2022

The Public Square Has Eyes (or Cameras): Anonymous Speech Under the First and Fourth Amendments in the Age of Facial Recognition

Apratim Vidyarthi
University of Pennsylvania

The Public Square Has Eyes (or Cameras): Anonymous Speech Under the First and Fourth Amendments in the Age of Facial Recognition

Apratim Vidyarthi*

Facial recognition technology ("FRT")—once a futuristic fantasy—is more pervasive than ever and shows no signs of becoming less prevalent. While this technology has its upsides, it elicits the notion of an omnipresent being that is watching and tracking us all the time. FRTs encroach on the First Amendment right to anonymous speech by revealing the identity of speakers and chilling speech. Yet, First Amendment doctrine does not provide much solace, since the right to anonymous speech regulates the government's ability to force disclosure of a speaker's identity rather than preventing it from collecting publicly available facial data. The right to anonymous speech also clashes with private actors' right to collect and disseminate information, which provides an avenue for private actors to destroy anonymity. And private actors' First Amendment rights allow them to collect and develop FRT they can use in private spaces.

In addition to inadequate speech rights, litigating FRTs' impacts on the right to anonymous speech is likely to face significant barriers in court. Specifically, plaintiffs will find it hard to show they have been affected by these systems and that their speech has been

* J.D. Candidate, Class of 2022, University of Pennsylvania Law School; M.S. 2016, Carnegie Mellon University; B.S., B.A. 2015, University of California, Berkeley. I am thankful to Professor Seth Kreimer for his guidance and edits of this Article. This Article would also not have been possible without Meghan Downey and Elle Allen. Finally, special thanks to the editors of Fordham's *Intellectual Property, Media & Entertainment Law Journal* for their thoughtful edits and hard work.

chilled, giving them no standing. Further, courts' deference to the legislative and executive branches on issues of crime control and national security might justify an encroachment on the right to anonymous speech. Finally, private parties' rights to collect and disseminate information pose serious barriers to challenge privately-operated FRTs and provides the government an additional avenue to gather facial data and track individuals. Prophylactic legislation is a stronger solution to remedy the issues caused by FRT. Such legislation can regulate the government's use of FRT, private actors' implementations of FRT, and the very creation of FRTs themselves.

INTRODUCTION

A face is worth a thousand words. Faces show feelings, reveal intentions, and carry the baggage of race, gender, religion, and perhaps socioeconomic status. Even a half-covered face, protected by a mask during a once-in-a-century pandemic, still manages to convey considerable information. Taken together, what a face reveals is not just a temporal reality but an image of the permanent self:[1] an inescapable fact, proof of our existence, and evidence of our presence. Unlike the transience of Donald Trump's Twitter account[2] or the fleeting existence of parts of the Watergate tapes, our faces are permanent identifiers, providing us with alibis, but also providing observers with a beacon to track, identify, and incriminate or exonerate.[3]

While flying cars, teleportation, and facial recognition have been mainstays of our imagination——from *The Jetsons* to James Bond to the *Halo* video games—facial recognition technology ("FRT") is slowly becoming a norm, fueled by humans' permanent and

---

[1] Perhaps, except for Clark Kent, for whom glasses completely changed his identity and rendered his true identity entirely invisible. *See* Michael Jung, *Superman's Glasses Are Secretly More Than Just a Disguise*, SCREEN RANT (July 21, 2020), https://screenrant.com/superman-glasses-secret-power-disguise/ [https://perma.cc/T4MD-KMJ7].

[2] *See, e.g.*, @realdonaldtrump, TWITTER, https://mobile.twitter.com/realdonaldtrump [https://perma.cc/3VRM-JMC8] (last accessed Oct. 12, 2021) (showing that Former-President Donald Trump's Twitter account has been suspended).

[3] *See, e.g.*, Lincoln Michel, *How* Curb Your Enthusiasm *Saved a Man from Death Row*, GQ (June 9, 2018), https://www.gq.com/story/how-curb-your-enthusiasm-saved-a-man-from-death-row [https://perma.cc/8E24-9RV5] (describing the story of a man exonerated after evidence showing him present in a *Curb Your Enthusiasm* clip provided an alibi).

identifying characteristics.[4] But, due to a face's permanent nature, facial recognition is not just a step toward realizing our fantastical futures. Instead, it poses risks: the risk of companies and governments tracking citizens, chilling speech, and removing the veil of anonymity from the public square. Where a photo accidentally capturing a face is a snapshot of a specific time and place, FRT has the capacity to identify a person across time and space, creating an invasive profile of where they have been, with whom they are associated, and what they are doing. Semantically, this is no different from many photographs being taken in succession. However, FRT's role in the public sphere creates unease—a feeling of being watched; discomfort with the potential to misinterpret a person's action or association; and a loss of inherent anonymity that was historically expected when part of a crowd.

This discomfort crystallized when the *New York Times* revealed that Clearview AI was scraping photographs from the internet.[5] The advanced artificial intelligence company was using the thousands of photographs on the internet as data to develop a facial recognition software and selling the technology to police and law enforcement agencies.[6] Can individuals talk in public without the fear of being identified and having their speech and actions be policed? How does the public deal with the use of FRT by the government or a shadowy company that is increasing the already disparate power of police and law enforcement agencies? The public's right to free speech and open communication, as well as the underlying principles of self-recognition and freedom of thought, are threatened by the prevalence of such technologies. This perceived encroachment of our civil liberties is reflected in the ongoing litigation against Clearview AI.[7]

---

4 *See, e.g.*, Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, 587 NATURE 350 (Nov. 19, 2020), https://media.nature.com/original/magazine-assets/d41586-020-03188-2/d41586-020-03188-2.pdf [https://perma.cc/R4W3-NEMB] (describing the global growth of FRT).

5 Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/PL7D-C892].

6 *Id.*

7 Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1242 (7th Cir. 2021).

It is no surprise that FRT implicates the First Amendment in more ways than one. For example, broad surveillance-like FRT may "chill association through overreaching relational surveillance," impacting the First Amendment's freedom of association guarantees.[8] And although the First Amendment is supposed to promote freedom of thought and foster ideas, surveillance hinders these freedoms.[9] A corollary to these First Amendment tenets is the right to anonymous speech, which allows citizens to be free from disclosing their identities to the government when they are speaking.[10] Current conceptions of the First Amendment's right to anonymous speech are limited to published literature and political speech.[11] This is partly because the Fourth Amendment is the traditional modality for challenging government surveillance and encouraging privacy.[12] Yet, the impact of FRT extends beyond just surveillance and privacy: it impacts discourse, speech, and behavior in the public sphere.[13] The First Amendment, through the right to anonymous speech, *should* protect against FRTs that chill speech.

This Article investigates why the First Amendment's right to anonymous speech does not protect against FRTs. It further explores how the First Amendment fails to provide a cause of action against public and private institutions that employ FRTs. As the Supreme Court has currently framed it, the right to anonymous speech is a right against disclosure, rather than one that prevents the collection of publicly available data, making it an unusable tool against FRTs.[14] Additionally, the right to anonymous speech clashes with other First Amendment rights to collect and disseminate

---

8 Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 741 (2008).

9 *See, e.g.*, Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 467 (2015) (describing how surveillance undermines the primary tenets of the First Amendment).

10 *See infra* Part I.A.

11 *Id*.

12 For a more detailed analysis of the privacy theory behind First and Fourth Amendments as applied to government data surveillance, see generally MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS (2007) (analyzing privacy theory as it pertains to data surveillance).

13 *See infra* notes 160–63 and accompanying text.

14 *See infra* Part I.A.

information. Further, even if these doctrinal questions were not at issue, litigating the use of FRT would run into significant hurdles. A more feasible approach to realizing the right to anonymous speech against FRTs is through legislation and regulation.

Part I explores the doctrinal history of the First Amendment's right to anonymous speech as one that focuses on preventing the disclosure of a speaker's identity, rather than one that prevents the collection of publicly available data. Part I also explores how the First Amendment's right to collect and disseminate information might conflict with the right to anonymous speech, and how the Fourth Amendment may inform this analysis. Part II explains what facial recognition is, how the government and private actors' use of FRT implicates the First Amendment in the context of anonymous speech, and how there may be tangential Fourth Amendment implications. Part III discusses issues that could arise when bringing a claim against a party using FRT, including difficulties with attaining standing, the Court's deference to national security and policing issues, and conflict with the right to collect and disseminate information by private entities. Finally, Part IV examines possible legislative solutions against the government, as well as ways to regulate private actors and FRT itself.

I. THE DOCTRINAL HISTORY OF THE RIGHT TO ANONYMOUS SPEECH

The history of the right to anonymous speech under the First Amendment started in the late 1950s, beginning with an allusion in *NAACP v. Alabama*.[15] However, the modern era of politics, combined with changing media ecosystems, has seen more cases flesh out this right. Even so, the right to anonymous speech clashes and competes with the right to collect and disseminate information. The Fourth Amendment complicates the picture, providing some solace, but also leaving questions unanswered regarding the extent of governmental authority.

---

[15] NAACP v. Alabama, 357 U.S. 449, 462 (1958).

A. The First Amendment Right to Anonymous Speech

The First Amendment prohibits the government from making any law that abridges "the freedom of speech, or of the press."[16] A corollary of the right to free speech is the right to anonymous speech. The right to anonymous speech has a jurisprudential history that starts in the late 1950s and spans a variety of cases. While most anonymous speech cases deal with political speech and advocacy, some raise questions about the nexus between First and Fourth Amendment rights.

