for news coverage that discloses private confidences of no legitimate public interest is an award of civil damages—not, as doxing statutes typically contemplate, prosecution and prison.

The tort of "public disclosure of private facts" is deeply rooted in U.S. common law.[62] To prevail on a claim of public disclosure, a plaintiff typically must establish that the defendant revealed personally identifiable information about the plaintiff, of the type that "would be highly offensive to a reasonable person," in which the public has no legitimate interest.[63] Because the plaintiff has

---

713 (1971) (finding that courts could not enjoin newspapers from publishing leaked classified documents purloined by a Pentagon insider, even though the leaker acted unlawfully in removing the documents from his workplace and sharing them).

[59] As Harvard law professor Charles Fried wrote in an oft-cited 1968 article for the *Yale Law Journal*, "Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves." Charles Fried, *Privacy*, 77 YALE L. J. 475, 482 (1968). While the right is rooted in common law, several states have memorialized the right in their constitutions, either explicitly (as in Hawaii) or by judicial inference from a more generalized guarantee of individual liberties (as in Pennsylvania). *See* HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."); Reese v. Pennsylvanians for Union Reform, 173 A.3d 1143, 1159 (Pa. 2017) (stating that Art. 1, § 6 of the Pennsylvania constitution—"Inherent rights of mankind"—has been interpreted to confer a right of informational privacy, "[T]he citizens of this Commonwealth . . . have a right to informational privacy, namely the right of an individual to control access to, and dissemination of, personal information about himself or herself.").

[60] *See* Single Moms, Inc. v. Mont. Power Co., 331 F.3d 743, 746-47 (9th Cir. 2003) ("The United States Constitution protects individual rights only from *government* action, not from *private* action. Only when the *government* is responsible for a plaintiff's complaints are individual constitutional rights implicated.").

[61] *See* Berger v. Hanlon, 129 F.3d 505, 514-15 (9th Cir. 1997) (holding that CNN could be liable alongside government agents for taking part in an intrusive "ride-along" raid that violated the subjects' Fourth Amendment rights), *later proceeding at* 188 F.3d 1155 (9th Cir. 1999).

[62] *See* John A. Jurata, Jr., Comment, *The Tort That Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts*, 36 SAN DIEGO L. REV. 489, 492-93 (1999) (tracing widespread recognition of the tort claim to an influential 1890 law review article by Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis, in which they decried the proliferation of gossip about socialites in the news publications of the day).

[63] RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977) ("Publicity Given to Private Life" characterizes the requisite elements to sustain a claim as follows, "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person,

the burden to establish the absence of a legitimate public interest in the information, the law has come to recognize a greater measure of safety for publishers to disclose secrets about prominent people, or people who have become newsworthy as a result of involvement in a public controversy.[64]

Successful claims generally involve the disclosure of highly intimate secrets, such as a medical condition or procedure that has been kept confidential[65]—not, as doxing statutes encompass, one's address, telephone number, or other contact information. Home addresses and telephone numbers have appeared in publicly circulated directories for nearly a century-and-a-half; indeed, telephone directories are almost as old as the telephone itself.[66] Until laws began changing in 2010, it was not just a universal business practice throughout the United States but also a requirement of state telecommunications regulations for carriers to deliver directories door-to-door showing the name, address, and phone number of each customer in the community.[67]

It is widely recognized that information that journalists obtain in connection with government proceedings is not "private" so as to give rise to liability for its disclosure, no matter how sensitive the information. As one appellate court stated in dismissing tort claims against news reporters for disclosing the name of a sex-crime victim who testified at a sentencing hearing in a high-profile court case, "[W]e cannot understand how the voluntary disclosure of information in an unrestricted, open courtroom setting could be anything but a matter of public interest."[68]

To the extent that invasion of privacy has been criminalized in U.S. law, criminalization has been limited to the intrusive gathering of information, such as

---

and (b) is not of legitimate concern to the public."); *see also* Shulman v. Group W Prods., Inc., 955 P.2d 469, 474 (Cal. 1998) ("The sense of an ever-increasing pressure on personal privacy notwithstanding, it has long been apparent that the desire for privacy must at many points give way before our right to know, and the news media's right to investigate and relate, facts about the events and individuals of our time.").

[64] *See* Curtis Publ'g Co. v. Butts, 388 U.S. 130, 155 (1967) (recognizing that First Amendment requires heightened standard for "public" plaintiff, such as a prominent college football coach, to plead and prove libel against a news publication).

[65] *See, e.g.*, Doe v. Mills, 536 N.W.2d 824 (Mich. Ct. App. 1995) (holding that clinic patients stated an actionable tort claim for public disclosure of private facts based on anti-abortion demonstrators displaying their names on protest signs, imploring them not to go through with terminating their pregnancies).

[66] *See* Philip Sutton, *A Look at "The Book": The Fall and Rise of the Telephone Directory*, N.Y. PUB. LIBR. (Dec. 14, 2010), https://www.nypl.org/blog/2010/12/14/look-book-city-directory (describing how the first known telephone directory was distributed to homes in New Haven, Connecticut, in 1878, which is just two years after Alexander Graham Bell was issued the first patent for telephone technology).

[67] *See* Joseph Stromberg, *The Infuriating Reason You Still Get a Phonebook Delivered Every Year*, VOX, https://www.vox.com/2014/8/21/6040585/phonebooks-yellow-pages-delivery (Dec. 17, 2014, 9:50 AM) (describing how Verizon began the erosion of the must-deliver trend in 2010 by asking regulators in Florida, New York, and Pennsylvania to make delivery optional).

[68] Doe 2 v. Associated Press, 331 F.3d 417, 421-22 (4th Cir. 2003).

by voyeuristic photography or electronically aided eavesdropping.[69] This criminalization can be rationalized constitutionally, since the penalty is arguably directed at the noncommunicative aspects of the offender's conduct (i.e., the act of intrusively capturing the private conversation on the recording device, not the act of publishing it). Even there, tensions exist. Attempts at criminalizing celebrity "paparazzi" photography, on the theory that the law can separate the aggressive behavioral aspects of the photographers from the expressive aspects of the photographs and punish only the former, are regularly opposed on First Amendment grounds.[70] The law is so protective of the ability to gather information that even prosecutions for taking nonconsensual "up-skirt" photos of women—a harmful act with no legitimate expressive purpose—have sometimes failed on constitutional grounds.[71]

The constitutionally protected right to gather and publish news is fortified by elaborate statutory schemes in all of the United States and its territories that entitle members of the public to examine, copy, and redistribute government records.[72] Transparency of government records is recognized as essential for the public to perform its civic oversight duties, to deter corruption and self-dealing by government officials, and to create a sense of confidence that government is functioning honestly.[73] While some of those freedom-of-

---

[69] *See* Christopher Brett Jaeger & Gregory D. Smith, *Computer and Electronic Snooping: Opportunities to Violate State and Federal Law*, 34 AM. J. TRIAL ADVOC. 473, 481 (2011) (observing that "[a]lmost every state has enacted statutes prohibiting wiretapping" and that statutes typically track the Federal Wiretap Act, 18 U.S.C. § 2511); H. Morley Swingle & Kevin M. Zoellner, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Toms*, 52 J. MO. BAR 345, 346 (1996) (describing evolution of "Peeping Tom" laws and stating that, as of a 1996 survey, "[seventeen] states specifically and unquestionably criminalize secret videotaping in all places where the victim has a reasonable expectation of privacy").

[70] *See, e.g.*, Raef v. App. Div. of Superior Ct., 193 Cal. Rptr. 3d 159 (Cal. Ct. App. 2015) (concluding that a statute providing enhanced penalties for traffic offenses when committed for the purpose of taking commercial photos did not violate the First Amendment).

[71] *See, e.g.*, *Ex parte* Thompson, 442 S.W.3d 325, 333, 337, 349-50 (Tex. Crim. App. 2014) (vacating conviction under since-superseded Texas statute criminalizing "Improper Photography and Visual Recording," because taking photos and videos is inherently expressive activity and statute was an unduly broad content-based restriction on expression).

[72] Michael Hoefges et al., *Privacy Rights Versus FOIA Disclosure Policy: The "Uses and Effects" Double Standard in Access to Personally-Identifiable Information in Government Records*, 12 WM. & MARY BILL RTS. J. 1, 2 (2003).

[73] State freedom-of-information statutes commonly begin with a statement of principle explaining the civic importance of transparency, such as this one from the Arkansas Freedom of Information Act: "It is vital in a democratic society that public business be performed in an open and public manner so that the electors shall be advised of the performance of public officials and of the decisions that are reached in public activity and in making public policy. Toward this end, this chapter is adopted, making it possible for them or their representatives to learn and to report fully the activities of their public officials." ARK. CODE ANN. § 25-19-102 (2022). *See also* Cowles Publ'g Co. v. State Patrol, 748 P.2d 597, 601 (Wash. 1988) (en banc) ("The basic purpose of the public disclosure act is to provide a mechanism by which the public can be assured that its public officials are honest and impartial in the conduct of their public offices."); Asbury Park Press v. Ocean Cnty. Prosecutor's Off., 864 A.2d 446, 458 (N.J. Super. Ct. Law Div. 2004) (explaining why New Jersey's Open Public Records Act is liberally construed in favor of access: "The salutary goal, simply put, is to maximize

information statutes provide that documents may be withheld, or partially redacted, based on the presence of personally identifiable information, courts typically are instructed to err on the side of disclosure[74] and to withhold otherwise-public documents only if there is a "clearly unwarranted invasion of personal privacy" outweighing the public's right to know.[75] One illustrative scenario in which public accountability and personal privacy recurrently come into tension is when a government agency pays a settlement to resolve a personal injury claim; journalists understandably want to know what the government has paid, and the parties understandably hesitate to see the payout publicized.[76] Courts overwhelmingly have found that the balance weighs in favor of disclosure because keeping watch over the way taxpayer dollars are spent is regarded as a central purpose for the existence of freedom-of-information laws.[77]

Imposing criminal penalties for disclosing information represents a stark departure from venerated principles of U.S. constitutional, common, and statutory law. The Supreme Court has strongly indicated its disinclination to create new categories of constitutionally unprotected speech beyond the handful of traditionally recognized exemptions, even for speech of exceptionally low

---

public knowledge about public affairs in order to ensure an informed citizenry and to minimize the evils inherent in a secluded process.").

[74] *See* State ex rel. Thomas v. Ohio State Univ., 643 N.E.2d 126, 128 (Ohio 1994) (explaining that the Ohio Public Records Act "is construed liberally in favor of broad access, and any doubt must be resolved in favor of disclosure of public records"); Title Rsch. Corp. v. Rausch, 450 So. 2d 933, 936 (La. 1984) ("Whenever there is doubt as to whether the public has the right of access to certain records, the doubt must be resolved in favor of the public's right to see.").

[75] The federal Freedom of Information Act codifies the "clearly unwarranted" standard at 5 U.S.C. § 552(b)(6). *See also* 5 ILL. COMP. STAT. § 140/7(1)(c) (2022) (providing that, under Illinois law, "clearly unwarranted invasion of personal privacy" is a lawful basis for an agency to withhold public records). The Illinois statute defines the type of invasiveness that would justify withholding records in accordance with the common law of invasion of privacy: "[T]he disclosure of information that is highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information." *Id.* But the statute goes on to emphasize the unique public importance of information about government employees: "The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy." *Id.*

[76] *See, e.g.*, David A. Dana & Susan P. Koniak, *Secret Court Settlements Are a Scourge on Society*, WASH. POST (Dec. 14, 2017), https://www.washingtonpost.com/opinions/secret-court-settlements-are-a-scourge-on-society/2017/12/14/7b9cb97e-e022-11e7-89e8-edec16379010_story.html (arguing that sealed settlements conceal safety hazards, and that some government agencies "use taxpayer funds to secretly settle in cases of police brutality and other serious wrongs, leaving the public in the dark on the facts").

[77] *See, e.g.*, Bradley v. Ackal, 954 F.3d 216, 233 (5th Cir. 2020) (finding that news organizations were entitled to details of a sealed settlement agreement resolving a wrongful death claim brought by the survivors of a Black man shot to death in the back of a sheriff's patrol car, and stating that "the public's interest in the settlement amount is particularly legitimate and important, not least because disclosure will allow the public to monitor the expenditure of taxpayer money"); Pengra v. State, 14 P.3d 499, 503 (Mont. 2000) (granting news organizations' request for access to a sealed settlement agreement in a lawsuit against the Montana prison system over a rape and murder committed by an escaped inmate, and observing, "Disclosure of such agreements provides an irreplaceable opportunity for taxpayers to assess the seriousness of unlawful and negligent activities of their public institutions.")

expressive value.[78] For a statute that criminalizes doxing to be constitutional, then, it would have to fit within a narrow exception to the formidable body of law highly protective of the ability to gather and publish information.

B. Criminalizing Speech

A dense, and at times confusing, thicket of case law has grown up around what might be called "crime-adjacent" speech—that is, speech indicating that harmful criminal wrongdoing will, or should, befall particular people.[79] That seemingly minor distinction—between "will befall" and "should befall"—can be a legally decisive one, as we shall see.

1. True Threats

The Constitution does not protect "true threats,"[80] since they have "little if any social value," may inflict "serious emotional stress" on the threatened person, and "may lead to a violent confrontation."[81] Although the "true threat" exception is in tension with principles of free speech, the Supreme Court has reasoned that this restriction on speech "protect[s] individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur . . . ."[82] The Supreme Court has considered the "totality of the circumstances, . . . whether the threat is 'conditional,' and the reaction of the listeners" when determining whether speech constitutes a true threat and therefore receives no protection from the First Amendment.[83]

The Court first explicitly stated that a "true threat" receives no First Amendment protection in the 1969 case of *Watts v. United States*, involving a speaker prosecuted for remarks at an anti-war rally on the National Mall in Washington, D.C., that were perceived as threats to assassinate President Lyndon Johnson.[84] Because the speaker phrased his remarks in terms of a conditional wish to shoot Johnson should the opportunity arise at some future time, and because the remarks were received by the audience as political hyperbole, the justices found that the speech was too abstract to constitute a prosecutable

---

[78] *See* United States v. Stevens, 559 U.S. 460, 470 (2010) (declining to find that depictions of animal cruelty constitute a new category of unprotected speech that can be criminalized and stating, "The First Amendment's guarantee of free speech does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits.").

[79] *See* Marc Rohr, *"Threatening" Speech: The Thin Line Between Implicit Threats, Solicitation, and Advocacy of Crime*, 13 RUTGERS J.L. & PUB. POL'Y 150, 155-67 (2015) (analyzing cases in which courts have struggled to decide whether speech urging others to commit bodily harm should be treated as a direct threat by the speaker or, alternatively, as a solicitation for others to commit violence, which requires a more demanding showing of the prosecution).

[80] Virginia v. Black, 538 U.S. 343, 359-60 (2003).

[81] Elonis v. United States, 575 U.S. 723, 746 (2015).

[82] R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992).

[83] United States v. Fullmer, 584 F.3d 132, 154 (3d Cir. 2009) (quoting Watts v. United States, 394 U.S. 705, 708 (1969)).