The Supreme Court first alluded to the right to anonymous speech in *NAACP v. Alabama*.[17] There, Alabama asked the Court to compel the NAACP to produce a list of its members.[18] The Court did not explicitly rule on First Amendment grounds and instead ruled on Fourteenth Amendment due process grounds (which the Court noted implicates freedom of speech, though never expressly mentioning the First Amendment) that the production of the membership list would violate freedom of association rights, especially "where a group espouses dissident beliefs."[19] The Court then explicitly pinpointed the notion of the right to anonymous speech in *Talley v. California*, where it struck down a Los Angeles ordinance requiring flyers to include the names and addresses of its publishers on the flyers.[20] In doing so, the Court noted that anonymity can be used for constructive purposes (exemplified by the Federalist Papers).[21] Thus, under *Talley* the Court's approach was to limit government authority by preventing the government from requiring identity disclosure.[22]

---

16 U.S. CONST. amend I.

17 *NAACP*, 357 U.S. at 462.

18 *Id.* at 451.

19 *Id*. at 462. An additional lens through which to look at *NAACP*'s ruling, is that a disclosure of such lists affects freedom of association by chilling relations between members and organizations whose images or beliefs may be frowned upon societally. Strandburg, *supra* note 8, at 786–88.

20 362 U.S. 60, 64–65 (1960).

21 *Id.*

22 *Id.* This approach is far more limited compared to prohibiting the collection or monitoring of identifying information that is publicly available. And given the facts of the case, such a rule makes far more sense than this broader conception of anonymous speech.

After these movements toward anonymous speech, in *Communist Party of United States v. Subversive Activities Control Board*, the Court noted a limit to the right to anonymous speech through limited disclosure, writing:

> Where the mask of anonymity which an organization's members wear serves the double purpose of protecting them from popular prejudice and of enabling them to cover over a foreign-directed conspiracy, infiltrate into other groups, and enlist the support of persons who would not, if the truth were revealed, lend their support, it would be a distortion of the First Amendment to hold that it prohibits Congress from removing the mask.[23]

While the Court was not dealing explicitly with a traditional "right to anonymous speech" case, this remark indicates that the right to anonymous speech has limits in the realm of national security. Subsequently, in *Lamont v. Postmaster General*, the Court implicitly noted that along with the right to anonymous speech, the First Amendment guarantees the right to receive information anonymously.[24] After these ambiguous genesis cases, the Court did not solidify the right to anonymous speech for almost thirty years. The subsequent cases address anonymous speech through limited identity disclosure.

In 1995, the Court in *McIntyre v. Ohio Elections Commission* struck down an ordinance similar to that in *Talley*, but specifically aimed at political leaflets.[25] It explicitly ruled that "[t]he freedom to publish anonymously extends beyond the literary realm."[26] Soon after, in *Bartnicki v. Vopper*, the Court noted that the right to anonymous and private speech encourages the uninhibited exchange of ideas, whereas "the fear of public disclosure of private conversations might well have a chilling effect on private speech."[27] Even so, the Court struck down state and federal statutes that forbade individuals

---

23 367 U.S. 1, 102–03 (1961).
24 381 U.S. 301, 307 (1965).
25 514 U.S. 334, 342 (1995).
26 *Id*.
27 532 U.S. 514, 533 (2001).

from recording intercepted private conversations, noting that the anonymity interest could not justify the statutes' restrictions on the *interceptors*' speech.[28] The Court then reaffirmed *McIntyre*'s right to anonymous speech in *Watchtower Bible v. Village of Stratton*, striking down an ordinance that required a permit to distribute door-to-door advocacy, since anonymous speech is protected by the First Amendment.[29] In doing so, the Court noted that one of the benefits of anonymous speech is that it allows individuals to advocate for unpopular causes.[30] Nearing the end of the political advocacy cases, in *Citizens United v. FEC*, Justice Thomas concurred with the striking down of the FEC's campaign finance disclosure requirements and reaffirmed *McIntyre*, reiterating that the right to anonymity is still pertinent in the modern context.[31] Finally and most recently, in *Americans for Prosperity Foundation v. Bonta*, the Court invalidated an overbroad disclosure law in California that required charitable organizations to disclose the identities of their major donors to the state Attorney General's Office.[32] Citing *NAACP* and its descendants, the Court noted that the California law placed too high a burden on donors' associational rights[33] and did not pass strict scrutiny.[34]

This line of cases distinctly takes a disclosure approach, striking down ordinances that require distributors of print media to *disclose* or *register* their identities with the government to be allowed to conduct speech-related activities. However, this disclosure approach seems inadequate. The secrecy paradigm notes that an individual has a privacy interest in ensuring that secret or private information remains secret.[35] The disclosure of such information destroys that

---

[28] *Id.* at 534–35.

[29] Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 167 (2002).

[30] *Id.*

[31] 558 U.S. 310, 480 (2010) (Thomas, J., concurring).

[32] 141 S. Ct. 2373, 2385 (2021).

[33] *Id.* at 2383.

[34] *Id.* at 2384. Note, however, that Justices Thomas, Alito, and Gorsuch disagreed about the level of scrutiny that should be applied to all such cases. *Id.* at 2389–91 (Thomas, J., concurring); *id.* at 2391–92 (Alito, J., concurring).

[35] Benjamin Zhu, Note, *A Traditional Tort for a Modern Threat: Applying Intrusion Upon Seclusion to Dataveillance Observations*, 89 N.Y.U. L. REV. 2381, 2396–400 (2014).

privacy interest.[36] But our facial identities are continuously disclosed to the public despite a privacy interest in concealing our facial identities if we would like to remain anonymous. Thus, disclosing our facial identities to the public is not disclosing private information to the public because our faces are never "secret." In other words, our faces are *de facto* a part of the public sphere, *even though* we have a privacy interest in keeping our faces or presence anonymous or secret. A broader conception that would protect anonymous speech under the secrecy paradigm is one that prevents the government from collecting or monitoring information about a speaker's speech *or presence*, thus keeping our presence anonymous. Preventing the collection or monitoring of faces implicates anonymous speech, because collecting or monitoring faces, by definition, destroys the speaker's anonymity and thus their right to *anonymous* speech.

Unfortunately, most lower court cases substantiate the disclosure approach. For example, in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit considered an aerial monitoring program that used camera-equipped airplanes to track the movements of people to fight violent crimes.[37] Rejecting the petitioner's argument that the program violated their First Amendment right to freely associate, the court noted that "people do not have a right to avoid being seen in public places. And even if that were not so, it is a stretch to suggest people are deterred from associating with each other [by the program] . . . ."[38] This is the disclosure approach in full visibility. This approach is substantiated by a variety of lower court cases that interpret *McIntyre* as implementing such an anti-disclosure rule.[39] In contrast, few cases interpret the First

---

[36] *Id.*

[37] 979 F.3d 219, 223 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021). Note that the reversal *en banc* was under Fourth Amendment reasoning, rather than the prior First Amendment reasoning. *Id.* at 341–48.

[38] *Leaders of a Beautiful Struggle*, 979 F.3d at 232.

[39] *See, e.g.*, Yes for Life PAC v. Webster, 74 F. Supp. 2d 37, 40–41 (D. Me. 1999) ("[T]he Court's references [in *McIntyre* and *Buckley II*] to information about sources and amount of money were in the context of disclosures to state regulatory authorities, not as attachments to First Amendment communications."); Ky. Right to Life v. Terry, 108 F.3d 637, 648 (6th Cir. 1997) (framing *McIntyre*'s reasoning as concluding that "additional First Amendment burdens exacted by requiring *identification disclaimers* on issue advocacy

Amendment right to anonymous speech—and troublingly, any First Amendment rights at all—as a restriction on the government's ability to collect publicly available facial data. *United States v. United States District Court* is the only Supreme Court case that alludes to First Amendment issues with governmental collecting/monitoring of facial data, and the Court only briefly mentions that government surveillance systems may chill political speech and dissent.[40]

Even when faced with the perfect fact pattern of government collection and monitoring of (ostensibly) freely-available data, lower courts have still taken the disclosure approach, protecting free expression by preventing the disclosure of the speaker's identity.[41] For example, in *Doe v. Harris*, the Ninth Circuit considered whether a regulation that required sex offenders to provide law enforcement agencies with a list of online accounts and identifiers violated the First Amendment.[42] Citing *McIntyre*, the court struck down the regulation and noted its chilling effect on anonymous speech because the regulation "too freely allow[ed] law enforcement to *disclose* sex offenders' Internet identifying information to the public."[43] Even here—with the perfect setup of digital anonymous speech and the government's coercive collection of online identifiers—the court refused to take the broader collecting/monitoring approach.[44] The Fourth Circuit took a similar approach to online anonymity in *Washington Post v. McManus*, striking down a Maryland state law that

---

expenditures" outweighed the state's interest in identifying proponents of issue advocacy) (emphasis added); Vt. Right to Life Comm., Inc. v. Sorrell, 221 F.3d 376, 387–88 (2d Cir. 2000) (phrasing *McIntyre* as a disclosure requirement ruling); Calzone v. Summers, 942 F.3d 415, 425 (8th Cir. 2019) (noting that "speakers ordinarily have the right to keep their identities private" and that the "right to remain nameless" is protected by the First Amendment, as per *McIntyre*; this implicates a prevention of disclosure of identity, rather than its collection); ACLU of Nev. v. Heller, 378 F.3d 979, 991 (9th Cir. 2004) (describing *McIntyre* and its progeny as implicating "state reporting and disclosure statutes"); Worley v. Cruz-Bustillo, 717 F.3d 1238, 1247 (11th Cir. 2013).

40 407 U.S. 297, 313 (1972).

41 For a detailed discussion of the theoretical underpinnings of expression and disclosure under the First Amendment (which is generally beyond the scope of this Article), see Margot E. Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 815, 833–42 (2012).

42 772 F.3d 563, 568–69 (9th Cir. 2014).

43 *Id.* at 578–80 (emphasis added).

44 *Id.*

required online platforms to collect and disclose online political advertisement purchases, also citing *McIntyre*.[45]

The problems do not stop with courts' limited disclosure approach in protecting anonymous speech. Courts also recognize that anonymous speech is not absolute and can be curtailed through two means: (1) where the government's policies meet the "exacting scrutiny" test noted in *Doe v. Reed*; or (2) through the publication of information by private parties.[46] In *Reed*, the Court upheld a law that allowed the state to disclose the names and addresses of those who signed referendum petitions due to the state's need to "preserv[e] the integrity of the electoral process."[47] The Court applied exacting scrutiny, requiring "a 'substantial relation' between the [policy] and a 'sufficiently important' governmental interest," thus slotting the test between intermediate and strict scrutiny.[48] In considering the governmental interest, courts balance the regulation's degree of impact and the degree of justification required.[49] Often, however, this balance weighs in favor of curtailing anonymous speech, especially where the impacts on speech are limited and the justification relates to national security investigative efforts.[50] Combined with the already limited disclosure approach, courts' implementation of "exacting scrutiny" further constrains the right to anonymous speech.

---

45 944 F.3d 506, 511–15 (4th Cir. 2019).

46 *See infra* note 58 and accompanying text.

47 Doe v. Reed, 561 U.S. 186, 197 (2010).

48 *Id.* at 196.

49 *See, e.g.*, Buckley v. Am. Const. L. Found., 525 U.S. 182, 195–96 (1999) (upholding a Colorado constitutional amendment requiring disclosure of identity in circulating petitions for constitutional amendments, the Court balanced the ease of registration to vote and the governmental justification of preventing lawbreakers amongst petition circulators); Meyer v. Grant, 486 U.S. 414, 425–26 (1988) (rejecting a Colorado law that would forbid the use of paid petitioners, the Court balanced the reduction of political discourse, versus the (inadequate) justification of protecting the integrity of the process).

50 *See* Socialist Workers Party v. Att'y Gen., 419 U.S. 1314, 1319–20 (1974) (upholding the FBI's surveillance of the Socialist Workers Party, given that the nature of the proposed monitoring was limited). Another line of cases that upholds anti-anonymity statutes has to do with anti-mask statutes that states have passed to prohibit people from wearing masks in public. In some cases, these statutes have been upheld by the courts, despite the right to anonymous speech; in other cases, these statutes have been struck down. The framing of the statute and the standard applied matter greatly. Kaminski, *supra* note 41, at 848–73.

Lower courts have adopted this balancing approach. In *In re Anonymous Online Speakers*, the Ninth Circuit considered whether a lower court's broad discovery order to disclose the identity of anonymous online speakers violated the First Amendment.[51] The court balanced the value of anonymous speech against the need for discovery of the speakers' identities.[52] The court ultimately required the plaintiff, a competing business, to show they had a clear claim before such information could be discovered.[53] On the other hand, where a government request (rather than a private business' request) for anonymous users' confidential information or internet data is issued through a narrow subpoena rather than a broad discovery order, courts have found that the marginal impact on user privacy and trust can be outweighed by advancements to the governments' legal case.[54] Finally, where private parties request copyright enforcement, the balance is between the public's interest in untainted speech and the private party's interest in protecting its intellectual property.[55] These cases reveal the boundaries of the right to anonymous speech and show that "the degree of scrutiny varies depending on the circumstances and the type of speech at issue."[56]

Private parties can also defeat the right to anonymity generally (which encompasses the narrower right to anonymous speech) by using their own speech. In *Smith v. Daily Mail Publishing Co.*, the *Daily Mail* published the name of a fourteen-year-old boy who was a school shooting assailant.[57] The Court struck down a law that prevented newspapers from publishing the names of juvenile delinquents since the law did not satisfy exacting scrutiny.[58] The newspapers' right to speak, publish, and inform the public trumped the anonymity needs of the juvenile assailant.[59] Additionally, private parties who obtain information from the government can also defeat the right to anonymity. For example, in *Florida Star v. B.J.F.*, a

---

51 661 F.3d 1168, 1176–78 (9th Cir. 2011).
52 *Id*. at 1176.
53 *Id.*
54 *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 680–84 (N.D. Cal. 2006).
55 *In re* DMCA Subpoena to Reddit, Inc., 383 F. Supp. 3d 900, 912–14 (N.D. Cal. 2019).
56 *Id*. at 910.
57 443 U.S. 97, 99–100 (1979).
58 *Id.* at 102.
59 *Id*. at 105–06.

Florida newspaper lawfully obtained the name of a rape victim from the government and published it.[60] The Court found that because the information was lawfully obtained, imposing damages on the newspaper would violate *the newspaper's* First Amendment rights—despite impacting the respondent's privacy and anonymity rights.[61]

This brief history leads to two conclusions. First, the right to anonymous speech protects speakers against forced identity disclosure to the government when engaging in speech, and courts apply at least exacting scrutiny to laws impacting this right. However, the right is more limited than enforcing a right to anonymous speech by preventing the government from monitoring speakers or collecting their information about their identities. Second, once a private party obtains the identity of a speaker, the private party's First Amendment rights to publish that information may overcome the individual's right to anonymity.

B. The Right to Collect and Disseminate Information

Private parties' ability to collect and disseminate information undermines this already limited right to anonymous speech.[62] One party's First Amendment right to disseminate information about another individual's identity can encroach on the latter person's anonymity. And even if the disseminating party does not release information related to the speaker's identity, the mere collection and collation of data can undermine a speaker's anonymity. In the context of private surveillance or FRTs, private actors can implement FRTs because of their right to collect and disseminate information.

In *Bartnicki*, the Court ruled that the private collection and dissemination of information is protected by the First Amendment.[63] Even if a private party does not collect first-hand information, it can use and disseminate data that is available widely and has other permissible uses. For example, in *Sorrell v. IMS Health Inc.*, the Court struck down a Vermont statute prohibiting pharmacies from

---

60 491 U.S. 524, 526–28 (1989).

61 *Id.* at 532.

62 For a more nuanced discussion of the right to gather information, see generally Barry P. McDonald, *The First Amendment and the Free Flow of Information: Towards a Realistic Right to Gather Information in the Information Age*, 65 OHIO ST. L.J. 249 (2004).

63 Bartnicki v. Vopper, 532 U.S. 514, 527 (2001).

disclosing prescriber-identifying information (such as the names of prescribing doctors) and using such data for marketing by pharmaceutical manufacturers.[64] The Court ruled that because the prescriber-identifying information at issue was widely available and had many uses, preventing *some* speakers from using and disseminating it did not satisfy strict scrutiny.[65] Finally, in a case striking down a similar statute in Virginia, the Court noted that a consumer's interest "in the free flow of *commercial* information" is protected by the First Amendment.[66]

The clash between the right to collect/disseminate information and the right to anonymous speech could easily be resolved by distinguishing between what kinds of information can be collected under each right. But the First Amendment right to collect and disseminate is broad, and its maximal interpretation arguably applies to most forms of data that "create[] knowledge,"[67] as a "prerequisite for free expression."[68] In contrast, the right to anonymous speech is not maximalist but is limited: it applies only against the government's ability to require disclosure of a speaker's identity.[69] And some courts do not consider conduct that encourages anonymity (like mask-wearing) as speech, but instead as *conduct* which is unprotected under the First Amendment.[70] Of course, which right prevails depends on the circumstances of the case; but, it is safe to say that a private entity's collection and distribution of a speaker's identity can undermine anonymity and the right to anonymous speech, which only protects against forced disclosures to the government.[71] Nonetheless, governmental regulations protecting anonymity or

---

64 564 U.S. 552, 580 (2011).

65 *Id.* at 573.

66 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 765 (1976) (emphasis added).

67 Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 59–60 (2014). *But see* G.S. Hans, *No Exit: Ten Years of "Privacy vs. Speech" Post*-Sorrell, 65 WASH. UNIV. J.L. & POL'Y 19, 25–26 (2021) (criticizing Bambauer's approach of framing most data collection as covered by the First Amendment as an approach that favors massive data collection and where the legal concept of privacy would not "meaningfully survive").

68 Bambauer, *supra* note 67, at 86.

69 *See supra* Part I.A.

70 Kaminski, *supra* note 41, at 862–74. And with mask-wearing, intent plays a factor in whether the anonymity is protected. *Id.*

71 *See supra* Part I.A.

privacy in the face of a private actor's right to collect and disseminate speech can survive heightened scrutiny, especially if the governmental interests are defined adequately.[72]

Another way to combat private parties' right to the collection and dissemination of information is through the privacy, liberty, statutory, and constitutional rights of other parties. In *Branzburg v. Hayes*, the Court affirmed that a newspaper reporter had to appear before a grand jury, because the public's interest in law enforcement and effective grand jury proceedings overrode the petitioner's information-gathering rights.[73] In so ruling, the Court noted that while newspapers can collect some information, there are limitations: newspapers cannot "circulate . . . reckless falsehoods damaging to private reputation . . . . [They] may also be punished for contempt of court . . . ."[74] In *Seattle Times Co. v. Rhinehart*, the Court upheld a protective order preventing a newspaper from disseminating information obtained through court-mandated discovery procedures, because it could have resulted in "annoyance, embarrassment and even oppression."[75] And in *Holder v. Humanitarian Law Project*, the Court upheld the Material Support Statute's provisions preventing respondents from providing legal training or advocacy (i.e., engaging in their First Amendment rights) to foreign groups deemed terrorist organizations, because the government identified such groups as national security threats.[76] Nonetheless, the Court has made clear that where the government aims to prevent the dissemination of information, it "carries a heavy burden of showing justification for the imposition of such a restraint."[77]

---

72 *See, e.g.*, Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1115–18 (2015) (defining the government's interest in providing notice to individuals and preserving some situations as surveillance-free). For a more thorough discussion of what this legislation could look like, see *infra* Part IV.B.

73 *See* 408 U.S. 665, 683–86 (1972).

74 *Id.* at 683–84.

75 467 U.S. 20, 21–29, 37 (1984).