[84] Watts, 394 U.S. at 706-07.

threat.[85] Then, in *Virginia v. Black*, the Court elaborated on its threat-speech jurisprudence in the context of a First Amendment challenge to a Virginia statute making it a felony to burn a cross.[86] Although the statute purported to require proof of an intent to intimidate, it provided that intent could be inferred from the mere act of burning the cross—which, in the view of five justices, made the statute unconstitutionally broad.[87] "The act of burning a cross may mean that a person is engaging in constitutionally proscribable intimidation. But that same act may mean only that the person is engaged in core political speech," Justice Sandra Day O'Connor wrote.[88]

The criminalization of threat speech raises questions about what, exactly, is the "wrong" that the law seeks to deter and punish. If the purpose of the law is to prevent people from committing violence by intercepting them during the planning stage, then "threat" prosecutions can be understood as a cousin of "attempt" law, so that the focus is properly on whether the speaker actually was preparing to follow through on the threat and had the means to do so. But it is often observed that threats can inflict harm even if made by speakers who have no intention of actually acting, if the targeted listener is placed in fear.[89] If the law's focus is on protecting the listener against the intimidating effect of the speech, then the speaker's ultimate intent becomes less relevant, and the way that the speech affects the reasonable listener becomes more relevant.[90]

There is ongoing disagreement in the courts over whether the "threatening" nature of speech is properly judged by reference to the speaker's intent or to a reasonable listener's impression of the speech. The Ninth Circuit has read the O'Connor opinion in *Black* as requiring proof that the speaker acted with intent to communicate a threat.[91] However, most circuits have concluded that *Black* did not fundamentally change the First Amendment threat analysis, and that a speaker may be convicted so long as a reasonable listener would perceive the speech as conveying an intent to commit violence.[92]

The Supreme Court had an opportunity, but ultimately failed, to clarify whether the First Amendment requires proof of some particular level of

---

[85] *Id.* at 708.
[86] Virginia v. Black, 538 U.S. 343 (2003).
[87] *Id.* at 364-67.
[88] *Id.* at 365.
[89] *See* Amy E. McCann, Comment, *Are Courts Taking Internet Threats Seriously Enough? An Analysis of True Threats Transmitted Over the Internet, as Interpreted in United States v. Carmichael*, 26 PACE L. REV. 523, 544 (2006) ("[T]hreats, even ones that the speaker has no intention of carrying out, disrupt the lives of the recipient.").
[90] *See Black*, 538 U.S. at 360 (observing that the First Amendment exception allowing for prosecution of true threats protects the listener from "the fear of violence" and "from the disruption that fear engenders").
[91] *See* United States v. Cassel, 408 F.3d 622, 633 (9th Cir. 2005).
[92] *See, e.g.*, Porter v. Ascension Par. Sch. Bd., 393 F.3d 608, 616-17 (5th Cir. 2004); United States v. Fuller, 387 F.3d 643, 646 (7th Cir. 2004). *But see* Paul T. Crane, Note, *"True Threats" and the Issue of Intent*, 92 VA. L. REV. 1225, 1272 (2006) (arguing that the Ninth Circuit's "reasonable speaker" approach, which fails to consider whether the speaker had the subjective intent to deliver a threat, "severely discounts the speaker's general First Amendment right to communicate freely" and is likely to lead people to self-censor in fear of being misunderstood).

culpability on the part of the speaker.[93] In *Elonis v. United States*, the Court vacated the conviction of a Pennsylvania man, Anthony Elonis, who posted a series of graphically violent statements on Facebook that he claimed were rap lyrics and comedy routines, but which his estranged wife—and law enforcement—perceived as threats to do harm.[94] Elonis' posts did not stop even after his wife obtained a protection order against him; in fact, he defiantly mocked the ineffectiveness of the order.[95] Federal prosecutors charged Elonis with communicating an unlawful threat in violation of 18 U.S.C. § 875(c); a jury convicted him, and the Third Circuit affirmed the conviction.[96] The Third Circuit rejected Elonis's contention that the "true threat" exception to the First Amendment requires that a jury find that the speaker subjectively intended his statements to be understood as threats to commit violence.[97]

Elonis appealed on First Amendment grounds, but the Supreme Court ruled in his favor on the narrower basis that Section 875(c) requires proof of an additional element—a culpable mental state, or *mens rea*—which was lacking in his case.[98] The Court held that the *mens rea* element would be "satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat."[99] Thus, sustaining a conviction for threat speech requires proof of some level of culpability on the part of the speaker that the communication meant to contain a threat. The Court did not specify exactly what level of culpability the prosecution must prove, but it did explicitly state that conviction requires more than a mental state of negligence.[100] Since *Elonis* was decided on statutory grounds, the larger question of whether the Constitution requires proof of any particular culpable mental state on the part of the speaker remains unsettled.[101] Nevertheless, the Supreme Court's solicitude in threat-speech cases for the rights of even unsympathetic speakers illustrates how high the bar has been set to prosecute someone for anything short of an unambiguous expression of intent to commit violence.

A Ninth Circuit case involving a website intentionally putting abortion clinic doctors in fear of violence furnishes a roadmap for how existing statutes can be used against threatening online speech without running afoul of the First

---

[93] Zachary Stoner, Comment, *What You Rhyme Could Be Used Against You: A Call for Review of the True Threat Standard*, 44 NOVA L. REV. 225, 236 (2020) (stating that "there was much hope" that the Court would use the *Elonis* case to clarify confusion over what level of culpability is constitutionally required to prosecute a speaker for threats, but the Court "failed to shed any kind of additional light on the true threat exceptions" to the First Amendment).
[94] Elonis v. United States, 575 U.S. 723, 726-28, 748 (2015).
[95] *Id.* at 729.
[96] United States v. Elonis, 730 F.3d 321 (3d Cir. 2013), *rev'd*, 575 U.S. 723 (2015).
[97] *Id.* at 332.
[98] *Elonis*, 575 U.S. at 737-38.
[99] *Id.* at 740.
[100] *Id.* at 738-39.
[101] *See* Megan R. Murphy, Comment, *Context, Content, Intent: Social Media's Role in True Threat Prosecutions*, 168 U. PA. L. REV. 733, 740 (2020) (urging the Court to clarify the constitutional standards that apply to prosecutions for threat speech because of continuing confusion among lower courts that persists after *Elonis*, particularly when the speech is conveyed over social media).

Amendment. In *Planned Parenthood v. American Coalition of Life Activists*, doctors and clinics sued anti-abortion activists under a federal statute, the Freedom of Access to Clinics Entrances Act, seeking to enjoin continued publication of a website featuring the names and addresses of abortion providers, as well as public figures perceived as supporting abortion rights.[102] The website used melodramatic language accusing the doctors of "crimes against humanity" and included references to three recently murdered doctors, giving the website the appearance of a checklist targeting doctors for assassination.[103] Based on that context—the plaintiffs reasonably fearing violence because they were aware that adherents of some of the defendant's organizations had killed other providers who appeared on the website's "Wanted" list—the court found the case decisively different from the Supreme Court's seminal threat-speech ruling in *Watts*, where the speech was hyperbolic and conjectural.[104] The court found no constitutional problem with applying the statute to the defendants' website and accompanying "Wanted" posters because the statute, by its terms, applied only to speech containing a threat of force delivered with the intent to intimidate, thus qualifying as a constitutionally unprotected "true threat."[105]

2. Incitement and Solicitation

When a speaker does not indicate a disposition to personally commit violence but rather urges others to harm targeted individuals, the speech is analyzed as incitement or solicitation as opposed to a "true threat."[106] The line between a "threat" case and an "incitement" case is an indistinct one, to be sure.[107] But a key distinction is that threat speech is considered punishable largely because it instills fear in the recipient, whereas incitement could be punishable even if there was no realistic likelihood that the person targeted for violence would see or be placed in fear by the speech: for instance, a "private" Facebook group viewable only by those admitted to see it, where members of a violent neo-Nazi organization plot their strategies.[108]

The Supreme Court's seminal case, *Brandenburg v. Ohio*, involved a Ku Klux Klan leader's challenge to his conviction under a state statute outlawing "criminal syndicalism."[109] The Court concluded that the statute was

---

[102] Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1062-63 (9th Cir. 2002) (en banc); 18 U.S.C. § 248.
[103] *See id.* at 1080.
[104] *See id.* at 1085 (citing United States v. Watts, 394 U.S. 705, 708 (1969)).
[105] *Id.* at 1076.
[106] *See* Rohr, *supra* note 79, at 153-54 (explaining differing legal analyses that apply to speech advocating crime versus speech directly threatening harm).
[107] Lyrissa Barnett Lidsky, *Incendiary Speech and Social Media*, 44 TEX. TECH L. REV. 147, 158 (2011). *See also* United States v. Wheeler, 776 F.3d 736, 745 (10th Cir. 2015) (observing that, when it comes to online speech, "the line between threats and incitement" is not "completely distinct").
[108] *See* Lidsky, *supra* note 107, at 158 ("Incitements are unprotected because they create a likelihood of violent actions, not because of the fear they engender.").
[109] Brandenburg v. Ohio, 395 U.S. 444, 445 (1969).

unconstitutionally overbroad because it criminalized mere "advocacy."[110] Time and again, courts applying *Brandenburg* have recognized that speech endorsing the use of violence as a general principle, or even commenting that a particular person or group is deserving of violence, remains within the broad umbrella of First Amendment protection and cannot be outlawed.[111]

The Court erected a high barrier for criminalizing speech that does not directly threaten violence but merely instructs or encourages listeners to act violently:

> [T]he constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[112]

In other words, while a direct threat is punishable even if the threatened violence is somewhat remote or uncertain in time (e.g. "I am watching you, and when you least expect it, I will put a bullet in your head"), a successful prosecution for incitement speech requires proof of "imminence."[113] This is regarded as a necessary safeguard because when the speaker is addressing others beyond the speaker's direct control, acting on the incitement requires a volitional choice by third parties who have time to decide whether to act.[114]

In an especially instructive case, *NAACP v. Claiborne Hardware Co.*, the Supreme Court decided that civil rights organizers who used threatening language in the context of enforcing a boycott against white-owned businesses could not be prosecuted because, under *Brandenburg*, their speech was constitutionally protected advocacy.[115] The Court found that the First

---

[110] *Id.* at 447-48.

[111] *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 253 (2002) (concluding that a congressional ban on possessing simulations of child pornography was unconstitutionally broad, despite proponents' contention that the simulations might encourage viewers to seek out actually unlawful child pornography, "The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it."); United States v. Miselis, 972 F.3d 518, 536 (4th Cir. 2020) (finding that aspects of the federal Anti-Riot Act, 18 U.S.C. §§ 2101-02, were unconstitutionally broad because they made it a crime to "encourage" or "promote" a riot without requiring proof that a riot was likely to imminently result).

[112] *Brandenburg*, 395 U.S. at 447.

[113] JoAnne Sweeny, *Incitement in the Era of Trump and Charlottesville*, 47 CAP. U. L. REV. 585, 597 (2019) ("Imminence is a unique and indispensable requirement for incitement. In order to qualify as incitement, the speech must call for violence or illegal acts to happen immediately, not at a later time or upon the satisfaction of a condition.").

[114] *See* Jennifer Elrod, *Expressive Activity, True Threats, and the First Amendment*, 36 CONN. L. REV. 541, 570 (2004) (observing that, under the doctrine of incitement speech, "no liability attaches to the speaker's words of incitement unless and until the third party acts on those statements by attempting to act or carrying out illegal actions . . . . Without the nexus of the speaker's words and the illegal action (or likelihood of it) by the third party, there is no violation of the law under the theory of incitement. The speaker is engaging in mere advocacy.").

[115] NAACP v. Claiborne Hardware Co., 458 U.S. 886, 902, 927-28 (1982).

Amendment prohibited prosecuting "emotionally charged rhetoric" in which an activist declared that violators of an NAACP-organized boycott would be "disciplined"—at one point, saying, "If we catch any of you going in any of them racist stores, we're gonna break your damn neck."[116] Even though some Black people suspected of breaking the boycott did experience violence, the Court still found that the speaker's advocacy was constitutionally protected, absent proof that the speaker "authorized, ratified, or directly threatened acts of violence."[117] As Justice John Paul Stevens wrote,

> Strong and effective extemporaneous rhetoric cannot be nicely channeled in purely dulcet phrases. An advocate must be free to stimulate his audience with spontaneous and emotional appeals for unity and action in a common cause. When such appeals do not incite lawless action, they must be regarded as protected speech.[118]

Solicitation shares qualities with incitement, in that it involves provoking illegal action by people other than the speaker and also with the category of unprotected speech commonly referred to as "speech integral to criminal conduct."[119] The Supreme Court's archetypal illustration of speech integral to criminal conduct was using the expressive tactics of picketing and boycotting in an attempt to coerce a business to violate antitrust laws.[120]

3. Harassment

While speech does not lose constitutional protection merely because it is unwelcome, a speaker can cross the line into criminally punishable behavior if speech is delivered in an especially menacing way. Harassment laws have been deemed constitutional in part because they are primarily directed to the manner in which speech is presented rather than to its content; for instance, a person could commit harassment by calling another person's home phone persistently in the middle of the night to alarm them, even if the caller said something meaningless—or said nothing— when the recipient answered the phone.[121] Indeed, there is a school of thought that harassment is not "speech" at all, but

---

[116] *Id.* at 902, 928.
[117] *Id.* at 929.
[118] *Id.* at 928.
[119] *First Amendment – Freedom of Speech – Criminal Solicitation* – United States v. Sineneng-Smith, 134 HARV. L. REV. 480, 487 (2020) ("Solicitation is commonly recognized as a subcategory of speech integral to criminal conduct.").
[120] *See* Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498-99 (1949).
[121] *See* Gormley v. Dir., Conn. State Dept. of Prob., 632 F.2d 938, 940 n.1, 942 (2d Cir. 1980) (rebuffing overbreadth challenge to Connecticut's telephone harassment statute, which made it a crime to place a call "with intent to harass, annoy or alarm another person" and observing, "Whether speech actually occurs is irrelevant, since the statute proscribes conduct, whether or not a conversation actually ensues.").

rather, is criminal conduct that happens to include words as an element of the conduct.[122]

Harassment statutes have flunked constitutional scrutiny when they fail to define the proscribed behavior narrowly and precisely, or when liability is triggered without a sufficiently demanding showing of intent. A common formulation of anti-harassment laws—making it a crime to "annoy" or "alarm" another person—has regularly been deemed unconstitutionally broad, because legitimate expression might trigger severe alarm or annoyance in some listeners.[123]

In one illustrative example, a Texas appellate court decided that a statute criminalizing harassment via electronic communication was unconstitutionally overbroad because it outlawed speech conveyed "in a manner reasonably likely to harass, annoy, alarm, abuse, torment, embarrass, or offend another."[124] Contrasting the statute with laws that outlaw harassing telephone calls, which have been held constitutional, the court found that the far greater reach of the electronic communication statute rendered it infirm: "[W]e conclude that the electronic-communications-harassment statute goes well beyond a lawful proscription of intolerably invasive conduct and instead reaches a substantial amount of speech protected by the First Amendment."[125]

The harassment statutes that best withstand constitutional challenge are those containing rigorous safeguards so that only speakers who intentionally inflict severe distress, with no legitimate purpose for speaking, can be held responsible.[126] For instance, Maryland's highest court rejected a constitutional

---

[122] *See* State v. Thorne, 333 S.E.2d 817, 819 (W. Va. 1985) ("Prohibiting harassment is not prohibiting speech, because harassment is not a protected speech. Harassment is not communication, although it may take the form of speech."). *But see* Aaron H. Caplan, *Free Speech and Civil Harassment Orders*, 64 HASTINGS L.J. 781, 809-10 (2013) (observing that "there is no categorical 'harassment exception' to the First Amendment . . . .", and questioning the circular reasoning of courts that treat harassing speech as punishable by simply relabeling it as "conduct").

[123] *See* People v. Marquan M., 19 N.E.3d 480, 484 (N.Y. 2014) (finding that ordinance making it a misdemeanor offense to disseminate information online "with the intent to harass, annoy, threaten, abuse, taunt, intimidate, torment, humiliate, or otherwise inflict significant emotional harm on another person" was unconstitutionally overbroad); State v. Bryan, 910 P.2d 212, 217 (Kan. 1996) (finding that anti-stalking harassment law making it a crime to "follow" someone was unconstitutionally broad because it "contains no guidelines to determine when a following becomes alarming, annoying, or harassing"); People v. Norman, 703 P.2d 1261, 1267 (Colo. 1985) (en banc) (concluding that Colorado harassment statute violated the Due Process Clause because it encompassed even "innocuous" speech based on its effect on the listener: "An actor, a clown, a writer or a speaker all might be subject to criminal prosecution because their acts are perceived by some official to annoy or alarm others."); State v. Blair, 601 P.2d 766, 768 (Or. 1979) (en banc) (holding that statute proscribing communications by telephone in a manner "likely to cause annoyance or alarm," which failed to require any proof that the victim was subjected to any particular injury, was unconstitutionally vague.).

[124] State v. Chen, 615 S.W.3d 376, 379 (Tex. App. 2020).

[125] *Id.* at 383.

[126] *See, e.g.*, State v. Brown, 85 P.3d 109, 111, 113 (Ariz. Ct. App. 2004) (concluding that Arizona's criminal harassment law does not regulate constitutionally protected speech, because "criminal liability under the statute is based on the 'manner' in which certain communication is conveyed and

challenge to the state's anti-harassment statute brought by a defendant who sent 130 unwanted letters to a woman he had previously been found guilty of kidnapping and stalking.[127] The court found that the law was neither unconstitutionally overbroad nor vague because it required proof of specific intent, applied only to conduct with no "legal purpose" and contained a savings clause excluding "any peaceable activity intended to express political views or provide information to others . . . ."[128] This Maryland statute exemplifies the type of narrow tailoring that might make a doxing statute defensible as well.