76 561 U.S. 1, 9–10 (2010) (upholding the statute that prevented petitioners from providing political advocacy and legal training to the Kurdistan Worker's Party and the Liberation Tigers of Tamil Eelam).

77 N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam) (quoting Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).

However, when it comes to collecting information about public officials or in public places, lower courts tend to favor First Amendment rights to collect and disseminate information. For example, some states prevent secretly recording another person's words without their consent.[78] But the First Circuit found such a prohibition overbroad, not satisfying intermediate scrutiny, because it prohibits recordings of police officers "discharging their official duties in public spaces."[79] Similarly, the Ninth Circuit ruled that Customs and Border Protection ("CBP") agents may be unable to prevent individuals from photographing and recording matters of public interest, including agents in CBP facilities.[80] Further, the Tenth Circuit ruled that statutes targeting the creation of speech by imposing heightened penalties on those who collect data in public or public-adjacent spaces are unconstitutional.[81] Together, these rulings indicate that recording and collecting data in public spaces, at least when directed at public officials, are protected First Amendment activities. However, in some cases, the government can articulate interests, such as an interest in privacy, that withstand the applicable level of scrutiny and prohibits public recording.[82] But these interests must be framed in the right manner, accompanied by adequately narrow laws.[83]

Thus, the collection and dissemination of information, especially in public spaces, is generally protected. However, the *collation* of publicly available data creates new issues regarding anonymity. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Court noted that disclosure of

---

[78] *Compare* CAL. PENAL CODE § 632(a) (requiring the consent of *all* parties to a confidential communication), *with* N.Y. PENAL LAW §§ 250.00, 250.05 (making it a crime to record or eavesdrop on a conversation unless at least *one* party (i.e. the recording party) consents).

[79] Project Veritas Action Fund v. Rollins, 982 F.3d 813, 817 (1st Cir. 2020); *see also* Fields v. City of Philadelphia, 862 F.3d 353, 362 (3d Cir. 2017) (making a similar ruling, stating that private individuals have a First Amendment right to observe and record police officers engaged in the public discharge of their duties).

[80] Askins v. U.S. Dep't of Homeland Sec., 899 F.3d 1035, 1046–47 (9th Cir. 2018).

[81] W. Watersheds Project v. Michael, 869 F.3d 1189, 1192 (10th Cir. 2017).

[82] *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 171–73 (2017) (providing a more detailed discussion of what interests can withstand heightened scrutiny).

[83] *See id.* at 199–218 (describing the need for the right temporal/spatial location and right definition of privacy for it to hold ground against the right to record).

government-compiled data—in this case, individuals' criminal records—went against the "practical obscurity" or anonymity-through-obscurity of uncollated data.[84] The Court emphasized that "the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information."[85] Finally, the Court focused on the importance of "the privacy interest in keeping personal facts away from the public eye."[86] Though unclear from what constitutional source this privacy interest arises, the Court indicated that anonymity within uncompiled data may also be relevant as a corollary to privacy rights, at least with respect to government databases.[87]

To summarize, collecting and disseminating information are activities protected by the First Amendment. In cases where collection and dissemination does not take place in the public sphere, governmental interests, statutes, and others' rights might hinder First Amendment rights to collect and disseminate information. Even if individuals can collect and disseminate information, collating information from different sources, though likely allowed by the First Amendment, might violate privacy rights and destroy data subjects' anonymity-through-obscurity.[88]

---

84 489 U.S. 749, 761–62 (1989).

85 *Id.* at 764.

86 *Id.* at 769.

87 An alternative approach that also conceptualizes how compiled data is greater than the sum of its parts can be found in a torts approach against data surveillance operations, in order to enforce seclusion (i.e., a watered-down form of anonymity). *See* Zhu, *supra* note 35, at 2402 (noting that the true privacy threat of data surveillance occurs at the information gathering stage because it is the first step in processing data, which is "more revealing than the sum of the 'unprocessed' data"). One problem with the tort approach is that it requires that if personal information were not voluntarily disclosed, then that information is private and subject to a possible privacy tort. *Id.* at 2408. But faces are personal information and are voluntarily disclosed, if only by a subject's presence in the public sphere. Thus, the basis for a privacy tort seems much weaker as applied to FRT.

88 *See, e.g.*, Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1755–56, 1756 n.182 (2014) (discussing how the combination of the NSA's metadata collection and data from other sources can easily destroy an individual's anonymity).

C. Fourth Amendment Cases

While First Amendment doctrine occasionally touches upon the right to anonymous speech, the Fourth Amendment has far more to say about anonymity broadly. The Fourth Amendment prohibits "unreasonable searches and seizures."[89] In line with the discussion of anonymous speech under the First Amendment, unreasonable searches of a person could undermine their anonymity. A variety of Fourth Amendment cases focus on the intersection between the First and Fourth Amendments, surveillance, national security, chilled speech, and data. A combination of the First and Fourth Amendments' protections could regulate governmental activity, though exactly how that plays out is unclear.[90] Generally, three trends emerge. First, when a third-party collects information about an individual and subsequently gives that information to the government—commonly known as the third party doctrine—such sharing of private information with the government can chill speech, which undermines First and Fourth Amendment principles. Second, where speech is chilled, plaintiffs have a hard time attaining standing. Finally, in cases with cell phones, traditional third-party and chilled speech doctrines may be inapplicable given *Carpenter v. United States*.

First, in *United States v. United States District Court* (hereinafter "*Keith*"), the Court considered whether the government should be required to disclose the information that it gathered through warrantless surveillance of suspected terrorists.[91] The Court noted that national security cases "reflect a convergence of First and Fourth Amendment values" that are not always present in cases of ordinary crime.[92] The Court held that the government must disclose the information, stating that "Fourth Amendment protections become . . . necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute . . . ."[93]

---

89 U.S. CONST. amend. IV.

90 For a detailed discussion of the intersection of the First and Fourth Amendments, see Strandburg, *supra* note 8, at 795–96.

91 407 U.S. 297, 297–302 (1972).

92 *Id.* at 313.

93 *Id.* at 314.

But lower courts have mainly applied *Keith* through the lens of analyzing how overbroad Fourth Amendment searches generally chill speech, rather than evaluating how the searches deter anonymity or anonymous speech. For example, the D.C. Circuit noted that the First Amendment "does not guarantee journalists the right to preserve the secrecy of their sources in the face of [g]ood faith criminal investigation . . .[g]overnment inspection of third-party records, while it may inhibit . . . news-gathering activity, does not impermissibly abridge such activity" when the government's investigation takes place in accordance with Fourth Amendment law.[94] Thus, the government could collect de-anonymizing or identifying information through a third-party where a good faith investigation exists. However, some circuits have moved in the other direction, using the chilling effects on speech to expand the Fourth Amendment's protections. The Ninth Circuit noted that where a subject has a reasonable expectation of privacy in a non-public space, like a mosque, the collection of private conversations is subject to the Fourth Amendment's reasonable expectation test.[95] The D.C. Circuit also noted that Fourth Amendment surveillance could lead to the government seizing innocent citizens' conversations[96] or chill the speech of those opposed to government policies.[97] Although these protections are positive, little discussion of anonymity exists in these cases.[98] They do not explicitly discuss whether collecting or disclosing identifying information is the underlying reason for potential chilled speech.

Even if the chilling effects argument under the First and Fourth Amendments is salient, standing issues arise where chilling effects are concerned. In *Whalen v. Roe*, the Court once again considered a prescription drug disclosure and recordkeeping statute.[99] The Court

---

94 Reps. Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1053 (D.C. Cir. 1978).

95 Fazaga v. FBI, 965 F.3d 1015, 1037 (9th Cir. 2020), *rev'd on other grounds*, 142 S. Ct. 1051 (2021).

96 Zweibon v. Mitchell, 516 F.2d 594, 634–35 (D.C. Cir. 1975).

97 Halkin v. Helms, 598 F.2d 1, 12 n.3 (D.C. Cir. 1979).

98 *See supra* notes 95–97.

99 429 U.S. 589, 591–92 (1977). It turns out that prescription drug disclosure issues are highly litigated—as the Sackler Family is learning, all too late. *See* Meryl Kornfield, *Judge Overturns Deal Giving Purdue Pharma's Sackler Family Civil Immunity From Opioid*

upheld the statute as constitutional, specifically noting, "[t]he patient-identification requirement was a reasonable exercise of the [state's] broad police powers" under the Fourth Amendment.[100] Further, the Court referenced the First Amendment, stating that its associational principles were not strong enough to prevent the government from enacting such a regulation[101] and that the impacts on freedom of association were too speculative.[102] Further, in *California Bankers Association v. Shultz*, the Court considered whether a statute requiring banks to maintain records of consumers' identities and deposits was constitutional under the Fourth and First Amendments.[103] Because banks already kept such records, and because they were not compelled to give the records up, the statute did not violate the Fourth Amendment.[104] Further, the Court ruled that reporting requirements for transactions involving domestic individuals did not violate the Fourth Amendment because the bank owned the records, not the individuals themselves.[105] Finally, the Court did not determine whether the statute violated First Amendment associational rights of certain petitioners because the claim was hypothetical.[106] In sum, two principles stand out. First, unless the government compels a third-party to give up records of an individual, no Fourth Amendment claim stands. Second, chilling effects to the First Amendment's associational aspects require tangible standing.

All this jurisprudence may be bucked by *Carpenter v. United States*, where the Court made a cautious ruling requiring the government to obtain a warrant to collect cell site location data produced by cell phones and stored in cell service providers' databases.[107] While the case had little to do with the First Amendment, it is notable as one of few cases where the Court adequately confronted the nature of cell phone data. The Court noted that cell phone records

Claims, WASH. POST (Dec. 16, 2021, 11:45 PM), https://www.washingtonpost.com/business/2021/12/16/purdue-pharma-sackler-ruling/ [https://perma.cc/V47D-TL5G].