C. Criminalizing Online Speech

While the doctrine of unprotected "crime-adjacent" speech evolved in the context of one-to-one telephone calls, the availability of online publishing has provoked widespread calls to rethink established speech-protective precedents. It is widely perceived that the internet, in particular social media, enables ordinary citizens to put harmful speech in front of mass audiences that previously were only reachable to an elite few who owned broadcasting licenses or printing presses.[129]

The Supreme Court has rarely accepted cases involving online speech, but in its most expansive pronouncement on the subject, *Reno v. American Civil Liberties Union*, the Court rejected arguments that the pervasiveness of online speech justifies diminishing its First Amendment protection.[130] The *Reno* case entailed a First Amendment challenge to provisions of the Communications Decency Act of 1996 that outlawed making "patently offensive" images accessible online to minors.[131] The Court declined to apply the stepped-down level of constitutional protection that applies to over-the-air television and radio broadcasting during family listening hours, and instead held that the First Amendment applies with full force to online speech, just as is does to books, newspapers, or any other medium.[132] As the Court said in a subsequent case

---

the underlying purpose for the communication," and noting that the statute contains a carve-out for "an otherwise lawful demonstration, assembly or picketing").

[127] Galloway v. State, 781 A.2d 851, 857 (Md. 2001).

[128] *Id.* at 862. *See also* State v. E.J.Y., 55 P.3d 673, 677-79 (Wash. Ct. App. 2002) (rejecting overbreadth challenge to Washington's criminal harassment statute, because the statute applies only to speech made "without lawful authority").

[129] *See* Murphy, *supra* note 101, at 744 (observing paradox that online speech is created and published with less formality than other forms of expression, yet is treated by many courts as being more consequential: "This inconsistent view of online speech—as generally less valuable or meaningful than other forms of speech, but with the potential to do acute, potentially legally actionable harm to individuals or discrete groups of hearers—creates a trap for the unwary social media user."); Frank D. LoMonte, *The "Social Media Discount" and First Amendment Exceptionalism*, 50 U. MEM. L. REV. 387, 389 (2019) ("Across American society, regulatory authorities—often with the acquiescence of credulous judges—are policing speech on social networking sites as if social media constituted a 'First Amendment-free zone' to which traditional free-speech principles no longer apply.").

[130] Reno v. Am. C.L. Union, 521 U.S. 844, 869-70 (1997).

[131] *Id.* at 859-60.

[132] *Id.* at 869-70.

striking down criminal penalties for selling violent video games to minors, "whatever the challenges of applying the Constitution to ever-advancing technology, 'the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary' when a new and different medium for communication appears."[133] Thus, when lawmakers seek to criminalize online speech, they must contemplate the same demanding level of First Amendment scrutiny that would apply in the paper-and-ink world.[134]

The ongoing debate over criminalizing "revenge porn"—the public dissemination of sexually explicit images to inflict harm on their subject[135]—illustrates the challenge of creating a special category of unprotected speech uniquely designed for the internet. As with doxing, the debate over revenge porn is only as old as smartphones and social media, testing First Amendment doctrines that courts fashioned in the context of books, magazines, and movie theaters. Concern for those victimized by the nonconsensual distribution of intimate photos is colliding with First Amendment principles that disfavor prior restraint of, or criminal prosecution for, nonthreatening speech. The nonprofit Cyber Civil Rights Initiative reports that forty-eight states plus the District of Columbia have statutes outlawing revenge porn,[136] but those statutes have faced a wave of constitutional challenges.[137]

"[R]evenge porn occurs when content intended for one person's private enjoyment is shared" without consent with a larger audience, frequently "on public websites specifically dedicated to hosting sexually explicit content . . . ."[138] The First Amendment generally protects the distribution of sexually explicit material from legal regulation unless the material is deemed legally obscene, which is a difficult burden to meet.[139] Still, constitutional challenges to the first generation of revenge porn statutes have generally failed—even though courts

---

[133] Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790 (2011) (quoting Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 503 (1952)).

[134] *See* Judge Lynn Adelman & Jon Deitrich, *Extremist Speech and the Internet: The Continuing Importance of Brandenburg*, 4 HARV. L. & POL'Y REV. 361, 371-72 (2010) (rejecting arguments that the perceived dangerousness of online speech justifies lowering the threshold for criminalizing it, noting that "all previous advances in communications technology, including the printing press, the telegraph, and the telephone, allowed speakers to reach larger audiences" and that anonymous speech has existed since the earliest days of the United States).

[135] *See* John A. Humbach, *The Constitution and Revenge Porn*, 35 PACE L. REV. 215, 215 (2014) ("Revenge porn refers to sexually explicit photos and videos that are posted online or otherwise disseminated without the consent of the persons shown, generally in retaliation for a romantic rebuff.").

[136] *Nonconsensual Pornography Laws*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/nonconsensual-pornography-laws/ (last visited May 29, 2022) (database of statutes is viewable online).

[137] *See* Katherine G. Foley, *"But, I Didn't Mean to Hurt You": Why the First Amendment Does Not Require Intent-to-Harm Provisions in Criminal "Revenge Porn" Laws*, 62 B.C. L. REV. 1365, 1389-93 (2021) (collecting cases in which people convicted of violating revenge porn laws have challenged their constitutionality).

[138] Scheller, *supra* note 23, at 558-59.

[139] Miller v. California, 413 U.S. 15, 36 (1973).

rigorously scrutinize the statutes as content-based restrictions on speech.[140] Courts have upheld revenge porn statutes, even in the face of strict scrutiny, because they contain safeguards so that only intentional harm-causing conduct is subject to prosecution.[141] But at least one court has concluded that a state's statutory prohibition on revenge porn ran afoul of the First Amendment.[142] A federal district court found Minnesota's nonconsensual porn statute to be overbroad, because the statute broadly criminalized sharing nude images in a way that could apply to innocent conduct (such as a photo that incidentally captured a woman in the background breastfeeding a baby) and lacked a sufficient *mens rea* requirement to protect unwitting third parties who reshare images unaware that the images were originally disseminated without consent.[143]

The ongoing debate over whether disseminating lawfully obtained nude images for purposes of causing distress can be criminalized[144] reflects just how protective First Amendment jurisprudence is, even in the face of highly sympathetic public policy arguments. Unlike true acts of revenge porn, which have no legitimate purpose and are intended solely to inflict harm, the bundle of behaviors known as "doxing" at times encompasses speech with a neutral or even societally beneficial purpose. Thus, if revenge porn is difficult to criminalize, doxing will logically be even more well-insulated against criminalization.

IV. THE LEGISLATIVE RESPONSE

A. Anti-Doxing Statutes Vary in Scope, Requisite Mental State

In 2007, Congress passed the Court Security Improvement Act,[145] which included among its provisions an early "anti-doxing" measure targeted to protect those connected with the federal legal system from threatening or intimidating disclosures.[146] The law criminalizes disclosing "restricted personal information" about anyone connected with federal criminal cases (judges, jurors, witnesses,

---

[140] *See* Foley, *supra* note 139, at 1392-1403 (explaining that, with the exception of one ruling in Illinois, courts reviewing constitutional challenges to revenge porn statutes have applied strict scrutiny).

[141] *See, e.g.*, *Ex parte* Jones, No. PD-0552-18, 2021 WL 2126172, at *13 (Tex. Crim. App. May 26, 2021) (salvaging Texas revenge porn statute by narrowly construing it to apply only to an intentional disclosure of sexually explicit material where there is proof of fault that the defendant revealed the identity of the person depicted in the images, and that the disclosure was made without consent); State v. VanBuren, 214 A.3d 791, 812 (Vt. 2019) (rejecting facial challenge to Vermont's revenge porn statute, and concluding that the statute is narrowly tailored because it requires "a specific intent to harm, harass, intimidate, threaten, or coerce the person depicted or to profit financially" as well as proof of, at least, knowledge that the disclosure was made without the victim's consent).

[142] State v. Ahmed, No. 34-CR-17-954, 2019 Minn. Dist. LEXIS 522 (D. Minn. Aug. 1, 2019).

[143] *Id.* at *32-33.

[144] *See* Cynthia Barmore, *Criminalization in Context: Involuntariness, Obscenity, and the First Amendment*, 67 STAN. L. REV. 447, 460 (2015) (acknowledging First Amendment arguments that criminalizing nonconsensual distribution of explicit images "unconstitutionally limits communication to willing listeners").

[145] Court Security Improvement Act of 2007, Pub. L. No. 110–177, 121 Stat. 2538 (2008).

[146] 18 U.S.C. § 119.

and so on), or any other "officer" of the United States government acting within the course of duty, "with the intent to threaten, intimidate, or incite the commission of a crime of violence" against that person or a family member.[147] "[R]estricted personal information" is broadly defined to include a person's "home address, home phone number, mobile phone number, personal email, or home fax number . . . ."[148] The statute has shown up only once in a published court decision, as part of the 2017 prosecution of an Ohio man who posted threatening messages targeting U.S. military service members.[149] A twenty-four-year-old Akron man was charged with using the blogging platform Tumblr to repost messages from the Islamic terrorist organization ISIS that called for the deaths of U.S. soldiers, including the soldiers' names, addresses, and photos.[150] The defendant challenged the sufficiency of the evidence supporting the indictment but did not challenge the constitutionality of the statute,[151] so whether Section 119(a) satisfies First Amendment standards remains to be tested.

Even before the current wave of legislative proposals specifically identified as "anti-doxing" laws, some state laws (explicitly or implicitly) already penalized disseminating information online in an attempt to harass. For example, since 2001, Virginia has criminalized publishing a person's "name or photograph along with identifying information" if there is proof of an "intent to coerce, intimidate, or harass" the person.[152] Georgia's anti-stalking statute, first enacted in 1993, makes it a crime to disseminate the home address or other personal information of a person who has obtained a restraining order or protective order "in such a manner that causes other persons to harass or intimidate such person" if there was reason to anticipate that the harassment or intimidation would occur.[153]

But statutes specifically tailored to respond to "doxing" are a recent phenomenon. Pressure for lawmakers to do something about the online hostility disproportionately targeting women and people of color intensified after a widely publicized campaign of threats and harassment directed at women in the video gaming field, which became known as "Gamergate."[154] As video game developer, Zoë Quinn, described the ordeal of having her online accounts hijacked by hackers who cracked her password, "The hackers weren't just

---

[147] *Id*. § 119(a).
[148] *Id.* § 119(b)(1).
[149] United States v. McNeil, 228 F. Supp. 3d 809 (N.D. Ohio 2017).
[150] Phil Helsel, *Ohio Man Sentenced to 20 Years Over ISIS Threats to Military*, NBCNEWS.COM (Aug. 2, 2017, 8:08 PM), https://www.nbcnews.com/news/us-news/ohio-man-sentenced-20-years-over-isis-threats-military-n789051.
[151] *See* McNeil, 228 F. Supp. 3d at 815-16 (finding that, based on the allegations of the indictment, a jury could find all of the elements of Section 119 satisfied: that the speaker knowingly made the addresses of U.S. military personnel publicly available, and that the posts were made with an intent to threaten, intimidate, or incite a crime of violence).
[152] VA. CODE ANN. § 18.2-186.4 (2022). The penalty is heightened if the targeted person is known to be a law enforcement officer. *See id.*
[153] GA. CODE ANN. § 16-5-90(a)(2) (2022).
[154] *See* Zoë Quinn, *What Happened After GamerGate Hacked Me*, TIME (Sept. 11, 2017, 12:37 PM), https://time.com/4927076/zoe-quinn-gamergate-doxxing-crash-override-excerpt/.

posting calls for me to die or talking about what a fat slut I was; they were sharing my personal information: my old address in Canada, cell-phone numbers from a few years back, my current cell-phone number and my current home address."[155]

During 2021, Arizona, Colorado, Florida, Kentucky, Minnesota, Oklahoma, and Oregon enacted (or, in the case of Colorado, substantially broadened) statutes that penalize publishing personally identifying information that might expose people to harassment or violence. While superficially similar, these laws vary in critical respects: (1) the scope of people whose information is protected against disclosure, (2) the type of information that may not be disclosed without consent, and (3) the degree of culpability on the part of the publisher that must be proven for liability to attach. Notably, the impetus for legislation to outlaw doxing has alternately originated from the political left (in states such as Colorado and Oregon) and from the political rig

ht (in states such as Florida and Oklahoma), depending on whether the proponents identify with the people viewed as likely to be targeted for doxing or with the people likely to be accused of it.

A breakdown of recently enacted state laws follows:

Arizona: In 2021, Arizona broadened its existing harassment statute to add an anti-doxing provision. The new statute makes it a crime to use electronic communication methods to share any person's personally identifying information, without consent, for the purpose of "imminently" causing physical harm or harassment, if the harm or harassment actually does occur.[156] The law covers a broad scope of disclosures, including a person's work address, "or other contact information that would allow the identified person to be located, contacted or harassed."[157]

Colorado: A preexisting 2002 state law that outlawed knowingly sharing personal information about a peace officer, judge, or prosecutor online was broadened in 2021 to also apply to information about public health workers or their families.[158] People working in public health found themselves targeted for insults and threats by extremists opposed to safety measures enacted in response to the COVID-19 pandemic that swept the globe throughout 2020-2022[159] The scope of the information covered by the statute is broad, including not just home address, phone number, or personal email address, but also a "personal photograph" or a photo of the person's home or vehicle.[160] Misdemeanor criminal penalties apply if the information is shared and two preconditions are satisfied: (1) the posting presents an "imminent and serious threat" to safety, and (2) the

---

[155] *Id*.
[156] ARIZ. REV. STAT. ANN. § 13-2916(A)(4) (2022).
[157] *Id.* § 13-2916(E)(4).
[158] *See* COLO. REV. STAT. § 18-9-313(2.7) (2022); see also *id.* § 18-9-313(1)(n).
[159] Marisa Fernandez, *Nearly a Quarter of Health Workers Threatened or Harassed, CDC Says*, AXIOS (June 28, 2021), https://www.axios.com/cdc-public-health-worker-mental-health-tolls-b0cbf9ed-947a-43b0-be2b-bee388a20718.html.
[160] *See* COLO. REV. STAT. § 18-9-313(1)(l).

publisher "knows or reasonably should know of the imminent and serious threat."[161]

Florida: A law enacted in 2021 that has attracted nationwide attention—and a civil rights lawsuit—primarily because of its curbs on protest activity[162] also includes a prohibition against "cyberintimidation."[163] The provision outlaws posting anyone's information online "with the intent to, or with the intent that a third party will use the information to . . . incite violence or commit a crime against the [targeted] person," or place the person in "reasonable fear of bodily harm."[164] The scope of protected information encompasses "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person" including, but not limited to, an email address, phone number, or postal address.[165] The American Civil Liberties Union of Florida denounced the entire legislative package, calling it overbroad, vague, and a direct attack on First Amendment rights.[166]

Kentucky: In April 2021, Governor Andy Beshear signed Senate Bill 267, which bans publishing anyone's personal information online when the disclosure "would cause a reasonable person to be in fear of physical injury to himself or herself, or to his or her immediate family member or household member" and when the disclosure is made "with the intent to intimidate, abuse, threaten, harass, or frighten . . . ."[167] Information encompassed by the statute, in addition to home contact information, also includes a person's school or work location.[168] The statute provides for escalating criminal penalties, depending on whether injury or death results.[169]

Minnesota: State lawmakers passed an omnibus public safety bill during a 2021 special session that incorporated a previously filed standalone anti-doxing bill.[170] The law applies to information only about law enforcement officers or their family members, and to a relatively narrow range of information: "a home

---

[161] *Id.* § 18-9-313(2.7).
[162] *See* Dan Whitcomb, *Judge Blocks Enforcement of Florida's 'Anti-Riot' Law*, REUTERS (Sept. 10, 2021, 8:19 AM), https://www.reuters.com/world/us/judge-blocks-enforcement-floridas-anti-riot-law-2021-09-09/.
[163] *See* FLA. STAT. § 836.115(2) (2022).
[164] *Id.*
[165] *Id.* § 817.568(1)(f).
[166] *See* Kenny Stancil, *"Racist, Unconstitutional, and Anti-Democratic": FL Passes Anti-Protest Law Ahead of Chauvin Verdict*, SALON (Apr. 21, 2021, 3:32 PM), https://www.salon.com/2021/04/21/racist-unconstitutional-and-anti-democratic-fl-passes-anti-protest-law-ahead-of-chauvin-verdict_partner/.
[167] KY. REV. STAT. ANN. § 525.085(2) (2022); *see also* Chad Mills, *Louisville Leader Applauds New State Law That Limits 'Doxing'*, WDRB (Apr. 14, 2021), https://www.wdrb.com/news/louisville-leader-applauds-new-state-law-that-limits-doxing/article_f5320594-9d8b-11eb-8498-8bd9b877f4d8.html.
[168] KY. REV. STAT. ANN. § 525.085(1)(d) (2022).
[169] *See id.* § 525.085(4).
[170] *See* Jennifer Lewerenz, *Public Safety Bill Makes Doxing a Police Officer a Crime*, KNSI RADIO (June 30, 2021, 11:52 AM). https://knsiradio.com/2021/06/30/public-safety-bill-makes-doxing-a-police-officer-a-crime/.

address, directions to a home, or photographs of a home."[171] The prohibition applies to making information "publicly available" in any medium and does not limit itself to online dissemination.[172] The requisite mental state for conviction is the same as that provided in Colorado: the existence of "an imminent and serious threat" to safety that the speaker "knows or reasonably should know of."[173]

Oklahoma: In 2021, Governor Kevin Stitt signed House Bill 1643, intended to protect Oklahoma law enforcement officers or government officials from being doxed.[174] The statute states that people cannot electronically publish or post anything online that includes personally identifying information about a protected individual if the intent is to threaten, harass, or intimidate, or to "facilitate" another in doing so, and the post actually causes the protected individual to reasonably fear "death or serious bodily injury . . . ."[175] The information that cannot be lawfully disseminated includes not just enumerated classes of confidential information, such as date of birth or Social Security number, but also "any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information . . . ."[176]

Oregon: Oregon's doxing statute differs from the remainder of the "class of 2021" of doxing statutes because it is enforceable by way of civil rather than criminal remedies.[177] A plaintiff can obtain money damages if the defendant, "with the intent to stalk, harass or injure the plaintiff, knowingly caused personal information to be disclosed," if the harm actually occurs, and if a reasonable person would have suffered harm.[178] Protected personal information includes, among other things, the plaintiff's home address, personal email address, personal phone number, or contact information for the plaintiff's employer.[179] The statute is narrowed by its definition of an actionable injury, which is limited to "bodily injury or death."[180]

As can readily be seen, these statutes vary significantly as to what information is considered to be protected against disclosure, what mental state must be shown to convict (or sue) a person accused of doxing, and what type of harm must be foreseen or intended to hold a speaker responsible. These features will be relevant when, inevitably, the statutes face constitutional challenge.

---

[171] MINN. STAT. § 609.5151(1)(3) (2022).
[172] *Id.* § 609.5151(2).
[173] *Id.*
[174] Kaylee Douglas, *Controversial Anti-Doxxing Bill Signed into Oklahoma Law By Gov. Stitt*, KFOR (Apr. 21, 2021, 5:28 PM), https://kfor.com/news/oklahoma-legislature/controversial-anti-doxxing-bill-signed-into-oklahoma-law-by-gov-stitt/.
[175] OKLA. STAT. tit. 21, § 1176(A) (2022).
[176] *Id.* § 1176(B)(4).
[177] *See* OR. REV. STAT. § 30.835 (2022).
[178] *Id.* § 30.835(2)(a).
[179] *Id.* § 30.835(1)(d).
[180] *Id.* § 30.835(1)(b).

B. "Doxing Before Doxing": The First Generation of Court Challenges

Even before "doxing" entered the popular lexicon, several states attempted to criminalize nonconsensual disclosures of personal information. It did not go well. Court after court has invalidated unduly broad statutes that penalized publishing home addresses, phone numbers, or other personally identifying information.

Relatively early in the history of online publishing, a federal court in Washington struck down a 2002 "doxing-before-doxing" statute making it a crime to release home addresses, phone numbers, or other personal information about law enforcement agencies or court employees with intent to harm or intimidate.[181] A police watchdog blogger challenged the statute as facially unconstitutional, and the court agreed.[182] While the state tried to defend the law by claiming that it criminalized only constitutionally unprotected true threats, the court found it substantially overbroad:

> [T]he word "threat" appears nowhere in the statute at issue here, rather, the statute regulates the mere release of personal identifying information. . . . That is, on its face, the statute *does not purport to regulate true threats* or any other proscribable *mode* of speech, but pure constitutionally-protected speech.[183]

Because people's home addresses and phone numbers are readily findable in public records, the court found no compelling government interest in penalizing publishers who disclose the information.[184] For good measure, the court also found the statute to be unconstitutionally vague, because its operative terms ("intent to harm or intimidate") lacked clarity and invited selective enforcement: "[A] statute that demands self-censorship—that one police one's own thoughts and subjective intent—impermissibly sacrifices the public interest in the free exchange of speech and ideas."[185]

Comparable statutes have fared no better elsewhere. A federal district court found that a Florida statute, which criminalized disseminating police officers' contact information, was facially unconstitutional.[186] The operator of a police watchdog website ("Ratemycop.com") was charged with violating the law,

---

[181] Sheehan v. Gregoire, 272 F. Supp. 2d 1135, 1139, 1150 (W.D. Wash. 2003). (In its entirety, the challenged passage stated, "A person or organization shall not, with the intent to harm or intimidate, sell, trade, give, publish, distribute, or otherwise release the residential address, residential telephone number, birthdate, or social security number of any law enforcement-related, corrections officer-related, or court-related employee or volunteer, or someone with a similar name, and categorize them as such, without the express written permission of the employee or volunteer unless specifically exempted by law or court order.").

[182] *Id.* at 1139, 1149.

[183] *Id.* at 1141-42.

[184] *See id.* at 1147 ("Thought-policing is *not* a compelling state interest recognized by the First Amendment.").

[185] *Id.* at 1149.

[186] Brayshaw v. City of Tallahassee, 709 F. Supp. 2d 1244, 1250 (N.D. Fla. 2010).

which proscribed "maliciously" publishing an officer's home address or telephone number "with intent to obstruct the due execution of the law or with the intent to intimidate, hinder, or interrupt any law enforcement officer in the legal performance of his or her duties . . . ."[187] The court rejected the state's claim that merely disclosing an officer's contact information could qualify as a "true threat," even if the speaker intended for the publication to be intimidating.[188] Rather, the court found that publishing lawfully obtained information about law enforcement officers relates to matters of public concern: "The publication of truthful personal information about police officers is linked to the issue of police accountability through aiding in achieving service of process, researching criminal history of officers, organizing lawful pickets, and other peaceful and lawful forms of civic involvement that publicize the issue."[189]The court recognized, then, that even facilitating picketing at a police officer's home was a constitutionally protected use of lawfully obtained information.

More recently, a pro-gun political blogger won a First Amendment challenge to a California statute enabling government officials to demand the takedown of their home contact information from the web.[190] The statute empowered elected or appointed officials to serve written notice on website operators that they believe disseminating their home address or phone number constitutes a safety hazard, obligating the publisher to pull down the information promptly or face civil penalties.[191] The blogger used an online public records search to gather the home addresses and phone numbers of forty California legislators who voted in favor of gun control, and he published their contact information in what he called a "tyrant registry."[192] After several legislators reported receiving intimidating phone calls at home, a legislative attorney served the blogger with the statutorily provided takedown notice, and he responded with a First Amendment lawsuit.[193]

The court found that the blogger used the legislators' contact information in connection with "core political speech," which is entitled to the highest degree of constitutional protection.[194] The court found that, even if the law was deemed necessary to advance the compelling objective of public officials' safety, it would flunk First Amendment scrutiny because it was not narrowly tailored to further that objective.[195] The law lacked narrow tailoring in several respects: it required merely an assertion that the public official felt unsafe, even if the feeling was not objectively reasonable; it made no allowance for publishing the officials' contact information for lawful and harmless reasons; and it made no distinction between revealing previously unpublished information versus disseminating information

---

[187] *Id.* at 1247.
[188] *Id.* at 1248.
[189] *Id.* at 1249.
[190] Publius v. Boyer-Vine, 237 F. Supp. 3d 997, 1028 (E.D. Cal. 2017).
[191] *Id.* at 1012.
[192] *Id.* at 1004.
[193] *Id.* at 1004-05.
[194] *Id.* at 1014.
[195] *Id.* at 1019.

that is already widely publicly available.[196] The statute was also deficient because of its underinclusiveness, restricting only online publishing and not other methods of communication—even a medium like television that might reach a far larger audience than the plaintiff's blog.[197]

A Virginia blogger's as-applied challenge to a state statute making it a crime to disclose Social Security numbers illustrates just how difficult it is to criminalize disclosing information about matters of public concern.[198] The disputed Virginia statute outlaws "intentionally communicating another individual's social security number to the general public."[199] The challenge came from, perhaps, an unlikely source: a privacy advocate, crusading to convince legislators that Social Security numbers were too easy to obtain from public court records.[200] The plaintiff operated a website designed to get the attention of public officials by publishing real estate transaction records that included property owners' unredacted Social Security numbers.[201] The Fourth Circuit found that the Social Security numbers were "integral" to the plaintiff's political advocacy message, stating that "[g]iven her criticism about how public records are managed, we cannot see how drawing attention to the problem by displaying those very documents could be considered unprotected speech."[202] The court's decision rested heavily on the public nature of the underlying real estate records; because government officials had made the records accessible, it would be "highly anomalous" to punish a member of the public for lawfully obtaining and sharing them.[203]

Notably, in each of these instances, courts have found doxing-type statutes to be content-based restrictions on speech that demand strict scrutiny.[204] The contemporary wave of anti-doxing measures, then, will start with a presumption of unconstitutionality and will be invalid unless narrowly tailored to serve a compelling government interest.

---

[196] *Id.* at 1019-20.
[197] *Id.* at 1020-21.
[198] *See* Ostergren v. Cuccinelli, 615 F.3d 263, 289 (4th Cir. 2010).
[199] *Id.* at 266.
[200] *Id.* at 268-69.
[201] *Id.* at 269.
[202] *Id.* at 271-72.
[203] *Id.* at 275 (quoting Fla. Star v. B.J.F., 491 U.S. 524, 535 (1989)). Rather than prosecuting the publisher, the court held, a more narrowly tailored remedy would be simply instructing court clerks to redact the Social Security numbers before releasing the real estate records. *Id.* at 286-87. *See also* Clay Calvert & Mirelis Torres, *Putting the Shock Value in First Amendment Jurisprudence: When Freedom for the Citizen-Journalist Watchdog Trumps the Right of Informational Privacy on the Internet*, 13 VAND. J. ENT. & TECH. L. 323, 328 (2011) (calling the Fourth Circuit's ruling "a remarkable victory for 'the shock value' in First Amendment jurisprudence" and also "a triumph for the watchdog role over government affairs that individual citizen-journalists—rather than professional reporters working for members of the institutional press—can play in a digital world").
[204] *See* Publius v. Boyer-Vine, 237 F. Supp. 3d 997, 1017 (E.D. Cal. 2017) (citing the *Sheehan*, *Brayshaw*, and *Ostergren* cases and observing that the truthful dissemination of lawful information already in the public domain cannot be prohibited unless the prohibition satisfies "exacting First Amendment scrutiny").

C. Legislative Overreach in Outlawing Doxing

There is considerable misalignment between what privacy advocates categorize as "doxing" on one hand versus what the first generation of statutes criminalizes—or what the Constitution allows legislatures to criminalize—on the other hand. Each of the "class of 2021" statutes contain some of the same infirmities that led courts in the aforecited *Ostergren*, *Sheehan*, *Brayshaw*, and *Publius* cases to rule in favor of constitutional challenges brought by speakers.

A concern common to all doxing statutes is that they expressly target what Professor Eugene Volokh refers to as "one-to-many" speech rather than one-to-one speech.[205] A message disseminated to a wide audience is harder to criminalize than a private message because the private message makes no contribution to the public discourse and is unambiguously a targeted attempt to affect a single recipient. Charging someone with a crime for "one-to-many" speech because a small subset of listeners *might* overreact to the speech in harmful ways means that the rest of the audience is also deprived of the information.[206] Moreover, criminalizing "one-to-many" online speech runs the added risk of subjecting a speaker to prosecution based on how it is interpreted by wholly unintended and unforeseen audience members, who may lack the contextual or cultural cues to properly understand the speaker's intent.[207]

The statutes likewise share the infirmity that none contemplates any exception for sharing information that is newsworthy, lawfully obtained, and already publicly accessible. It is impermissible to hold a speaker either civilly or criminally liable for disclosing legally obtained and newsworthy information that relates to matters of public concern.[208] While each doxing statute requires some culpable mental state that, if faithfully applied, would insulate journalists and commentators against prosecution for routine publishing activity, the statutes do not provide that the invidious purpose—threatening people, or provoking others to do so—must be the speaker's *only* purpose. To the contrary, it appears that culpability can attach if *any part* of the speaker's motivation is to bring about the

---

[205] *See generally* Eugene Volokh, *One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and "Cyberstalking*", 107 NW. U. L. REV. 731 (2013).

[206] *See* United States v. Carmichael, 326 F. Supp. 2d 1267, 1289 (M.D. Ala. 2004) (observing, in refusing to order a drug defendant to take down a website naming key witnesses and law enforcement agents in an intimidating way, that "the general rule in the case law is that speech that is broadcast to a broad audience is less likely to be a 'true threat,' not more").

[207] *See* P. Brooks Fuller, *Evaluating Intent in True Threats Cases: The Importance of Context in Analyzing Threatening Internet Messages*, 37 HASTINGS COMMC'NS. & ENT. L.J. 37, 76 (2015) ("Allegedly threatening communications through social media are able to reach unintended and innumerable recipients at the 'blink of an eye' even when the original speaker never intends that certain recipients receive the communications. . . . [V]iolent speech can reach notoriously dangerous like-minded groups, as well as the Internet version of passersby who, without the benefit of context, may legitimately fear that a dangerous true threat has been communicated.").

[208] *See* Romaine v. Kallinger, 537 A.2d 284, 298-99 (N.J. 1988) (finding that First Amendment would not permit imposing tort liability on author's disclosure of admittedly embarrassing facts about a newsworthy event that were gleaned from public court records).

prohibited harms.[209] This raises obvious concerns over a speaker's inability to obtain summary dismissal,[210] leaving the speaker to face a prolonged legal ordeal ending with a jury that may infer motive from circumstantial evidence.[211]

1. Overbreadth and Underinclusiveness

If the primary rationale for doxing statutes is to protect people against being tracked down at home and attacked, it will be quite difficult to justify prohibitions that have nothing to do with physical safety, such as criminalizing the disclosure of email addresses. While it asks too much to expect a person to change residences to avoid harassers, it is a simple matter to change one's personal email address or to block emails from unwelcome senders. To criminalize the disclosure of information that would incite others to, at most, send threatening emails rather than actually commit violence results in a "threat speech, once removed" regime, in which one speaker is legally responsible for others' choice of words.

Even less defensible is any statute that criminalizes revealing professional, rather than personal, contact information for public employees or their employers, as the laws in Kentucky and Oregon explicitly do. Government employees are expected to be available for public contact; indeed, it would be quite uncommon for a government employee's professional contact information to be inaccessible to the public. Professional contact information for government employees is so widely available, through such means as online agency directories, that charging someone with doxing for disclosing the information would pose serious questions both of causation and of blameworthiness. If doxing is considered to be a crime separate-and-apart from the underlying threat or harassment, something about the disclosure itself should be wrongful, and it would be quite difficult to argue that posting the governor's mailing address on Facebook is a malignant act worthy of criminalization. Privacy law recognizes that there can be no liability for invasion of privacy if the information disclosed

---

[209] *See* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 827-29 (2013) (noting that hackers' release of information about vulnerable computer systems is an example of speech that may have both invidious purposes but also salutary purposes, helping identify security weaknesses so they can be patched).

[210] *See, e.g.*, Slocum v. State, 757 So. 2d 1246, 1252 (Fla. Dist. Ct. App. 2000) ("Intent is usually a jury question.").

[211] *See, e.g.*, United States v. Hoffman, 806 F.2d 703, 708-09 (7th Cir. 1986) (affirming conviction of man who mailed letter to President Reagan stating, "Resign or You'll Get Your Brains Blown Out," and holding that jury could infer that the defendant "might very well have had a motive" to genuinely do harm to the president based on witness testimony that the defendant was displeased with Reagan for refusing to pardon the imprisoned leader of the Unification Church, to which the defendant belonged); *see also* Pumphrey v. State, 47 So. 156, 157 (Ala. 1908) ("Intent, we know being a state or condition of the mind, is rarely, if ever, susceptible of direct or positive proof, and must usually be inferred from the facts testified to by witnesses and the circumstances as developed by the evidence.").

was already widely accessible and if the individual to whom the information refers made no reasonable effort to keep the information private.[212]

The Florida, Kentucky, and Oklahoma statutes are plainly overbroad in extending criminal liability to the disclosure of information that is not merely identifiable on its face, but which can be used in combination with other information to make a match with an identifiable individual. The data-privacy community regularly expresses concern over the relative ease of "re-identifying" data even after efforts have been made to anonymize it, because of the possibility of cross-validating one data point with another.[213] None of the three statutes contains any knowledge requirement as to the possibility of re-identification. Without a knowledge or intent qualifier, even a person who removes personal identifiers before making a disclosure could be deemed a violator if—unbeknownst to the speaker—a data scientist in the audience is capable of reverse-engineering the redacted names.