100 *Whalen*, 429 U.S. at 598.

101 *Id.* at 609 (Stewart, J., concurring).

102 *Id.* at 600–02.

103 416 U.S. 21, 25–28 (1974)

104 *Id.* at 51–54.

105 *Id.* at 66.

106 *Id.* at 75–76.

107 138 S. Ct. 2206, 2223 (2018).

are unique and reveal incredibly private and detailed information.[108] Thus, the Fourth Amendment's third-party doctrine does not apply to this "qualitatively different" data.[109] Alluding to issues of anonymity, the Court noted that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'"[110] Similarly, in *United States v. Jones*, Justice Sotomayor's concurrence implied that data aggregation through surveillance may impact First Amendment associational rights.[111] She asserted that GPS monitoring creates a precise record "of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[112] Taken together, *Carpenter* and *Jones* may provide an avenue to argue that a broad-based government data collection program collects "qualitatively different" data that could unmask an individual's identity and therefore affect First Amendment associational rights. But this is a novel argument, and not one completely substantiated by extant cases.

At this interesting intersection between the First and Fourth Amendment, the chilling of speech through surveillance is a real concern and one the Court has addressed. While the underlying principles of the Amendments intersect in some fashion, applying First and Fourth Amendment principles directly to surveillance technology may yield different results compared to applying just the First Amendment. This is primarily due to the heightened scrutiny required for the government to interfere with First Amendment rights, culminating in the need to demonstrate heightened interest and narrow tailoring of the policy (in this case, surveillance). The Fourth Amendment has a lower threshold for permitting government action, allowing for overbroad data collection and non-minimally-invasive surveillance techniques.[113] A successful argument under the

---

108 *Id.* at 2216–19.

109 *Id.*

110 *Id.* at 2217 (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

111 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

112 *Id.*

113 See Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J. F. 444, 455–56 (2017), for a brief analysis on the First and Fourth Amendments' applicability to surveillance technologies.

nexus of the First and Fourth Amendments may posit that collection of publicly-available data is a seizure under *Carpenter*, but is not just subject to the Fourth Amendment's probable cause requirements. Instead, if a surveillance policy either chills speech or discloses the identity of the speaker to the government, the First Amendment's heightened scrutiny standards *also* apply. Thus, the critical issue of collecting/monitoring can be tackled using the Fourth Amendment, and the issue of chilling speech can be tackled using the First Amendment. However, this theory remains untested in the courts.

Even with such novel nexus theories, there are hurdles to bring such a claim: the need for non-speculative harm, national security concerns, and private speakers' own First Amendment rights.

II. FACIAL RECOGNITION AND THE FIRST AMENDMENT

The doctrinal outline provided in Part I may be entertaining on an exam or in a doctrinal constitutional law course, but it does not tell the whole story. As applied to FRT, the First Amendment right to anonymous speech has complex and unfortunate consequences. To understand these implications, this Part first describes FRT and how it works. It then assesses First Amendment implications of the government and private companies' use of FRT. Finally, this Part briefly evaluates Fourth Amendment implications.

A. What Is Facial Recognition and How Is It Used?

While facial recognition has only recently become a technological reality, the basic concept has been around since the 1960s, when Batman used the "batphotoscope" to label a villain's secret identity.[114] Today, Apple's iPhone is a popular example of a personal device using FRT. Apple launched the iPhone X with "Face ID" technology, which uses a variety of sensors and cameras to create a three-dimensional mask of the user's face.[115] The mask (also called

---

[114] *Batman: The Clock King's Crazy Crimes* (ABC television broadcast Oct. 12, 1966).

[115] *See* Rachel Metz, *Facial Recognition Is Only the Beginning: Here's What to Expect Next in Biometrics on Your Phone*, MIT TECH. REV. (Sept. 20, 2017), https://www.technologyreview.com/2017/09/20/4026/facial-recognition-is-only-the-

a mapping or model) is unique to each user, with a low probability that an imposter could deceive the technology.[116] On an individual user's device, the purpose is innocent: unlocking the device or authenticating the user's identity to activate a credit card or access a password.[117] The FRT detects a person's face and compares it against a preexisting map to determine whether it is the face of the person preauthorized to unlock the phone.[118]

However, when such technology is scaled to monitor public spaces and the faces of the public at large, the power and potential threat of FRT becomes more evident.[119] This expansion is not just in scope, but also in kind. Unlike the detection and analysis system on an iPhone, facial recognition *systems* are used to detect and recognize individuals by using many cameras or a variety of data sources.[120] This can implicate privacy issues in public spaces since, by identifying a person's presence at a certain location, these systems can track individuals' movements and locations.[121] These systems generally compare captured images to existing photos in a database (often called a facial recognition database) that have been collected through photo shots, web searches, mugshots, prior surveillance camera footage, and other sources, in order to identify a person.[122]

---

beginning-heres-what-to-expect-next-in-biometrics-on-your/ [https://perma.cc/F499-4YPH] (describing Apple's Face ID technology).

116 *Id*.

117 *See generally About Face ID Advanced Technology*, APPLE, https://support.apple.com/en-us/HT208108 [https://perma.cc/J7WS-TLDN] (describing the uses of Face ID).

118 Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/8WQN-FHWZ].

119 Batman, once again, is a great visual guide, this time in Christopher Nolan's iteration. In *The Dark Knight*, Batman uses a not-quite-facial-recognition system which spies on cell phone users through their microphones and cameras (which is, in some sense, more invasive than static facial recognition). THE DARK KNIGHT (Warner Brothers Pictures, 2008).

120 *See Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/J9H9-QVRJ].

121 Klosowski, *supra* note 118.

122 *See* Karen Hao, *This Is How We Lost Control of Our Faces*, MIT TECH. REV. (Feb. 5, 2021), https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-

Using algorithms and deep learning,[123] these systems can go beyond simply identifying a person, determining a subject's personality, ethnicity, and other intimate traits and characteristics.[124] This creates two categories of consequences. First, the systems' ability to compare faces to those in an existing database could constitute a search under the Fourth Amendment. Second, the identification of an individual's behavioral and other intimate traits challenges a person's subjective expectation of privacy under the Fourth Amendment.[125] Undermining this expectation of privacy could chill that person from appearing in public spaces for fear of having their anonymity destroyed, which also implicates that person's ability to speak anonymously in public and their relevant First Amendment right to anonymous speech.

Beyond these speculative legal risks, there are real issues with existing facial recognition *systems* (as opposed to FRT on individual devices). Such systems are not always accurate, especially when identifying non-white subjects.[126] This is likely due to the overrepresentation or underrepresentation of certain races in the databases upon which systems rely to train and deploy algorithms.[127] For example, Black people are disproportionately represented in mugshot databases and, as such, may be more quickly labelled criminals by an FRT system.[128] Further, these systems can go beyond simply identifying an individual, by making predictive determinations

---

recognition-data-history/ [https://perma.cc/D6UD-7YSE] (describing how facial recognition systems have evolved).

123 Deep learning is a type of machine learning (which is learning based on training algorithms using data sets) that is structured similarly to a neural network and allows the system to discover representations that are needed to detect features or classify data. *See* Juergen Schmidhuber, *Deep Learning in Neural Networks: An Overview*, 61 NEURAL NETWORKS 85, 86 (2015).

124 *See* Hao, *supra* note 122.

125 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

126 Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/KKM8-CCWN].

127 *Id.*; *see also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/CG2Z-56RP] (describing how machine learning algorithms discriminate based on classes like race and gender).

128 *See* Lohr, *supra* note 126.

about a subject's identity, sexuality, IQ, or political leaning.[129] Finally, how data is collected and whether it was used consensually implicates questions of privacy and notice, among other issues.[130]

Despite these concerns, facial recognition databases are ubiquitous. As of 2016, more than 117 million Americans' faces were in a law enforcement facial recognition database.[131] Facebook, which has more than 2.8 billion users,[132] has amassed the largest facial dataset to date.[133] Both the government and private companies' use of the technology is worrisome, though the former raises stronger First and Fourth Amendment concerns. The government's use of facial recognition includes police and law enforcement. As of 2016, at least twenty-five states, including a variety of state and local law enforcement agencies, used facial recognition databases.[134] This includes local law enforcement's access to facial recognition databases, as well as to the Federal Bureau of Investigation's ("FBI") database and access to local law enforcement's databases.[135] In

---

129 Jamie Condliffe, *Facial Recognition Is Getting Incredibly Powerful—and Ever More Controversial*, MIT TECH. REV. (Sept. 8, 2017), https://www.technologyreview.com/2017/09/08/149250/facial-recognition-is-getting-incredibly-powerful-and-ever-more-controversial/ [https://perma.cc/3MUY-STWH]; *see generally* Michal Kosinski & Yilun Wang, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images*, 114 J. PERSONALITY & SOC. PSYCH. 246 (Feb. 2018) (describing the ability for such systems to determine sexuality based on one image).

130 *See* Klosowski, *supra* note 118. Note that the list of issues with facial recognition systems goes beyond the three listed here, but for the purposes of this Article, these are the three most relevant issues.

131 Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/PRG3-8FAR].

132 *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2021*, STATISTA (Nov. 1, 2021), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [https://perma.cc/L4V3-CL27].

133 April Glaser, *Facebook's Face-ID Database Could Be the Biggest in the World. Yes, It Should Worry Us.*, SLATE (July 9, 2019, 7:20 PM), https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html [https://perma.cc/5FA4-3E76].

134 The full list of states includes Alabama, Arizona, Arkansas, Colorado, Delaware, Florida, Illinois, Iowa, Kentucky, Maryland, Maine, Michigan, Minnesota, Nebraska, North Carolina, North Dakota, Ohio, Pennsylvania, South Carolina, Tennessee, Texas, Vermont, Virginia, and Washington D.C. *See* Garvie et al., *supra* note 131. Of course, Florida's inclusion on this list is the least surprising. *See The Daily Show with Jon Stewart: Florida Haters* (Comedy Central television broadcast Jan. 13, 2015).