The statutes that will be easiest to defend as narrowly tailored will be those that penalize threatening or inciting serious physical harm, since protecting people's physical safety is perhaps the archetypal compelling governmental interest.[214] By that regard, the Florida statute is uniquely vulnerable to overbreadth challenge. Florida law penalizes the disclosure of any information with the intent to incite a person to commit a crime against another person, without limitation as to the nature of the crime.[215] Even a minor nonviolent crime might satisfy the statute, so that a speaker might be guilty of inciting trespassing by posting, "[h]ere's the mayor's home address—walk right up on his front lawn and give him a piece of your mind."

Because five of the statutes (Arizona, Colorado, Florida, Kentucky, and Oklahoma) apply selectively to disclosures made by electronic means, they are susceptible to challenge as insufficiently tailored to address the harm they purport to remedy. Since the Supreme Court in *Reno* repudiated any notion of a stepped-down First Amendment for digital speech, a platform-specific carve-out for electronic media raises questions about underinclusiveness. Speech-restrictive statutes that are substantially underinclusive lack the precise tailoring that the First Amendment requires, because they restrict only a small subset of the speech

---

[212] *See* Interphase Garment Sols., LLC v. Fox Television Stations, Inc., 566 F. Supp. 2d 460, 467 (D. Md. 2008) (rejecting tort claim by executive who claimed that television news station's airing of his business dealings with a school district violated his right to privacy: "Any information that was already in the public domain when published cannot qualify as private facts. . . . [T]he invasion of privacy claim fails because public court documents are not private facts."); *see also* Bozzi v. City of Jersey City, 258 A.3d 1048, 1050 (N.J. 2021) (finding that city could not refuse to honor public records request for database of dog license holders on the grounds of personal privacy, because there is no reasonable expectation of privacy in dog ownership).

[213] *See* Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019, 5:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ (asserting that "research has shown for years how frighteningly easy it is to re-identify individuals within anonymous data sets").

[214] *See In re* Reps. Comm. for Freedom of the Press, 128 F. Supp. 3d 238, 241 (D. D.C. 2015) (recognizing an asserted threat to physical safety as the rare compelling governmental interest that can justify sealing records of a plea agreement, overriding the public's constitutional right of access).

[215] FLA. STAT. § 836.115(2)(a) (2022).

responsible for the harm they purport to address.[216] In a state with a platform-specific doxing statute, a speaker could freely use leaflets or flyers to post the very same information that, if shared electronically, would result in prison time. That is true even if the electronic disclosure was made to a limited universe of online viewers; for instance, a person in Oklahoma could lawfully hand out 100 pamphlets containing the name and workplace address of a police officer but risk prosecution for posting the same information on a "protected" Twitter account viewable to only 100 people.[217]

The same underinclusiveness argument could be applied to statutes that selectively protect only police officers or government officials against doxing, as in Colorado, Minnesota, and Oklahoma. As the Supreme Court has explained, an underinclusive statute is suspect because, when a statute only selectively addresses a problem, there is reason to doubt whether that purported problem is genuinely the motivation or whether it is an artifice concealing content discrimination.[218] Granting government employees special protection above-and-beyond what ordinary citizens receive raises obvious concerns: first, that government officials will regard criticism as "harassment" and seek to prosecute their critics; and second, that the people who benefit from the law include the very people in charge of making discretionary arrests and prosecution decisions.[219] If anything, the people singled out for protection in the Colorado, Minnesota, and Oklahoma statutes have a significantly diminished expectation of privacy regarding their contact information as compared with the general public.[220]

---

[216] Clay Calvert, *Legislating the First Amendment: A Trio of Recommendations for Lawmakers Targeting Free Expression*, 35 CARDOZO ARTS & ENT. L.J. 279, 294 (2017).

[217] *See* Adrienne Scheffey, Note, *Defining Intent in 165 Characters or Less: A Call for Clarity in the Intent Standard of True Threats After* Virginia v. Black, 69 U. MIAMI L. REV. 861, 867 n.42 (2015) ("Twitter allows for public or private (protected) Twitter accounts. Public accounts can be followed by anyone without approval (allowing for communication with any follower) and can be seen online by anyone, even those without Twitter accounts. Protected Twitter accounts require each person to be individually approved for communication and profile visibility.").

[218] *See* Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 802 (2011) ("Underinclusiveness raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint.").

[219] These statutes raise additional "tailoring" concerns because none specify that the threats or harassment incited against government employees must be motivated by their government employee status. In other words, online hostility directed toward someone because of a personal grievance, such as a broken romantic relationship, could be a crime—or not—depending on where that person works.

[220] *See* Int'l Fed'n of Pro. & Tech. Eng'rs v. Superior Ct., 165 P.3d 488, 493-94 (Cal. 2007) (ruling that salaries of law enforcement officers and other municipal employees were subject to disclosure as public records, even though non-government employees consider their personal finances to be confidential "[t]o the extent some public employees may expect their salaries to remain a private matter, that expectation is not a reasonable one . . . ."); Comm'n on Peace Officer Standards & Training v. Superior Ct., 165 P.3d 462, 473 (Cal. 2007) (holding that database of law enforcement officers' names, employers, and dates of hire was a public record and not subject to withholding on personal privacy grounds: "The public's legitimate interest in the identity and activities of peace officers is even greater than its interest in those of the average public servant.").

2. Lack of Requisite Culpable Mental State

Of all of the first-generation doxing statutes, the Florida formulation is the one that raises the most obvious constitutional concerns because it extends beyond directly inciting people to commit crimes and also applies, derivatively, to inciting others to incite criminal behavior.[221] While speakers can legitimately be held responsible for listeners that they intend to incite, the Florida statute suggests that liability can attach to "incitement-once-removed," holding speakers criminally liable for how other people share and characterize their speech—with no temporal limitation to satisfy the *Brandenburg* requirement of imminence. If the First Amendment protects advocacy up to the point that it crosses the line of a threat to commit violence or incitement for others to do so, then "incitement to incite" would seem to fall squarely within what the Constitution protects. Proving an intent to incite violence follows a well-trod path: under the *Brandenburg* standard, the speech must be both "directed to inciting or producing imminent lawless action" and "likely to incite or produce such action."[222] But criminalizing an intent to incite *incitement* could expose speakers to prosecution for speech short of the *Brandenburg* standard. Based on the face of the Florida statute, a speaker could be a violator in any of the following scenarios:

X intentionally furnishes information that could facilitate incitement to *Y*, knowing that *Y* has volatile propensities—even if *Y* does not engage in incitement until some far-removed future date or does not end up engaging in incitement at all;

X intentionally furnishes information to *Y* that could facilitate incitement, but *Y* was already intent on engaging in incitement and did not need the information and was not influenced by it; or

X intentionally furnishes information to *Y*, who then speaks to *Z* with intent to incite *Z*, even if *Y* does not share *X*'s information—or *Y does* share the information, but it has no effect on *Z*.[223]

Relatedly, the Colorado and Minnesota statutes lack the exacting mental state requirement that is typically regarded as necessary for a speech-punitive statute to be constitutional.[224] The Colorado and Minnesota statutes apply to a

---

[221] FLA. STAT. § 836.115(2) (2022).

[222] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

[223] In a detailed exploration of the constitutional constraints on criminalizing various types of crime-adjacent speech, Professor Susan W. Brenner analyzes congressional attempts to criminalize publishing the instructions for making bombs, and concludes, "The First Amendment does not permit Congress to outlaw the general dissemination of bomb making information when the natural consequence of that dissemination is that the information will be used for an unlawful purpose, i.e., to inflict injury and destruction upon persons and property."). Susan W. Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data Be Criminalized?*, 13 ALB. L.J. SCI. & TECH. 273, 350 (2003).

[224] *See* Buchhandler-Raphael, *supra* note 18, at 1701 ("Under contemporary criminal law, the default mens rea is typically recklessness, thus requiring a conscious disregard of a substantial and unjustifiable risk of harm."); M. Katherine Boychuk, *Are Stalking Laws Unconstitutionally Vague or Overbroad?*, 88 NW. U.L. REV. 769, 796 (1994) ("Generally, courts look more favorably on laws that specify offenders' specific intent because this narrows the scope of the statute.").

speaker who knows or "reasonably should know" of the existence of a serious threat, which is a mere negligence standard.[225] A statute with this formulation could be triggered by, for example, an article and photo on a newspaper's website that shows enhanced security outside the home of the county health department director in response to death threats. The news organization has done every act necessary to commit a crime in Colorado or Minnesota: furnished a photo of a public health employee's home, with at least a reasonable suspicion that people who have made death threats in the past are prone to make them again. Any statute allowing for conviction based on something less than a proven intent to cause harm would risk making criminals out of blameless speakers who merely foresee, but do not intend, that their speech will provoke hateful reactions.[226]

This is one reason that criminalizing the mere provision of information is so fraught. When a defendant like Anthony Elonis is prosecuted for threat speech, the speech itself must contain harm-causing elements of which the speaker is, at a minimum, aware.[227] But doxing statutes extend to the provision of harmless information—"this is the police chief's email address and cellphone number"—which becomes harmful only when weaponized volitionally by third parties over whom the speaker has no control. Because of that distance between the disclosure and the harm, proof of a culpable mental state beyond negligence should be understood as a constitutional imperative.

Only Arizona's statute contains the safety valve commonly found in more traditional harassment statutes—that the release of personal information constitutes a crime only if the disclosure serves "no legitimate purpose."[228] This

---

[225] *See* Papa Nick's Specialties, Inc. v. Harrod, 747 F. Supp. 1240, 1242 (N.D. Ohio 1990) (ruling that criminal liability under federal drug paraphernalia statute cannot constitutionally be premised on a mere negligence standard, that the defendant "reasonably should know" that the product he sold will be used for consuming drugs). In Daniels v. State, 448 S.E.2d 185, 188 (Ga. 1994), the Georgia Supreme Court decided that a defendant cannot constitutionally be convicted of the crime of wearing a mask in public based on proof that the wearer "reasonably should know" that wearing the mask will "threaten, intimidate, or provoke the apprehension of violence." Rather, the court explained, a criminal conviction typically requires at least a showing of "reckless disregard of consequences, or a heedless indifference to the rights and safety of others, and a reasonable foresight that injury would probably result." *Id.* (quoting *Bowers v. State*, 338 S.E.2d 457, 458 (Ga. 1985).

[226] In the illustrative recent case of People v. Ashley, 162 N.E.3d 200, 217 (Ill. 2020), the Illinois Supreme Court largely upheld that state's cyberstalking statute against constitutional challenge but struck down the portion of the statute that allowed for criminal prosecution based on a mere negligence standard. The court found that the statute was infirm to the extent that it penalized engaging in a course of conduct that the defendant "should know" will cause a reasonable person to fear specified harms. *Id.* at 209. *See also* Erin Coyle & Eric Robinson, *Chilling Journalism: Can Newsgathering Be Harassment or Stalking?*, 22 COMMC'N. L. & POL'Y 65, 88 (2017) ("To avoid the possibility of being applicable to newsgathering communications, laws should restrict harassment to speech or activities made with a 'purpose to harass another,' or for unlawful purposes, that are not protected by the state or federal constitutions.").

[227] *See* Elonis v. United States, 575 U.S. 723, 740 (2015) (interpreting federal threat-speech statute and stating that "[t]here is no dispute that the mental state requirement in [the statute] is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat").

[228] ARIZ. REV. STAT. § 13-2916(E)(3) (2022).

caveat should adequately protect a journalist or activist who publishes personal contact information in connection with legitimate news, commentary, or advocacy speech, even if the speaker is aware that some subset of the audience may be sufficiently angered to take vigilante action, and even if the disclosure takes place in the context of ongoing threats.[229] The other doxing statutes fail to explicitly carve out speech that serves a legitimate purpose, so that in those states, a speaker could be held criminally liable for speech that is primarily intended to serve a benign purpose.

The breadth of these statutes imposes a potentially chilling level of criminal exposure on publishers. Because the acts made criminal under doxing laws are themselves routine journalistic practices— acts that could be as run-of-the-mill as publishing the professional contact information of a government employee—the distinction between everyday journalism and a crime rests solely on mental state and not on any overt act. In jurisdictions other than Arizona, an arrest and indictment can be justified by alleging, circumstantially, that some small portion of the publisher's motive was to provoke volatile people, leaving the publisher to the mercy of a jury's mind-reading capabilities.

3. Selectively Protecting Law Enforcement Officers or Public Officials

Laws that selectively criminalize disclosing information about only public officials or people with sensitive government positions are questionably constitutional, because they uniquely protect a class of people whose contact information is of highest public interest – and whose responsibilities are understood to include accepting unwelcome speech. Colorado limits the protection of its doxing statute to people with particular government positions or their family members, Minnesota only to employees of law enforcement agencies or their families, and Oklahoma to law enforcement and elected or appointed "public official[s]."[230] However, First Amendment law fiercely protects the right to criticize public officials, even in harshest terms—including the right to wish violence upon them.[231] Likewise, First Amendment law recognizes that police officers are expected to absorb all manner of vitriol that would constitute

---

[229] *See* State v. Burkert, 174 A.3d 987, 1000 (N.J. 2017) (finding that New Jersey cyberharassment statute was unconstitutional because, among other defects, it lacked a limiting clause protecting speech that serves a "legitimate purpose")*; see also* State v. Fratzke, 446 N.W.2d 781, 783-84 (Iowa 1989) (holding that "constitutional safety valve" in Iowa's harassment law, excluding from its reach speech made with a "legitimate purpose," made the statute constitutional and foreclosed prosecuting a letter-writer who called a police officer a profane insult and wished him an early death).

[230] COLO. REV. STAT. § 18-9-313(1)(n) (2022); MINN. STAT. § 609.5151(2)(a) (2022); OKLA. STAT. tit. 21, § 1176(A) (2022).

[231] *See* Rankin v. McPherson, 483 U.S. 378, 381, 391-92 (1987) (finding that First Amendment protected public employee against being fired for workplace comment wishing that assassin's unsuccessful attempt on President Reagan's life had succeeded).

provocation to fight (if leveled at ordinary civilians) because of the sensitivity of their jobs and the volatile nature of their interactions with the public.[232]

For purposes of defamation law, which establishes a heightened burden to recover damages for false statements when the plaintiff is a public official or public figure, a police officer is generally recognized as a "public" plaintiff because of the inherently sensitive and important nature of police work.[233] The public has a well-recognized interest in whether police officers are qualified and adequately trained to do their jobs and whether they perform those jobs in a fair and nondiscriminatory way.[234] Since newsworthiness is regarded as defeating a claim for the public disclosure of private facts,[235] the burden to justify prosecuting a person who discloses information about a police officer who has been involved in a high-profile controversy would be quite demanding.

As two decades of experience with online hostility sadly demonstrates, government employees do not hold the monopoly on victimization. Athletes, television personalities, and journalists are frequent targets of hateful posts and messages.[236] There is no reason to believe that a person who is, for instance,

---

[232] *See* City of Houston v. Hill, 482 U.S. 451, 461 (1987) ("[T]he First Amendment protects a significant amount of verbal criticism and challenge directed at police officers."); *see also* Resek v. City of Huntington Beach, 41 Fed. App'x. 57, 59 (9th Cir. 2002) ("Along with good judgment, intelligence, alertness, and courage, the job of police officers requires a thick skin. Theirs is not a job for people whose feelings are easily hurt.").

[233] *See, e.g.*, Rotkiewicz v. Sadowsky, 730 N.E.2d 282, 287 (Mass. 2000) ("We conclude, because of the broad powers vested in police officers and the great potential for abuse of those powers, as well as police officers' high visibility within and impact on a community, that police officers, even patrol-level police officers such as the plaintiff, are 'public officials' for purposes of defamation."); *see also* Costello v. Ocean Cnty. Observer, 643 A.2d. 1012, 1021 (N.J. 1994) ("In New Jersey, courts have consistently found that police officers are public officials and thus have applied the actual-malice standard to police officers acting in their official capacities.").