135 *See* Garvie et al., *supra* note 131.

addition, police not only use facial datasets from government databases, but also images amassed from social media.[136]

In addition to databases, a variety of airports, transit systems, and police forces have active camera systems that capture individuals' faces, which can subsequently be compared to those already in a facial recognition database.[137] Both Immigrations and Customs Enforcement ("ICE") and the FBI use facial recognition systems; the former at the border and airports,[138] and the latter across the country.[139] Reacting to both the local and federal government's use of facial recognition databases and systems, cities like San Francisco and Oakland, California, and Somerville, Massachusetts banned local law enforcement from using facial recognition.[140] Advocacy groups are also bringing suits against federal agencies.[141]

Beyond the government, private companies use facial recognition systems and datasets. Their possession and use of these systems is concerning because of the potential privacy violations of nonconsenting individuals, as well as the government's potential access to

---

[136] *See* James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, VERGE (Aug. 18, 2020, 5:26 AM), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram [https://perma.cc/5CST-D9XT] (reporting that the NYPD may have used social media photographs to investigate a Black Lives Matter activist, without having an active search warrant).

[137] *See Ban Facial Recognition*, FIGHT FOR FUTURE, https://www.banfacialrecognition.com/map/ [https://perma.cc/4XJN-XYER] (showing a variety of state and local law enforcement agencies and transit authorities that use facial recognition).

[138] Exec. Order No. 13,780, 82 Fed. Reg. 13,209, 13,216 (Mar. 9, 2017) (calling for the "expedite[d] . . . completion and implementation of a biometric entry-exit tracking system for in-scope travelers to the United States").

[139] Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/685H-ZYS3].

[140] Shirin Ghaffary & Rani Molla, *Here's Where the US Government Is Using Facial Recognition Technology to Surveil Americans*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future [https://perma.cc/C8NW-UQJV]; *see also Ban Facial Recognition*, *supra* note 137 (providing an updated list of cities banning the technology).

[141] *See, e.g.*, Elec. Priv. Info. Ctr. v. Customs & Border Prot., 248 F. Supp. 3d 12 (D.D.C. 2017) (granting summary judgment for petitioners regarding a Freedom of Information Act request regarding respondent's facial recognition systems).

such data and systems. For example, Facebook's facial recognition feature was[142] consumer-facing; although it made the feature opt-in due to privacy and related litigation concerns.[143] Further, the company agreed to obtain "affirmative express consent" before using facial recognition beyond the permission granted in a user's privacy settings.[144] But, while Facebook did not allow third parties to access its facial database,[145] the National Security Agency's ("NSA") Prism program did collect information from companies like Google and Facebook,[146] though it is unclear whether they ever accessed facial data.

Other private companies like Amazon, IBM, and Microsoft sell commercial facial recognition systems and software.[147] All three companies have expressed concerns or issued moratoria about selling such technology to the government.[148] Vendors of facial recognition systems that have not expressed such qualms include 3M, Cognitec, DataWorks Plus, Dynamic Imaging Systems, FaceFirst,

---

142 In late 2021, Facebook announced that it would shut down its facial recognition system and its underlying data. But the company retains the algorithm and software (DeepFace), which is incredibly accurate because it has been trained on the billions of photographs that Facebook used when the facial recognition system was in operation. Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html [https://perma.cc/85TA-Q4PX].

143 *See generally In re* Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535 (N.D. Cal. 2018) (certifying a class action lawsuit regarding Facebook's use of FRT as a violation of an Illinois biometric privacy law), *aff'd*, Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); *see also Facebook Settles Facial Recognition Dispute*, BBC (Jan. 30, 2020), https://www.bbc.com/news/technology-51309186 [https://perma.cc/ZQ5N-QWY8] (describing the origins of Facebook's facial recognition software and subsequent lawsuits).

144 *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FTC (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep [https://perma.cc/NS9Y-M3H7].

145 *See* Glaser, *supra* note 133.

146 Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps Into User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/V75F-37BQ].

147 Pam Greenberg, *Spotlight | Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. STATE LEGISLATURES (Sept. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx [https://perma.cc/85NW-A6J5].

148 *Id.*

and NEC Global.[149] Finally, Clearview AI is the most relevant and has amassed more than three billion facial images by scraping the internet, including sites like Facebook, YouTube, and Venmo.[150] The company has sold its facial recognition software to more than six-hundred police departments throughout the United States and Canada.[151]

While the use of FRT in these contexts raises many concerns—including privacy, contractual, and ethical concerns—for the purposes of this Article, two issues are pertinent. First, whether such technologies in the hands of (1) the government and (2) private actors implicate the First Amendment right to anonymous speech. Second, whether they implicate Fourth Amendment issues that could, in turn, raise First Amendment issues.

B. First Amendment Implications

A variety of First Amendment issues could arise from the use of FRT. First, when the government uses such systems, it has the potential to chill speech and de-anonymize speakers. However, because the government's use of FRT does not require registration prior to speech like that of *McIntyre*, and since the right to anonymous speech is viewed through the disclosure approach, legal hurdles arise. Second, private companies' First Amendment rights might invalidate anonymous speech claims and their interactions with the government fall in a legally ambiguous zone.

1. The Government's Use of Facial Recognition

The government's use of FRT may raise First Amendment issues because its collection of individuals' faces and therefore whereabouts may deter people from speaking in the public sphere, protesting, and engaging in protected expressive activity, which would chill anonymous speech. Unfortunately, an individual's face and facial expressions are not considered protected speech by the Court. The Supreme Court noted that "[i]t is possible to find some kernel

---

149 *Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/7CVR-8658].

150 *See* Hill, *supra* note 5.

151 *Id*.

of expression in almost every activity a person undertakes—for example, walking down the street or meeting one's friends at a shopping mall—but such a kernel is not sufficient to bring the activity within the protection of the First Amendment."[152] Instead, whether speech is protected by the First Amendment depends on the "expressive content" it conveys.[153] And, the extent to which the government's use of FRT burdens expressive speech protected by the First Amendment "depends on the likelihood that legitimate *expressive* associations will be exposed to government scrutiny."[154] Here, since only subjects' faces are being exposed to government scrutiny, no underlying *speech* is directly being captured, since the images captured by FRT are unlikely to be considered expressive, and thus the underlying facial expressions are unprotected by the First Amendment.[155]

Instead, the government's collection of images of individuals' faces implicates different First Amendment concerns centering around the chilling effect on speech rather than the right to anonymous speech directly. This is because FRT does not require an individual to disclose who is speaking or producing political literature—unlike the issues considered in *McIntyre*, *Bartnicki*, and *Watchtower Bible*—since individuals here are not directly producing speech and registering their speech with the government.[156] Nor are the general principles of these cases implicated. For example, no individual is publishing leaflets, and so the freedom to publish is not implicated.[157] Nor is a private conversation being disclosed publicly.[158] Nor are individuals advocating for unpopular causes.[159] Instead, a government-run FRT is simply collecting publicly available data by

---

152 City of Dallas v. Stanglin, 490 U.S. 19, 25 (1989).

153 Hurley v. Irish-Am. Gay, Lesbian and Bisexual Grp. of Bos., 515 U.S. 557, 572–73 (1995).

154 Strandburg, *supra* note 8, at 803 (emphasis added).

155 *See, e.g.*, Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 253 (2002) (referencing *Stanglin* and noting that government's inhibition "of association is generally not a violation of the First Amendment unless the group is engaged in some type of speech activity.").

156 *See supra* Part I.A.

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

158 Bartnicki v. Vopper, 532 U.S. 514, 533–34 (2001).

159 Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 167 (2002).

collecting images of people in public. Thus, it is unlikely that the right to anonymous speech is implicated, at least through the disclosure approach.

Rather, the government's capture of individuals' faces creates a chilling effect on speech, including anonymous speech made in the public square.[160] Such usage of FRT can distort speech, reinforce behavior,[161] influence the beliefs of those whose beliefs are undecided, increase anxiety and unease, create cognitive dissonance and self-censorship, and generally weaken minority influence.[162] Despite these commonly-accepted impacts on speech, chilling effect arguments have found little traction in post-9/11 government surveillance cases.[163] Further, the Court generally does not find this argument enticing. For example, in *Law Students Civil Rights Research Council, Inc. v. Wadmond*, petitioners argued that the New York Bar's character and fitness screening process violated the First Amendment by chilling speech.[164] The Court was unconvinced, holding that respondents showed "every willingness to keep their investigations within constitutionally permissible limits."[165] Further, the Court emphasized that the chilling effect argument was an inappropriate policy argument for the Court to adjudicate.[166] Similarly, the Court has ignored arguments that overly punitive laws chill speech,[167] and that chilling effects to speech are a strong enough consideration to prohibit state action.[168]

Where the Court has struck down statutes because of chilling effects, the bar for showing that a policy or law chills speech is high. In *Reno v. ACLU*, respondents challenged the Communications Decency Act's ("CDA") provisions that proscribed the "knowing

---

160 *See* Kaminski & Witnov, *supra* note 9, at 485–93 (describing the effects of surveillance). Specifically, surveillance *and the threat of surveillance* can cause an individual to conform to a group's behavior or beliefs and can more broadly change a subject's behavior. *Id.* at 492.

161 *Id.* at 483.

162 *Id.* at 499–500.

163 Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 433 (2008).

164 401 U.S. 154, 156–59 (1971).

165 *Id.* at 167.

166 *Id.*

167 Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 59 (1989).

168 Younger v. Harris, 401 U.S. 37, 51 (1971).

transmission of obscene or indecent messages to any recipient under [eighteen] years of age."[169] The Court struck down these provisions, identifying the CDA as a content-based regulation and finding it sufficiently vague as to deter speech, "silenc[ing] some speakers whose messages would be entitled to constitutional protection."[170] Similarly, in *Dombrowski v. Pfister*, the Court struck down parts of Louisiana's Subversive Activities and Communist Control Law because the arrests and prosecutions of the petitioners were proof that the law chilled speech.[171] The Court concluded that "[t]he chilling effect upon the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospects of its success or failure."[172]

Thus, a case against the government's use of FRT would have to show that any FRT system is statutorily overbroad or leads to arrests and prosecutions of individuals in a manner that chills speech. Showing this will be difficult. Government policies that permit government agencies to use FRT do not directly regulate content and are generally not unconstitutionally vague, because most policies are implemented through administrative decisions rather than through statutes like the CDA.[173] Further, a wide variety of these FRT systems are used to track down and capture individuals who had already committed crimes,[174] which helps provide evidence for successful prosecutions. Unlike in *Dombrowski*, where the statute

---

169 521 U.S. 844, 859 (1997). For a retrospectively entertaining read and the Court's description of the internet and the presence of sexually explicit material on the internet, see *id.* at 849–55.

170 *Id.* at 872–74.

171 380 U.S. 479, 487, 498 (1965).

172 *Id.*

173 *See, e.g.*, NGI System of Records Notice, 81 Fed. Reg. 29,284 (May 5, 2016) (documenting the creation of the Next Generation Identification system and detailing, among other things, an "interstate photo system" and "the addition of face recognition technology to permit law enforcement to search photos against the interstate photo system"); 84 Fed. Reg. 54,182 (Oct. 9, 2019) (proposing the use of iris images and fingerprints to the FBI's Next Generation Identification system).

174 *See, e.g.*, Ryan Lucas, *How a Tip—and Facial Recognition Technology—Helped the FBI Catch a Killer*, NPR (Aug. 21, 2019, 5:01 AM), https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer [https://perma.cc/C3J9-J7LW] (showing that the FBI compared a photograph provided by a tipster against the FBI's database of facial images to track a most wanted fugitive).

threatened to prosecute people because of their speech, FRT systems simply substantiate that someone has *already* committed a crime. In effect, the government's use of FRT systems simply facilitates the government's general crime-control function.[175] Without allegations that the government's use of FRT goes beyond "constitutionally permissible limits,"[176] the use of FRT appears to fit within the confines of justified self-regulated behavior like in *Wadmond*, even if it could be considered overly punitive.

Ultimately, case law and history do not provide a good avenue for challenging the government's use of FRTs under the First Amendment. The problem only intensifies when looking at private actors' use of the technology.

2. Private Actors' Use of Facial Recognition

While an exhaustive discussion of private actors' use of FRT is beyond the scope of this Article, this Article discusses two major issues with respect to private actors. First, private actors' own First Amendment rights indicate that they may be able to use facial recognition systems without significant constraints. Second, private actors who partner with the government may also not be regulatable, allowing the government a means to circumvent the First Amendment.

Private actors use facial recognition for a variety of purposes: preventing theft at retail stores,[177] micro-targeting sales to

---

[175] The Court frequently favors crime control, even when it slightly impacts the First Amendment. *See, e.g.*, Paris Adult Theatre I v. Slaton, 413 U.S. 49, 57–63 (1973) (upholding a Georgia court's decision to prevent the screening of two hardcore pornographic films because the state's proper concern with safeguarding crime and other effects of obscene materials was a legitimate interest that satisfied the Court's ambiguous level of scrutiny).

[176] Law Students C.R. Rsch. Council, Inc. v. Wadmond, 401 U.S. 154, 167 (1971).

[177] *See, e.g.*, Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition, and They Won't Need Your Consent*, BUZZFEED NEWS (Aug. 17, 2018, 10:28 AM), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at [https://perma.cc/G77M-WSBP] (describing the proliferation of facial recognition to prevent shoplifting).

customers,[178] and monitoring employee behavior to improve safety[179] or performance,[180] reduce security threats,[181] or mitigate COVID-19 exposures.[182] How regulatable these technologies are depends on the kinds of databases and underlying systems that exist. For example, if the facial recognition system is a closed environment that simply tracks individuals who enter a LEGO Store[183] and maintains records of those behaving suspiciously, the system does not implicate the First or Fourth Amendments since it operates within the confines of a private environment.[184]

But if the LEGO Store surveillance system matches the faces it tracks to those in an external database, the source of the data in the external database has relevant implications. For example, if the external database's data originates from social media or data profiles, the origins of the data may implicate contract law and regulatory scrutiny if user agreements *from the source of the data* (i.e., the

---

178 *See, e.g.*, Daniel Thomas, *The Cameras That Know if You're Happy—Or a Threat*, BBC (July 17, 2018), https://www.bbc.com/news/business-44799239 [https://perma.cc/2GX8-JC2R] ("A supermarket might use it in the aisles, not to identify people, but to analyse [sic] who came in in terms of age and gender as well as their basic mood. It can help with targeted marketing and product placement.").

179 Sara Castellanos, *Chevron CIO Says Technology Triggers Faster Human Decisions*, WALL ST. J. (Jan. 29, 2019), https://www.wsj.com/articles/chevron-cio-says-technology-triggers-faster-human-decisions-11548808058 [https://perma.cc/J9QE-ZAS3].

180 *See, e.g.*, Drew Harwell, *Managers Turn to Surveillance Software, Always-on Webcams to Ensure Employees Are (Really) Working from Home*, WASH. POST (Apr. 30, 2020), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/ [https://perma.cc/A3W6-3UT5] (discussing the use of webcams and a potential facial recognition feature).

181 *See, e.g.*, Mike Rogoway, *Intel Starts Using Facial Recognition Technology to ID Workers, Visitors*, OREGONIAN, https://www.oregonlive.com/silicon-forest/2020/03/intel-starts-using-facial-recognition-technology-to-scan-workers-visitors.html [https://perma.cc/HS8P-9YVB] (Mar. 11, 2020, 6:16 AM) ("Computers analyze those [facial] images to identify these people, part of a broad program Intel says will help identify 'high risk individuals' who might pose a threat to the chipmaker or its workers.").

182 *See, e.g.*, Natasha Singer, *Employers Rush to Adopt Virus Screening. The Tools May Not Help Much*, N.Y. TIMES (May 14, 2020), https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html [https://perma.cc/DAN2-F66X] (describing the use of a fever-detection and facial recognition camera service known as PopID to identify workers and gauge their temperature).

183 In the Author's opinion, one of the best store franchises offered in the United States.

184 *But see* Slobogin, *supra* note 155, at 256 (noting that where employers use photography and surveillance to track employees who have been involved in strikes, the Court has been willing to find a chilling effect on speech, at least in the labor context).

origin social media website) were abused. For example, Facebook's nonconsensual disclosure of users' phone numbers to third parties led to the FTC imposing a fine and mandatory privacy regime on the company.[185] However, where a middleman creates the database by scraping data from the internet, the middleman company's First Amendment rights may permit it to collect the data. This is the argument Clearview AI has put forth in pending litigation, though the matter is far from finished.[186] Notably, what is missing from the discussion is the right to anonymous speech, since no actor—the LEGO store, middlemen like Clearview AI, or social media companies—is chilling anonymous speech as was intended in the Court's relevant case law dealing with public speech and disclosure of a speaker's identity to the government.[187]

Of course, the mechanics of this system might implicate the First Amendment—if the Court deems social media platforms and the internet as public forums. The state of this issue is currently in flux, both because technology moves rapidly[188] and because the Court is reluctant to make broad decisions in the internet context.[189] And where the Court has spoken, the waters are muddy. For example, in *Packingham v. North Carolina*, the Court struck down a statute preventing sex offenders from using social media websites.[190] The Court noted that social media was a principle source "for knowing current events, checking ads for employment, speaking and listening in *the modern public square*, and otherwise exploring the vast

---

185 In the Matter of Facebook, Inc., C-4365, 2020 FTC LEXIS 80 (F.T.C. Apr. 27, 2020), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf [https://perma.cc/B9TL-2BZF].

186 Defendant's Motion to Dismiss, ACLU v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. 2021), https://www.aclu.org/sites/default/files/field_document/2020.10.07_memo_of_law_iso_mtd.pdf [https://perma.cc/5MYN-SBC2].

187 *See supra* Part I.A.

188 As Mark Zuckerberg may have said, technology clearly breaks things (like our democracy). *See, e.g.*, Hemant Taneja, *The Era of "Move Fast and Break Things" Is Over*, HARVARD BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over [https://perma.cc/UX72-25J9]; Randall Munroe, *Move Fast and Break Things*, XKCD, https://xkcd.com/1428/ [https://perma.cc/UJA5-76XE].

189 *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (where the Court cabins its decision about requiring warrants for cell site location information ("CSLI") only to CSLI, rather than renovating all third party doctrine).

190 137 S. Ct. 1730, 1737 (2017).

realms of human thought and knowledge."[191] But this slight statement does not indicate whether public forum doctrine applies to all social media or whether the public square was being used metaphorically. Some indication can be found in *Knight First Amendment Institute at Columbia University v. Trump*, where the Second Circuit deemed a government official's Twitter account a public forum.[192] While the case was vacated as moot, Justice Thomas advocated for social media platforms to be considered public forums based on the power held by these companies.[193] All this is to say that if social media sites are considered public forums, then the discussion and First Amendment implications surrounding data scraping and anonymous speech might differ. But this is not currently the case.