[234] *See* Am. C.L. Union of Or., Inc. v. City of Eugene, 380 P.3d 281, 297-98 (Or. 2016) (stating that "the public interest in the transparency of government operations is particularly significant when it comes to the operation of its police departments and the review of allegations of officer misconduct. Every day we, the public, ask police officers to patrol our streets and sidewalks to protect us and to enforce our laws. Those officers carry weapons and have immense power.").

[235] *See* Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993) ("People who do not desire the limelight and do not deliberately choose a way of life or course of conduct calculated to thrust them into it nevertheless have no legal right to extinguish it if the experiences that have befallen them are newsworthy, even if they would prefer that those experiences be kept private."); *see also* Doe 2 v. Associated Press, 331 F.3d 417, 421-22 (4th Cir. 2003) (finding no actionable claim for public disclosure based on truthful news report of sentencing hearing at which sex-crime victim was identified: "[W]e cannot understand how the voluntary disclosure of information in an unrestricted, open courtroom setting could be anything but a matter of public interest.").

[236] *See* Wayne Sterling, *Sloane Stephens Says She Received More Than 2,000 Messages of 'Abuse and Anger' After US Open Defeat*, CABLE NEWS NETWORK (Sept. 6, 2021, 4:57 AM), https://www.cnn.com/2021/09/05/tennis/sloane-stephens-us-open-abuse-spt-intl/index.html (quoting U.S. professional tennis star, Sloane Stephens, on "exhausting" number of hateful social-media messages received after recent tournament loss, one of which read, "I promise to find you and destroy your leg so hard that you can't walk anymore"); *see also* Tyler McCarthy, *'Real Housewives' Star Lisa Rinna Defends Erika Jayne After Revealing She Gets Death Threats Online*, FOX NEWS (Aug. 22, 2021, 1:01 PM), https://www.foxnews.com/entertainment/real-housewives-lisa-rinna-defends-erika-jayne-death-threats (reporting that star of "Real Housewives" reality television series

elected to head the Oklahoma Department of Agriculture is more likely to receive threats, or more severely affected by threats, than a player on the University of Oklahoma football team who has a bad game. Yet the very same words would be treated as a crime—or not—depending on whether their target was the athlete or the commissioner of agriculture. Statutes that selectively criminalize only speech directed to government employees are unlikely to pass muster as adequately tailored to address the problem of doxing, as they would raise significant concern for selective enforcement against government critics.

The prosecution of a New Hampshire citizen gadfly for insults directed at a police officer on social media[237] provides an ominous preview of the type of cases that are likely to proliferate under "doxing-the-police" statutes. Robert Frese, a colorful small-town New Hampshire character habitually banned from local eateries for raiding their garbage bins for food, used the comment feature on the local newspaper's Facebook page to call the city's retiring police chief "the dirtiest cop I've ever met in my life."[238] In response, police arrested him under New Hampshire's criminal libel statute, one of just thirteen of these laws remaining on the books in the United States.[239] After more than two years of proceedings, Frese's case was argued in October 2021 before the U.S. Court of Appeals for the First Circuit, which is considering whether the criminal libel statute is unconstitutionally vague or overbroad.[240] It is doubtful that the former chief could even have mounted a successful civil defamation case over the Facebook post, as the statement is a classic hyperbolic statement of opinion about

---

received threatening social media messages after filing for divorce from her husband, a wealthy attorney facing accusations of embezzlement); *see also* Zac Ntim, *Piers Morgan Says Internet Trolls Threatened to Murder Him in Front of His Children Over Meghan Markle Row*, INSIDER (May 29, 2021, 4:44 AM), https://www.insider.com/piers-morgan-says-trolls-sent-death-threats-meghan-markle-row-2021-3 (quoting controversial British talk-show host who reported threatening social media messages, including some directed to his children, in apparent reaction to his unfavorable comments about members of the British royal family); *see also* Michael Dugandzic, *Charles Barkley Blasts Internet Trolls After Ohio State Player Received Death Threats*, BASKETBALL NETWORK (Mar. 20, 2021), https://www.basketballnetwork.net/charles-barkley-blasts-internet-trolls-after-ohio-state-player-received-death-threats/ (describing "gruesome messages, with numerous insults and even death threats" directed at Ohio State University basketball player after his team was upset in an NCAA postseason tournament game); *see also* Sarah Rense, *This Video of Men Reading Disgusting Tweets to Women Is Painful to Watch*, ESQUIRE (Apr. 26, 2016), https://www.esquire.com/sports/videos/a44351/female-sports-reporters-mean-tweets/ (describing widely circulated video in which prominent female sports journalists showed their Twitter messages to male volunteers and asked them to play-act reading the messages, many of which contained harsh profanity, misogynist name-calling, and wishes of violent death).

[237] *See* Frese v. MacDonald, 512 F. Supp. 3d 273, 279 (D.N.H. 2021).

[238] Todd Bookman, *Model Citizen? No. But Exeter Man Is at Center of First Amendment Dispute*, N.H. PUB. RADIO (Apr. 22, 2019, 7:19 AM), https://www.nhpr.org/nh-news/2019-04-22/model-citizen-no-but-exeter-man-is-at-center-of-first-amendment-dispute.

[239] *See* Thomas F. Harrison, *Jailed Over Facebook Taunts: Free-Speech Battle Hits 1st Circuit*, COURTHOUSE NEWS (Oct. 28, 2021), https://www.courthousenews.com/jailed-over-facebook-taunts-free-speech-battle-hits-1st-circuit/.

[240] *Id.*

a public figure, making it nearly impervious to a libel claim.[241] But there was no point in the chief expending personal resources to pursue a likely doomed civil claim when the criminal code meant that the police would pursue the claim for him at no charge. Regardless of whether Frese is ultimately vindicated, a prolonged legal battle carries its own financial and psychological costs and can inhibit journalists and activists from pursuing their government oversight role.[242]

V. CONCLUSION AND RECOMMENDATIONS

It is perhaps curious that, while U.S. anti-doxing statutes have received overwhelming bipartisan support and drawn little discernible opposition, free-speech advocates and technology companies have widely decried the enactment of a rigid doxing law in Hong Kong.[243] The justifications put forth for Hong Kong's statute echo those offered in the United States; one proponent told Hong Kong lawmakers, "We are talking about the disclosure of personal information of individuals including their family members and young children—these people have to live in fear and young children are scared as they go to school."[244] As described by Reuters, the new Hong Kong law largely mirrors those being proposed and enacted across the United States: it is illegal, without consent, to disclose "personal data . . . with an intent to cause specified harm or being reckless about the harm . . . includ[ing] harassment, threats, intimidation," and physical or psychological harm.[245] When the law was being debated, U.S.-based technology firms sounded the alarm that its enactment "could soon make Hong Kong an unsustainable place to do business" for fear of liability.[246] Of course, technology firms do not face the same risk of legal liability in the United States,

---

[241] *See* McDougal v. Fox News Network, LLC, 489 F. Supp. 3d 174, 182-84 (S.D.N.Y. 2020) (holding that former actress and model who gained prominence by naming President Trump as her paramour could not recover for a television commentator's figurative and hyperbolic remark that her acceptance of payment in exchange for silence constituted "a classic case of extortion").

[242] *See* Lexis-Olivier Ray, *Seven Months of Being Scared to Work: The City Attorney Charged Me with Committing a Questionable 'Crime' While Reporting*, L.A. TACO (Oct. 28, 2021), https://www.lataco.com/police-attack-reporter-crime-law/ (In his column for a Los Angeles culture blog, Ray describes how he "lived in fear" of reporting on the police for the seven months that he was facing a misdemeanor charge of "failing to disperse," imposed while he was covering an unruly public celebration after the Los Angeles Dodgers won the World Series: "As a result of my experiences, I took a break from working on certain projects and walked away from others altogether. I questioned my own ability to report on law enforcement and protests going forward safely.").

[243] *See* Pak Yiu, *Hong Kong Legislature Passes Controversial Anti-Doxxing Privacy Bill*, REUTERS (Sept. 29, 2021, 7:01 AM), https://www.reuters.com/world/asia-pacific/hong-kong-legislature-passes-controversial-anti-doxxing-privacy-bill-2021-09-29/.

[244] Kari Soo Lindberg, *Hong Kong Says Doxxing Law Alarming Tech Firms Strikes 'Balance*,*'* BLOOMBERG, https://www.bloomberg.com/news/articles/2021-07-20/hong-kong-to-debate-doxxing-law-that-alarms-tech-companies (July 21, 2021, 3:48 AM).

[245] Yiu, *supra* note 245.

[246] Robert Hart, *Anti-Doxxing Law Could Force Tech Giants Including Amazon, Google from Hong Kong, Industry Group Warn*s, FORBES (July 5, 2021, 10:55 AM), https://www.forbes.com/sites/roberthart/2021/07/05/anti-doxxing-law-could-force-tech-giants-including-amazon-google-from-hong-kong-industry-group-warns/?sh=7a5e76ed95d8.

due to the nearly impenetrable liability shield of the Communications Decency Act of 1996.[247] So the liability risk is entirely on the platform's users, who do not have nearly the same lobbying influence.

Policymakers should ask an existential question before enacting more doxing statutes: what is the perceived hole that the statute is intended to fill? If a doxing post is accompanied by a threat to do violence or an overt call for others to do so, as in the *Planned Parenthood* case,[248] then the post is already a crime, with or without the disclosure of information. And if the post is *not* accompanied by a threat to do violence or an overt call for others to do so, then it is likely to be constitutionally protected speech.

Federal and state laws already criminalize quite a bit of the speech that is popularly referred to under the umbrella term of "doxing." The Interstate Communications Statute makes it a felony to use electronic communication systems to transmit a threat to commit bodily harm.[249] The Interstate Stalking Statute makes it a felony to use any computer service to place someone in fear of death or serious injury, or to cause a person "substantial emotional distress," which goes beyond direct threats of violence.[250] An array of computer crime and anti-hacking statutes, including the Computer Fraud and Abuse Act (CFAA), make it a federal offense to gain unauthorized access to a computer system, such as obtaining embarrassing photos from a person's online "cloud" storage.[251] States buttress this regime of federal criminal codes with their own anti-harassment and "terroristic threat" statutes.[252] One 2017 study found statutes on the books in forty-seven states and the District of Columbia that criminalize the use of communication devices for purposes of harassment or stalking.[253] That serious acts of antisocial online behavior go unpunished likely speaks more to the unwillingness of police and prosecutors to use existing legal tools to pursue hard-

---

[247] 47 U.S.C. § 230.

[248] *See e.g.*, Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1086 (9th Cir. 2002) (en banc) (where the defendant creating "wanted"-style posters was a call for others to incite violence).

[249] 18 U.S.C. § 875(b). *See also* MacAllister, *supra* note 15, at 2470 (opining that the statute could have been used to prosecute "Gamergate" trolls who targeted video game developer Brianna Wu, among others, with graphically detailed online messages threatening violence).

[250] 18 U.S.C. § 2261(A)(2).

[251] *See* 18 U.S.C. §1030(a)(2)(C) (making it a crime to intentionally gain unauthorized access to any computer system or to exceed the bounds of authorized access). *See also* Laura M. Holson, *Hacker of Nude Photos of Jennifer Lawrence Gets 8 Months in Prison*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/arts/hack-jennifer-lawrence-guilty.html (reporting that the hacker who accessed actress Jennifer Lawrence's photo storage and disseminated intimate photos in a password "phishing" scheme was one of four people sentenced to prison in the scheme, after pleading guilty to violating the CFAA).

[252] *See* Susan W. Brenner & Megan Rehberg, "*Kiddie Crime?" The Utility of Criminal Law in Controlling Cyberbullying*, 8 FIRST AMEND. L. REV. 1, 62 n.255 (2009) (cataloging state threat statutes patterned after Model Penal Code Sec. 211.3).

[253] *See* Coyle & Robinson, *supra* note 228, at 70 n.31 (cataloging state statutes and noting that several were the subject of recent or ongoing constitutional challenges on the grounds of overbreadth).

to-solve cases involving anonymous online speakers than it does to a lack of statutory weaponry.[254]

Significantly, almost all of the contemporary wave of doxing statutes applies exclusively to online speech, and essentially all of the discourse surrounding doxing focuses on social media. As the Supreme Court recognized in the *Claiborne Hardware* case, advocacy on political issues can be heated and hyperbolic, and references to violence are not uncommon.[255] This is doubly so online, where overheated discourse often spirals into wishing death on one's perceived adversaries.[256] While the legal system is struggling to figure out how to categorize social media speech—is it more like a words blurted out at a political rally, or more like a newspaper column that is scripted and planned[257]—the reality is that people use social media spontaneously in loose and figurative ways to react to emotionally charged issues, without ever intending to commit or provoke real world violence.[258] Unlike the political protests and rallies where much of the Supreme Court's crime-adjacent speech doctrine took shape, online speech is capable of reaching unforeseen recipients isolated in time and place from the speaker.[259] For this reason, there is obvious peril in exposing online speakers to criminal liability for how the justice system anticipates that some especially unreasonable audience members are likely to respond.

First Amendment doctrine strongly disfavors what is known as the "heckler's veto," the principle that a speaker may be silenced or punished

---

[254] *See* Anna Merlan, *The Cops Don't Care About Violent Online Threats. What Do We Do Now?*, JEZEBEL (Jan. 29, 2015, 3:10 PM), https://jezebel.com/the-cops-dont-care-about-violent-online-threats-what-d-1682577343 (quoting Professor Citron on the failure of law enforcement agencies to prioritize online harassment prosecutions, "The problem often is that they often say, 'We're in the business of worrying about murder and terrorism, we don't enforce cyberstalking laws.'").

[255] *See* NAACP v. Claiborne Hardware Co., 458 U.S. 886, 928 (1982).

[256] *See* Dave Levinthal, *First Came the Drudge Link. Then the Death Threats.*, DAILY BEAST, https://www.thedailybeast.com/first-came-the-drudge-link-then-the-death-threats (Apr. 13, 2017, 3:53 PM) (reporting that Democratic appointee to the Federal Elections Commission was targeted by a deceptive headline in a widely read conservative blog, accusing her of seeking federal regulation of internet content: "[I]n a sign of how toxic American politics have become, it spawned unbridled ugliness, including death threats that have drawn the attention of law enforcement.").

[257] *See generally* LoMonte, *supra* note 131 (urging that courts, educational institutions, and employers recognize the casualness of online speech and its frequent use of exaggeration or irony, and avoid assigning literal weight to a medium known for inside jokes and other speech that is uniquely susceptible to cultural miscommunication).

[258] *See* State v. Taylor, 841 S.E.2d 776, 827 (N.C. Ct. App. 2020) ("It is general knowledge that Facebook, like many other sides on the Internet, often serves as a place where people air their grievances. Further, it is not uncommon for some of the posts on Facebook and other Internet platforms to be 'over the top,' exaggeratedly offensive, threatening, or irrational."); *see also* Enrique A. Monagas & Carlos E. Monagas, *Prosecuting Threats in the Age of Social Media*, 36 N. ILL. U. L. REV. 57, 77 (2016) ("People's sense of what is threatening has yet to catch up with technology. They fail to appreciate their lack of context and do not have the sense to seek it out. Just because words can be misconstrued online does not mean that the default position should be that the speaker is punished for someone else's misinterpretation.").

[259] *See* Sweeny, *supra* note 113, at 599 (noting that social media does not neatly fit into the traditional First Amendment analysis for incitement speech, because "[t]he audience is not contained in a room; they come and go and the speaker usually cannot see them or know how many people have even heard them.").

because of the anticipated violent overreactions of some audience members.[260] To let the most violent fringe of listeners set the standard for what is legal to say online would be the ultimate validation of the heckler's veto, which is why liability cannot attach—as it does in Colorado and Minnesota—merely because some radical fringe of readers predictably will escalate the disclosure of unflattering information into online threats. As Professor Volokh has written, "Much advocacy of crime is protected because of its potential value to noncriminal listeners, despite its tendency to cause crime by some other listeners."[261]

A. Putting Journalists and Activists in the Crosshairs

On July 4, 2021, John Thompson, a Minnesota state legislator, was pulled over by St. Paul police and cited for driving without a front license plate.[262] That seemingly minor traffic stop opened up Thompson's background to scrutiny because he presented an out-of-state driver's license to police, and then gave police a Minnesota address that is outside his legislative district, raising questions about his eligibility to serve.[263] The questions deepened after it came to light that Thompson had been the subject of a string of domestic violence complaints a decade ago, though none resulted in a criminal conviction.[264] Whether an elected official has lied about being qualified to hold office is a matter of legitimate public concern, even if that means publishing information that the official would prefer remained secret.[265]

At times, news reporting, commentary, and political advocacy involve using personal information of the sort that might fall within a broadly worded doxing prohibition. For example, the case of a St. Louis couple who pointed firearms at Black Lives Matter protesters marching past their house on the way to picket the mayor's home became a subject of international curiosity.[266] Nothing about the event was private; the couple openly brandished weapons in a

---

[260] Forsyth Cnty. v. Nationalist Movement, 505 U.S. 123, 134, 140 (1992) ("Listeners' reaction to speech is not a content-neutral basis for regulation."). *See* Reno v. Am. C.L. Union, 521 U.S. 844, 880 (1997) (finding that law criminalizing online speech harmful to minors would confer "heckler's veto" on any would-be censor who could cause a website to be shut down simply by attesting that a teenager would be viewing the site).

[261] Eugene Volokh, *The "Speech Integral to Criminal Conduct" Exception*, 101 CORNELL L. REV. 981, 1002 (2016).

[262] Theo Keith, *Questions Swirl Over St. Paul Lawmaker's Residency After Traffic Stop*, FOX9 (July 12, 2021, 7:36 PM), https://www.fox9.com/news/questions-swirl-over-st-paul-lawmakers-residency-after-traffic-stop.

[263] *Id.*

[264] *Walz, DFLers Call On Rep. John Thompson To Resign Following Allegations Of Domestic Violence*, CBS MINN. (July 17, 2021, 9:18 PM), https://minnesota.cbslocal.com/2021/07/17/walz-dflers-call-on-rep-john-thompson-to-resign-following-allegations-of-domestic-violence/.

[265] *See id.* (stating that Thompson took advantage of an option in Minnesota law to withhold his home address from publicly accessible documents when he filed qualifying papers to run for legislature).

[266] *See* Jessica Lussenhop, *Mark and Patricia McCloskey: What Really Went On in St Louis That Day?*, BRIT. BROAD. CO. NEWS (Aug. 25, 2020), https://www.bbc.com/news/election-us-2020-53891184.

confrontation recorded by photographers, and were later criminally charged (though not prosecuted).[267] News coverage of the event necessarily included depicting where the couple, Mark and Patricia McCloskey, lived in relation to the mayor's home, and how close the march did or did not get to their house. Both the McCloskey family and the prosecutor who initially brought charges reported receiving multiple death threats following the widely publicized episode.[268] In such a volatile environment, it is implausible that anyone publishing photos of the McCloskeys or a description of where they live would be unable to foresee further threats. Yet the ability to accurately describe the scene of a nationally publicized news event manifestly serves the public's interest.

Josh Hawley, a polarizing member of the U.S. Senate from Missouri, found his residency to be a matter of public interest and debate, when it was disclosed that he used his sister's Missouri home as his voting address, raising questions about whether he genuinely resides in the state he represents.[269] This was the second time that Hawley, also a former Missouri attorney general, faced questions about whether he was voting in a location that was not his legal residence.[270] After the most recent incidence came to light, both Hawley and his sister reported that they had faced threats,[271] including one credible enough to result in an arrest and prosecution.[272] In February 2021, Hawley's wife initiated criminal charges against a protest leader who organized a demonstration outside the family's suburban Virginia home, even though police had concluded that no charges were warranted, and the demonstration consisted largely of chanting and sign-waving on public streets and sidewalks.[273] Providing documents, or links to

---

[267] *Id.*

[268] *See* Kim Bell, *'I'd do it all again,' says armed lawyer who confronted St. Louis protesters,* ST. LOUIS POST-DISPATCH (July 17, 2020), https://www.stltoday.com/news/local/crime-and-courts/i-d-do-it-all-again-says-armed-lawyer-who-confronted-st-louis-protesters/article_e4b5d080-62ec-51e1-85e8-3d8c909730e5.html (reporting that McCloskey family has been "deluged with threats" following the confrontation at their house); CBS News, *St. Louis prosecutor facing relentless resistance as she works to reform justice system*, 60 MIN. OVERTIME, https://www.cbsnews.com/news/kim-gardner-st-louis-prosecutor-60-minutes-2021-03-11/ ("Kim Gardner has endured death threats, racial slurs and the relentless opposition of the police union as she tries to keep her election promise and remake the justice system.").

[269] *See* Bryan Lowry, *Josh Hawley, Who Owns a House in Virginia, Uses Sister's Home as Missouri Address*, K.C. STAR (Nov. 19, 2020, 8:33 AM), https://www.kansascity.com/news/politics-government/article247260219.html.

[270] *See Hawley's Vote in Boone County Raises Questions on Residency*, ASSOCIATED PRESS (Aug. 15, 2017), https://apnews.com/article/ce7a36dc20674f7083f739e1c2a96cb6 (reporting that Missouri attorney general, Josh Hawley, cast a vote in rural Boone County, Mo., despite a state statute requiring the attorney general to live in the seat of government, Jefferson City).

[271] *See* Bryan Lowry, *Police Investigate Alleged Harassment of Josh Hawley's Sister in Springfield*, K.C. STAR (June 26, 2021, 10:54 AM), https://www.kansascity.com/news/politics-government/article252373763.html.

[272] *Man Given Time Served for Threatening Missouri Senator*, ASSOCIATED PRESS (July 23, 2020), https://apnews.com/article/u-s-news-josh-hawley-michael-brown-7b1cfb6cc91b7b215afb46c53714bec0.

[273] *See* Daniel Desrochers, *Virginia District Court Judge Dismisses Complaint Against Protester at Hawley's Home*, MCCLATCHY NEWS SERV. (Aug. 24, 2021, 9:16 AM), https://www.mcclatchydc.com/news/politics-government/article253690018.html.

documents, that disclose an elected official's address is a standard journalistic practice if the residence is a matter of public controversy—and indeed, disclosing the address might be an effective journalistic technique for eliciting further information from people in the neighborhood who can attest to whether the elected official genuinely lives in the area. But if a blogger or commentator disclosed a senator's home address, knowing that the senator had a history of receiving threats, and the senator then received further threats, authorities might have the necessary ingredients to initiate a doxing prosecution.

It is not universally accepted that protesting outside a prominent person's home to express outrage with the person's behavior is inherently a malicious act that should be punishable as a crime, so long as the protest is conducted nonviolently and without breaking trespass laws. For example, Supreme Court Justice Brett Kavanaugh faced protests outside his suburban Washington, D.C., home in September 2021 after the Court refused to block implementation of a restrictive Texas anti-abortion law.[274] The sign-waving demonstrators remained in a public street, and there is no indication that any laws were broken.[275] If the protest itself is not a crime, then equipping people with information about where to protest, even with the hope and intent that protesters will act on the information, likewise cannot be a crime. Since doxing is largely a derivative offense—that is, it depends on proof of a connection between disclosing the information and criminal behavior by others—doxing necessarily cannot be a crime if the anticipated or intended consequence of the disclosure is not a crime. Unless the speaker accompanies disclosure of the address with a direct instruction to commit criminal wrongdoing that is likely to provoke an imminent response (i.e., "There's gasoline and matches in the tool shed, burn that house to the ground right now," when directed to a mob already gathering nearby), there will be no easy way for the legal system to distinguish between the speaker who intends to incite a peaceful protest and the speaker who intends to incite arson. If the post *does* instruct an angry mob to commit arson, then it is legally punishable regardless of whether it also contains a "dox." That is to say, disclosing the address is really not the harm-causing element of the sentence. Particularly in the case of people whose addresses are readily publicly available, it is equally harmful to say, "I instruct you to burn Smith's office immediately," or "I instruct you to burn Smith's office at 111 Main Street immediately." But, although the statements are equally harmful, only the latter would violate doxing laws.

As the Supreme Court has said, "[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards."[276] Any statute purporting to make it a crime to distribute lawfully obtained information, particularly if the information pertains to people whose conduct is a matter of public concern, will face deserving skepticism if challenged constitutionally. After the Supreme Court issued a string of rulings during the 1970s and 1980s

---

[274] Alejandro Alvarez, *Abortion-Rights Advocates March on Kavanaugh's Chevy Chase Home*, WTOP (Sept. 14, 2021, 4:51 AM), https://wtop.com/gallery/montgomery-county/abortion-rights-advocates-march-on-kavanaughs-chevy-chase-home/.
[275] *See id.*
[276] Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 102 (1979).

finding that the First Amendment overrode laws penalizing the publication of lawfully obtained news, commentators widely declared that the tort of public disclosure of private facts was on its deathbed, irreconcilable with prevailing constitutional doctrine.[277] Judge Posner, taking stock of where privacy law stood at the Supreme Court as of the early 1990s, wrote, "The Court must believe that the First Amendment greatly circumscribes the right even of a private figure to obtain damages for the publication of newsworthy facts about him, even when they are facts of a kind that people want very much to conceal."[278] Unless very narrowly drafted, doxing laws run the risk of becoming "publication of not-especially-private-facts" proscriptions, destined for the same fate as now-invalidated prohibitions against publishing crime victims' names.

That lawmakers feel compelled to respond to antisocial online behavior is understandable. There is no disputing that the internet, in particular social media, is awash in malignant speech by people who are either bent on inflicting distress or simply indifferent to the consequences of their behavior. In the words of author and commentator, Roxane Gay, a frequent target for racist and anti-gay trolling on Twitter, "Every harm is treated as trauma. Vulnerability and difference are weaponized. People assume the worst intentions. Bad-faith arguments abound, presented with righteous bluster. And these are the more reasonable online arguments."[279]

Undeniably, political extremism in our country can be disturbingly confrontational and violent, as we saw on the streets of Charlottesville, Virginia, when a murderous neo-Nazi drove into a crowd of racial justice protesters and killed thirty-two-year-old Heather Heyer.[280] Advocates for the rights of women and people of color are, understandably, especially frustrated that it is impossible to hold social media companies and other website hosts legally responsible for harassing posts by third-party users because of the near-ironclad immunity protection of Section 230 of the Communications Decency Act.[281] The frustration

---

[277] *See* Jurata, *supra* note 62, at 508-09 (citing scholarly consensus in recent years that "declared the tort to be ineffective or on the verge of collapse" as a result of the courts' embrace of the newsworthiness defense).

[278] Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993).

[279] Roxane Gay, *Why People Are So Awful Online*, N.Y. TIMES (July 17, 2021), https://www.nytimes.com/2021/07/17/opinion/culture/social-media-cancel-culture-roxane-gay.html.

[280] *See* Paul Duggan & Justin Jouvenal, *Neo-Nazi Sympathizer Pleads Guilty to Federal Hate Crimes for Plowing Car Into Crowd of Protesters at Charlottesville Rally*, WASH. POST (Apr. 1, 2019, 2:19 PM), https://www.washingtonpost.com/local/public-safety/neo-nazi-sympathizer-pleads-guilty-to-federal-hate-crimes-for-plowing-car-into-crowd-of-protesters-at-unite-the-right-rally-in-charlottesville/2019/03/27/2b947c32-50ab-11e9-8d28-f5149e5a2fda_story.html.

[281] *See* Leonard, *supra* note 17, at 86 ("Section 230, as it currently stands, has abandoned the victims of cyber violence and harassment. Women, particularly young women, are often targets of online harassment that discourages victims from participating in online forums and leaves portions of the internet feeling like a regressive boys' club."). Author Danielle Keats Citron is a leading critic of the breadth of immunity afforded to websites and social media platforms, contending that courts have afforded it an unduly broad interpretation that leaves victimized people without practical recourse against tormentors who hide behind anonymity. *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE

is compounded by halfhearted or ineffectual self-policing by platforms that host third-party content whose proprietors do not always promptly and consistently enforce their own standards that, on paper, prohibit the worst excesses associated with doxing.[282]

But before more jurisdictions pursue criminal penalties for doxing, it is worth asking the following questions: would police and prosecutors *really* use an arsenal of new criminal penalties to bring the most extreme online trolls to justice—or would the penalties instead primarily result in silencing commentators and activists who criticize law enforcement?

The fact that the first generation of government responses to doxing has been to selectively protect only government employees is a foreboding sign for how, and against whom, these laws might be enforced. There is obvious invitation for abuse when the same people protected by the statutes—police officers—are also those with discretion to enforce them. Many police officers are reputation-conscious about how they are portrayed online and at times will cross the line of propriety in an effort to silence critics.[283] As a practical matter, the worst-of-the-worst purveyors of digital slime—many of whom are not even in the United States[284]—are not the most likely targets for police and prosecutors to pursue; U.S.-based journalists and activists are much easier to find and much easier to bring into court. It is not at all implausible that the same police officers

---

L.J. 1870, 1943 (2019) ("[T]he overbroad interpretation of § 230 has given content platforms a free pass to ignore destructive sexual-privacy invasions, to repost illegal material knowingly and deliberately, and to solicit sexual-privacy invasions while ensuring that abusers cannot be identified."). An especially heartbreaking case unfolded in the early days of ubiquitous internet access, when an Oregon woman, Cecilia Barnes, sued digital media company, Yahoo!, Inc., for hosting a fake profile page created by her ex-boyfriend, purporting to be Barnes soliciting men for sex and using her real home and work addresses. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009). A federal appeals court found that Yahoo! could not be held liable in tort, even though the profile remained visible for more than a month after Barnes complained, because of the immunity afforded by virtue of 47 U.S.C. § 230(c)(1). *Id.* at 1103.

[282] *See* Homchick, *supra* note 12, at 1329 (stating that Twitter and other websites "technically have policies that prohibit doxing" but do not always enforce their own policies).

[283] *See* Michael Safi et al., *'I'm Getting Shot': Attacks on Journalists Surge in US Protests*, THE GUARDIAN (June 5, 2020, 8:03 AM), https://www.theguardian.com/media/2020/jun/05/im-getting-shot-attacks-on-journalists-surge-in-us-protests (documenting 148 attacks on U.S. journalists by police at the scene of protests spawned by the May 2020 police killing of George Floyd in Minneapolis, including numerous instances in which police gassed, beat, or shot rubber bullets at people they knew to be news reporters).

[284] *See* Alexa Lardieri, *Russia Still Largest Driver of Disinformation on Social Media, Facebook Report Finds*, U.S. NEWS & WORLD REP. (May 26, 2021, 2:44 PM), https://www.usnews.com/news/politics/articles/2021-05-26/russia-still-largest-driver-of-disinformation-on-social-media-facebook-report-finds (reporting on release of self-study by Facebook, which "has uncovered disinformation campaigns in more than 50 countries since 2017," with Russia identified as the leading source); *see also* Craig Silverman & Lawrence Alexander, *How Teens in the Balkans Are Duping Trump Supporters with Fake News*, BUZZFEED NEWS (Nov. 3, 2016, 6:02 PM), https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo#.nfGBdzv3rN (describing "digital gold rush" in the former Yugoslav Republic of Macedonia, where purveyors of "fake news" maintained a profitable cottage industry of well-trafficked websites spreading fabrications calculated to be socially shareable by enthusiasts of then-candidate Donald Trump).

who spent much of 2020 intentionally beating, gassing, and shooting rubber bullets at journalists and activists with little apparent accountability,[285] might also train their enforcement sights on those same antagonists.

It is especially parlous to equip law enforcement agencies with a new tool to arrest their critics based on speech when the Supreme Court has just made it even harder to hold police accountable for ill-motivated arrests.[286] The takeaway from the Court's 2019 ruling in *Nieves v. Bartlett* is that probable cause for arrest on any charge will be fatal to bringing a retaliatory arrest claim under the First Amendment.[287] That means an officer in a state with a broad anti-doxing law, who is angry that his name was published in the press or on social media, could drag the publisher to jail and suffer no legal consequences—even if the true motive was retaliatory.

There is already powerful anecdotal evidence that some law enforcement officials are disposed to use their arrest authority to silence critics. In Texas, police working for the City of Laredo used a seldom-enforced statute that criminalizes the misuse of government information, which was intended to penalize bid-rigging, to arrest a citizen-journalist with a loyal Facebook following whose blog posts were unflattering to the police department.[288] In

---

[285] *See* Mollie Simon, *Few Cops We Found Using Force on George Floyd Protesters Are Known to Have Faced Discipline*, PROPUBLICA (June 17, 2021, 1:45 PM), https://www.propublica.org/article/few-cops-we-found-using-force-on-george-floyd-protesters-are-known-to-have-faced-discipline (reporting results of survey of dozens of law enforcement agencies that showed, despite hundreds of documented instances of police tear-gassing or otherwise using force to suppress nonviolent and nonthreatening protests during 2020, only ten officers have faced any documentable discipline). During 2020-21, as cities across the United States roiled with resentment over the unjustified use of deadly force against Black people, police attacks on demonstrators and bystanders became so commonplace that courts were forced to issue injunctions in both Minneapolis and Portland, two epicenters of protest, instructing police to cease retaliatory arrests and violence targeting journalists, legal observers, and nonviolent protesters. *See* Index Newspapers LLC v. City of Portland, 480 F. Supp. 3d 1120, 1155-57 (D. Or. 2020), *aff'd*, 977 F.3d 817 (9th Cir. 2020) (enjoining federal law enforcement agencies from arresting, using force against, or otherwise interfering with journalists and legal observers at the scene of racial justice protests); Woodstock v. City of Portland, No. 3:20-cv-1035-SI, 2020 WL 3621179 (D. Or. July 2, 2020) (issuing temporary restraining order against city and state law enforcement personnel in Portland, based on testimony that police arrested three journalists and repeatedly threatened others with arrest merely for remaining on the scene of protests, and used force against an ACLU legal observer); Goyette v. City of Minneapolis, 338 F.R.D. 109 (D. Minn. 2021) (entering temporary restraining order against Minneapolis police accused of shooting journalists with rubber bullets, in defiance of orders from Minnesota's governor).

[286] *See* Michael G. Mills, Note, *The Death of Retaliatory Arrest Claims: The Supreme Court's Attempt to Kill Retaliatory Arrest Claims in* Nieves v. Bartlett, 105 CORNELL L. REV. 2059, 2078-79 (2020) (critiquing Court's 2019 ruling, which affirmed qualified immunity protection for police who arrested a man for interjecting his comments during an arrest, even though there was evidence that officers were punishing him for the content of speech).

[287] Nieves v. Bartlett, 139 S. Ct. 1715, 1728 (2019).

[288] *See* Derek Hawkins, *Popular Texas Blogger Scooped Police on a Story. They Charged Her with 2 Felonies, Searched Her Phone Records.*, WASH. POST (Dec. 22, 2017, 6:09 AM), https://www.washingtonpost.com/news/morning-mix/wp/2017/12/22/popular-texas-blogger-scooped-police-on-a-story-so-they-charged-her-with-2-felonies/ (stating that amateur journalist with

Nutley, New Jersey, a police officer brought cyber harassment charges against five Black Lives Matter protesters, all of them twenty-one or younger, who posted the officer's photo on Twitter, asking whether anyone knew the officer's name.[289] The officer claimed that the tweet of his photo made him fear for his safety and the safety of his family, though a judge ultimately dismissed the charges.[290]

Officers are already exhibiting a propensity to use the civil justice system to silence and retaliate against their critics. In Cincinnati, a police officer suing under the protection of anonymity has been bombarding his online critics with defamation suits over Facebook posts publicizing both the history of excessive force complaints against him and allegations that he used a hand gesture indicative of white supremacy.[291] An Ohio police union leader supportive of the unnamed officer told his Facebook followers that police everywhere would be taking more aggressive tactics against their online critics. "These parties need to be dealt with aggressively and publicly. To be blunt they need to be sued every time they sneeze! When you mess with us, we will mess with you should be our message."[292] A prominent leader in the Black Lives Matter movement, author and educator DeRay Mckesson, has spent five years defending himself against a liability suit brought by a Baton Rouge police officer injured during a rowdy protest that Mckesson helped organize.[293] The Fifth Circuit found that the officer, who was hit in the head with a rock allegedly thrown by a demonstrator, could proceed against Mckesson on a theory that he negligently brought about the injury by causing the protesters to unlawfully obstruct a roadway in front of the police station.[294] The Supreme Court threw out the decision on a state law technicality without addressing the merits of the theory,[295] but the underlying

---

80,000 Facebook followers was arrested and charged under obscure "misuse of official information" statute after she published information about the suicide of a federal agent that she obtained from a police department source, which she and her lawyers called retaliatory for her unflattering coverage). A 2-1 panel of the Fifth Circuit ruled in November 2021 that police so obviously violated Villarreal's constitutional rights that they could not take advantage of qualified immunity to avoid liability for civil damages. Villarreal v. City of Laredo, 17 F.4th 532, 540 (5th Cir. 2021).

[289] Kaitlyn Kanzler, *First Amendment Lawsuit Filed Against Nutley Cop*, S. BERGENITE, Feb. 25, 2021, at B4.

[290] *Id.*

[291] Nick Swartsell, *Cincinnati Police Officer Sues for Defamation Over Protest Posts on Social Media*, CITYBEAT (Aug. 11, 2020, 3:06 PM), https://www.citybeat.com/news/blog/21142781/cincinnati-police-officer-sues-for-defamation-over-protest-posts-on-social-media; *see also* M.R. v. Niesen, No. C-200302, 2020 WL 5406791 (Ohio Ct. App. Sept. 9, 2020) (declining appellate review of trial court's temporary restraining order that directed the defendants, four critics of the pseudonymous officer, to refrain from disseminating identifiable information about the officer).

[292] Swartsell, *supra* note 292.

[293] Marissa J. Lang, *A Police Officer Sued a Black Lives Matter Protester for Violence He Didn't Commit. What's Next Has Free-Speech Advocates Worried.*, WASH. POST (Dec. 13, 2019, 2:39 PM), https://www.washingtonpost.com/local/a-police-officer-sued-a-black-lives-matter-protester-for-violence-he-didnt-commit-whats-next-has-free-speech-advocates-worried/2019/12/13/f02cd082-1d09-11ea-b4c1-fd0d91b60d9e_story.html.

[294] Doe v. Mckesson, 945 F.3d 818, 827 (5th Cir. 2019), *rev'd*, 141 S. Ct. 48 (2020).

[295] Mckesson v. Doe, 141 S. Ct. 48, 51 (2020).

case was left alive. Howard University scholar Tasmin Motala criticized the legal standard the Fifth Circuit embraced—which would leave protest organizers vulnerable to civil suits for any "foreseeable" damage caused by people they have no control over—if any of the protesters so much as violate a traffic law.[296]

> [The case] opens the door to unfettered liability against protesters, of which Black and racial justice protesters will bear the brunt. . . . The recent wave of protests against racial injustice and ensuing police violence has made clear that law enforcement, legislators, and even judges do not apply the right to protest in a race-neutral manner.[297]

If legislators issue police and prosecutors a new set of anti-doxing tools that encourages them to sue or prosecute people for online harassment—in particular, if that speech is directed to law enforcement agents or public officials—it is farfetched to expect that they will use their new tools primarily to protect vulnerable doxing victims whose anonymous online aggressors are hard to find. It is far more likely that this new weapon will be pointed at easy-to-find antagonists, such as Texas citizen journalist Priscilla Villarreal, whose criticism of police might cause officers to assert that they fear violence from people incited by Villarreal's unflattering commentary.

B. Narrower and Less Speech-Restrictive Remedies Exist

Harassment and threat laws already exist to penalize people who cross the line from disclosing information to actually acting on the information. Some behavior that is called doxing already falls under those prohibitions and can be penalized. As seen in the Seventh Circuit's *Turner* case,[298] police and prosecutors have effective tools to pursue people who disclose information about targeted individuals and couple that disclosure with advocacy of violence. The question naturally arises: if the criminal justice system already punishes people like Harold Turner, who used a blog to encourage fellow gun enthusiasts to assassinate specific federal judges,[299] then what is the additional set of conduct for which doxing statutes are intended? Either these statutes are redundant, because they overlap with existing criminal codes, or they criminalize speech

---

[296] *See generally* Tasnim Motala, *'Foreseeable Violence' & Black Lives Matter: How* Mckesson *Can Stifle a Movement*, 73 STAN. L. REV. ONLINE 61 (2020), https://www.stanfordlawreview.org/online/forseeable-violence-black-lives-matter/.
[297] *Id.* at 61-62.
[298] *See* United States v. Turner, 720 F.3d 411, 420 (2d Cir. 2013) (affirming conviction for online threats to kill federal judges under 18 U.S.C. § 115(a)(1)(B), which contains both objective and subjective standards that ensure only a person who has directed a threat toward a judge with the intent to retaliate or to interfere with the performance of judicial duties will be convicted).
[299] *Id.* at 415.

other than threats, incitement, or solicitation—essentially all of which is constitutionally protected.

The needs of an informed society require narrow specificity in any law that penalizes disclosing information that facilitates crime. Consider, for example, a television station's coverage from the scene of a newsworthy crime (let's say a drive-by shooting attributed to a gang rivalry). The news might well air footage of neighborhood residents filling the streets, so it can depict the community's outraged reaction to the crime or to dramatize the brazenness of a shooting on a busy street full of witnesses. Even if a person complicit in the shooting identified a witness from the broadcast and threatened her (by saying, for example, "If you tell the cops what you saw, I'll kill you"), no one would seriously argue that the television broadcaster has committed a crime. This is so even if the broadcaster is aware that people who are witnesses to violent gang crimes are likely targets of retaliation. We readily recognize that the television news broadcast is not punishable because it has a legitimate nonthreatening purpose, and also because the broadcaster had no intent to bring about the threat. These two common sense elements—the lack of any legitimate communicative purpose, coupled with an intent to produce a specific unlawful result—are not reliably present in this first generation of doxing statutes.

One bright-line solution would be to tailor doxing statutes to protect only the subset of information that is universally understood to be affirmatively confidential under freedom-of-information (FOI) law: Social Security numbers, bank account numbers, and other such information that could be weaponized by identity thieves.[300] Because legislators and courts have already determined that such intensely personal information with obvious potential for exploitation is not a matter of public record, penalizing their intentional disclosure with the sole purpose of causing harm[301] does not meaningfully deprive the public of information that would otherwise be available. But when information is widely accessible to the public under FOI law, such as the contact information of government employees, it strains well-established First Amendment standards to make disclosing it a crime, even if the disclosure is highly unwelcome.[302] The

---

[300] *See* Tex. Comptroller of Pub. Accts v. Att'y Gen., 354 S.W.3d 336, 345 (Tex. 2010) (stating that employee birthdates are subject to withholding from public records because of the possibility that they could be combined with other information to facilitate identity crimes); Del. Cnty. v. Schaefer *ex rel.* Phila. Inquirer, 45 A.3d 1149, 1157 (Pa. Commw. Ct. 2012) (making same point under Pennsylvania's Right-to-Know Law); *see also* Thomas v. Smith, 882 So. 2d 1037, 1045 (Fla. Dist. Ct. App. 2004) (applying Florida statutory exemption that makes Social Security numbers confidential when contained in otherwise-public records, on the grounds that those numbers can be misused to gain access to individuals' medical, financial and other confidential records).

[301] By cabining liability to people who act with the sole purpose of doing harm, the blogger in *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010), who disclosed Social Security numbers for the purpose of creating awareness about a privacy risk, would remain insulated from prosecution.

[302] *See* Sherman v. U.S. Dep't. of Army, 244 F.3d 357, 366 (5th Cir. 2001) (finding that Social Security numbers were covered by statutory exemption in federal FOIA, 5 U.S.C. § 552(b)(6), for records that would constitute a clearly unwarranted invasion of personal privacy if disclosed); Progressive Animal Welfare Soc'y. v. Univ. of Wash., 884 P.2d 592, 598 (Wash. 1994) (en banc)

availability of seemingly limitless online storage and computer-assisted reporting makes it possible for journalists to analyze and publicly share vast quantities of data that previously were siloed within government computers.[303] Modern data journalism could be greatly inhibited by overbroad doxing statutes, unless "intent" is tightly drawn and strictly construed so that "intent" refers to the harmfulness of the information journalists disclose—not just to the intentional disclosure of a database that incidentally happens to contain harmful information.

Another possible approach might be to emulate the example of the State of Georgia, where an early iteration of a doxing statute protects only the most vulnerable subset of people: those who have already established that they are at risk of harassment and intimidation, so that they qualify for a judicial order of protection.[304] Extending protection solely to people who have made a threshold showing of individualized vulnerability would avoid the worst overbreadth concerns of a statute such as those in Colorado, Minnesota, and Oklahoma that apply to all employees of select government agencies, even employees with mundane "desk jobs" who are unlikely targets for professionally motivated threats. Such a narrowly tailored approach would help ensure that newsmakers do not weaponize doxing laws to shut down unfavorable coverage and commentary.

Any statute purporting to criminalize doxing must be drawn in recognition that there are times when distributing people's contact information furthers the interests of advocacy, commentary, and journalism—as in the Eric Adams and Josh Hawley examples. In the context of defamation, the law already recognizes greater latitude to criticize pervasively famous public figures, even inaccurately, because their behavior is a matter of public interest and because they have the wherewithal to rehabilitate their own reputations through counterspeech.[305] Any attempt to criminalize doxing should likewise recognize that pervasively public people are already easily located, so that disclosing their contact information cannot constitute a crime, apart from any threat or incitement that might accompany the disclosure. A contrary rule would, for example, potentially open a social media user up to doxing liability simply for publishing

---

(applying exemption under Washington Public Records Act and stating, "[D]isclosure of a public employee's Social Security number would be highly offensive to a reasonable person and not of legitimate concern to the public."); State *ex rel.* Beacon J. Publ'g Co. v. City of Akron, 640 N.E.2d 164, 166 (Ohio 1994) (finding that employees' Social Security numbers are not accessible under Ohio Public Records Act, because disclosure would compromise employees' constitutionally protected right to informational privacy).

[303] *See* Phillip Hammond, *From Computer-Assisted to Data-Driven: Journalism and Big Data*, 18 JOURNALISM 408, 411 (2017) (citing examples of journalists using crowdsourcing methods to involve audience members in reviewing publicly shared databases too large for the journalists to analyze on their own).

[304] GA. CODE ANN. § 16-5-90(a)(2) (2022).

[305] *See* Aaron Perzanowski, Comment, *Relative Access to Corrective Speech: A New Test for Requiring Actual Malice*, 94 CAL. L. REV. 833, 847 (2006) ("The current actual malice rule presumes that countering defamation with corrective speech will reduce the harm caused by published falsehoods . . . . Public figures, because of their greater access to the means of mass communication, are better equipped to utilize corrective speech to redress these harms" stemming from defamatory publications).

information as harmless as the address of the state governor's mansion on a discussion board that is known to be frequented by anti-government extremists.

In addition to rethinking how we regulate, it's also important to consider how we talk about the expansive bundle of behaviors that have loosely become known by the shorthand of "doxing." Once speech is regarded as "doxing," then it carries a stigma suggesting it is malicious and harmful, and therefore should be outlawed. Worse, being branded a "doxer" may embolden retaliatory action by people who feel that they are on the high ground in bringing a wrongdoer to heel—even if the "wrongdoing" consists of writing news stories about the behavior of public figures.[306] "Doxing" should be reserved for only that subset of behaviors that carries no defensible purpose, other than to threaten or harass; certainly not, for instance, publishing a sitting president's tax records or exposing white supremacists lurking within police forces.[307] The author George Orwell is widely credited with the saying, "Journalism is printing what someone else does not want printed; everything else is public relations."[308] Publishing unwanted disclosures about people who are figures of public controversy—the type of people who, in contemporary discourse, invariably will be targets of online vitriol—is fundamental to effective news reporting and commentary. Characterizing everyday acts of journalism as "doxing" will likely produce more online harassment, not less—except that the harassment will be directed at the journalists.[309] If our shared societal objective is to dial down the rage quotient of online discourse, we must avoid casually vilifying speakers whose only "crime" is disclosing unflattering information.

---

[306] Well-known tech journalist Taylor Lorenz, who covers social media companies for *The Washington Post*, experienced a bombardment of invective after writing a news story discussing the previously undisclosed ownership of an account on the TikTok social platform, "Libs of TikTok," popular among conservatives for its mockery of liberals. *See* Kara Alaimo, *There's a Proper Term for What Happened to the 'Libs of TikTok' Creator. It's Not 'Doxxing.'* NBCNews.com (Apr. 21, 2022, 3:17 AM), https://www.nbcnews.com/think/opinion/doxxing-libs-tiktok-creator-justified-rcna25280 (observing that right-wing commentators accused Lorenz of "doxing" the proprietor of the TikTok account, even though she gleaned her reporting from publicly accessible registries).

[307] *See supra* note 28 and accompanying text.

[308] Paul Berton, *The True Definition of Journalism; Why Journalists Collaborated on the Panama Papers*, HAMILTON SPECTATOR, Apr. 9, 2016, at A2.

[309] *See* Julie Posetti et al., *Women Journalists Are Facing a Growing Threat Online and Offline*, AL JAZEERA (Nov. 25, 2020), https://www.aljazeera.com/opinions/2020/11/25/women-journalists-are-facing-a-growing-threat (reporting that seventy-three percent of female journalists in a worldwide survey reported being targeted by online harassment and threats, and that twenty percent of all respondents said they had experienced real-world abuse or attacks, and suggesting that the two are causally related).