A final issue is that private actors share information and technology with the government. Those whose speech is chilled by the government's acquisition of such data are at a disadvantage. The government already acquires data from private companies, especially regarding border issues.[194] There are two issues that apply, likely rooted in the Fourth Amendment. First, the Stored Communications Act likely prevents the digital platforms where data originates (e.g., Facebook, Google, Twitter) from sharing the data directly with the government without a subpoena or warrant.[195] But a middleman, such as Clearview AI, is not prohibited from doing so.[196] Such middlemen are allowed to scrape publicly available data from Facebook and Google and share it with the government, as

---

191 *Id.*

192 928 F.3d 226, 237 (2d Cir. 2019), *vacated as moot*, Biden v. Knight First Amend. Inst., 141 S. Ct. 1220 (2021).

193 *Biden*, 141 S. Ct. at 1227 (Thomas, J., concurring).

194 *See, e.g.*, Bryan Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 [https://perma.cc/8P53-JQ4R] (reporting that ICE bought millions of dollars of licenses to access location data for immigration enforcement purposes); Foreign Intelligence Surveillance Act § 702, 50 U.S.C. § 1881(a) (exemplifying the U.S. government's ability to access foreign consumer data).

195 18 U.S.C. § 2702(a).

196 *Id*. (the statute only applies to "a person or entity *providing* an electronic communication service . . . .") (emphasis added).

Clearview AI currently does.[197] Barring collusion between the government and private officials to censor speech,[198] there are few limitations on selling and sharing data with the government. Second, there are Fourth Amendment considerations, outlined in Part II.C.

Despite these (minimal) limitations, if history is any indicator, the government seems to get its way, especially when issues of national security and crime are implicated. The Prism Program—which collected information based on government demands to private companies[199]—has survived a variety of court challenges since its inception.[200] Similarly, the NSA's bulk telephone metadata collection program stood for more than ten years before the Second Circuit declared it unconstitutional.[201] On a positive note, it is possible, through the collection/dissemination doctrine discussed above, that the compilation of this data through various sources might dissipate the anonymity that individual pieces of data might have, which would then create a cognizable claim under reasoning from *Reporters Committee*.[202] Even so, the right to anonymity in *Reporters Committee* was based on a statutory right, which is a

---

197 *See, e.g.*, Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, WIRED (Feb. 11, 2020), https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/ [https://perma.cc/5KL9-DCNE] (noting that the Stored Communications Act "probably doesn't apply to a broker . . . that doesn't deal with consumers directly").

198 Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 72 (1963) (holding that a "scheme of state censorship effectuated by extralegal sanctions" in cooperation with a private party is unconstitutional).

199 Barton Gellman & Askan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [https://perma.cc/Y59N-RV2U] (describing private companies who were subject to this data sharing requirement).

200 *See, e.g.*, Schuchardt v. Trump, No. 14-705, 2019 U.S. Dist. LEXIS 17174 (W.D. Pa. Feb. 4, 2019), *aff'd*, Schuchardt v. President of U.S., 802 F. App'x 69 (3d Cir. 2020) (dismissing a claim that plaintiff was affected by the Prism program because the plaintiff did not show that his information was collected through the program); *see also* Wikimedia Found. v. Nat'l Sec. Agency, 335 F. Supp. 3d 772, 790 (D. Md. 2018) (dismissing plaintiff's motions for discovery regarding data collected by the Prism program due to procedural constraints and the state secrets doctrine).

201 ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015).

202 *See generally* U.S. Dep't. of Just. v. Reps. Comm. for Free Press, 489 U.S. 749 (1989); *see also supra* note 87 and accompanying discussion.

complicated route to ensure the protection of anonymous speech given the lack of any current statutes regulating FRT or creating a right to anonymous speech.

Ultimately, from the perspective of current case law, not much prevents private companies from scraping data and implementing their own FRT systems. Recent history indicates that where the government buys this data, or collates it by pressuring companies, there may be few means of recourse in preserving the right to anonymous speech.

C. Fourth Amendment Implications and Inferences

FRT may also implicate the Fourth Amendment, whose penumbra might, in turn, impact the First Amendment right to anonymous speech. This Section is an abridged discussion of relevant Fourth Amendment principles implicated by FRT, and how they might invoke First Amendment principles.

Generally, FRT in the public sphere does not violate the Fourth Amendment because "[w]hat a person knowingly exposes to the public . . . is not [subject to] Fourth Amendment protection."[203] This applies regardless of the type of technology employed to conduct such surveillance.[204] However, the granularity with which data provides information about a subject may limit what the government can collect without a warrant. In *Carpenter*, the Court explicitly noted the unique nature of cell site location information ("CSLI") data, stating that the granularity of such data gave the government "perfect surveillance" abilities rather than general ones.[205] CSLI data could also enable the government to create a profile about an individual's whereabouts retrospectively and continuously, without limitation.[206] This shows the Court's concern about technologies

---

[203] Katz v. United States, 389 U.S. 347, 351 (1967). For a practical example, see Byron Tau, *License-Plate Scans Aid Crime-Solving but Spur Little Privacy Debate*, WALL ST. J. (Mar. 10, 2021, 12:23 PM), https://www.wsj.com/articles/license-plate-scans-aid-crime-solving-but-spur-little-privacy-debate-11615384816 [https://perma.cc/WHU9-XZF7] (discussing the widespread use of license plate scanners to track insurrectionists after January 6th, in addition to other crime-fighting purposes).

[204] United States v. Knotts, 460 U.S. 276, 281–82 (1983) (applying *Katz* to an electronic device used to track an individual for more than 100 miles).

[205] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

[206] *Id.*

that allow the government to create such warrantless profiles of individuals' whereabouts with a high level of precision and accuracy, precisely like FRT.

Despite the professed protection for such revealing data, the government could circumvent the warrant requirement from *Carpenter* by simply buying data (rather than subpoenaing it, as in *Carpenter*) from a third-party that collected the data.[207] And there are limited protections for data given to third parties, as the Court noted in *Smith v. Maryland*.[208] There, the Court found that the government's use of a pen register[209] to collect the phone numbers dialed by petitioner did not violate the Fourth Amendment, because the dialed numbers were being transmitted to a third party, and so the petitioner did not have a reasonable expectation of privacy in this non-content data.[210]

Three inferences can be drawn from the Fourth Amendment's public exposure doctrine, *Carpenter*, and third party doctrine. First, preserving autonomy—which is central to the Fourth Amendment—might depend on being identified in a large mass of people, rather than remaining totally anonymous in public.[211] Taking a cue from this Fourth Amendment doctrine, this leads to possible solutions in preserving the First Amendment right to anonymous speech, which might have to focus on ensuring some threshold level of fungibility among other members of the public rather than total anonymity. Second, where personal data is transferred to third parties from whom the government subsequently accesses that data, it may not be protected under the third party doctrine.[212] Finally, despite tomes of doctrine, with *Carpenter*, the Court has shown that it is open to changing direction when dealing with technological advancements

---

207 *See* Edelman, *supra* note 197.

208 442 U.S. 735, 745 (1979).

209 *Id*. at 748 (Marshall, J., dissenting). In the olden days when phones had cords and buttons, a pen register was used to collect the numbers that were dialed on a phone. *Id.* at 736 n.1. We would probably call this "metadata" collection now.

210 *Id.* at 745.

211 *See* Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 UNIV. CHI. L. REV. 47, 81–82 (1974).

212 *Smith*, 442 U.S. at 744.

that are qualitatively and quantitatively different from analogous historical technologies.

One final observation is that the penumbras of the First and Fourth Amendments may together create a cause of action for finding that FRT violates privacy rights. The penumbra theory intersects with the right to anonymity, especially in terms of freedom of thought, belief, and personhood.[213] However, an exploration of the penumbra theory is beyond the scope of this Article.

III. CHALLENGES TO LITIGATING AGAINST FRT UNDER THE RIGHT TO ANONYMOUS SPEECH

Despite the challenges presented by extant case law and barriers of the First and Fourth Amendments, potential plaintiffs may still want to challenge the government's use of FRT through litigation under the right to anonymous speech. Such litigation would face an uphill battle on three fronts: (1) finding plaintiffs who could meet standing requirements; (2) overcoming national security issues; and (3) defeating the right of private third parties to collect and receive information.

A. Issues of Standing

A party must be "entitled to have the court decide the merits of the dispute or of particular issues" for it to have standing before a court.[214] Here, there are three main issues with attaining standing. First, the Court's bar for the kind of injury that constitutes a particularized and legally-cognizable harm has narrowed in recent years; combined with *Twombly* and *Iqbal*, the threshold is difficult to overcome. Second, regardless of whether a party can articulate a concrete harm, finding the right plaintiff is difficult. And even if these

---

[213] *See* Slobogin, *supra* note 155, at 258–67 (discussing the penumbra theory and additional implications to freedom of movement and repose, posed by surveillance cameras). For an extended discussion about the right to privacy under the Fourth Amendment and how that intersects with the right to anonymity (as opposed to the specific right to anonymous speech), see Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 715–20, 725–31 (2015).

[214] Warth v. Seldin, 422 U.S. 490, 498 (1975). For a broader discussion about standing requirements, see generally ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES, ch. 2, § 2.5 (2019).

two hurdles are overcome, understanding whether collected information was used for infringing purposes presents additional difficulties. Taken together, these issues mean that even though the right to anonymous speech exists in theory, it may be less applicable in practice as applied to FRT.

Standing for chilling effects and anonymous speech is difficult to attain. For example, in *Laird v. Tatum*, respondents challenged the U.S. Army's surveillance of civilians, alleging that it caused a chilling effect on citizens' First Amendment rights.[215] The Army's surveillance program was intended to "quell insurrection and other domestic violence," and collected "information about public activities that were thought to have at least some potential for civil disorder."[216] Rejecting the argument on standing grounds, the Court said that respondents did not show that they "sustained, or [were] immediately in danger of sustaining, a direct injury as the result" of the government's program,[217] and instead were inadequate "[a]llegations of a subjective chill."[218] The Court then went further in *Clapper v. Amnesty International*.[219] It rejected respondent's claim that the fear of surveillance under Section 702 of the Foreign Intelligence Surveillance Act caused respondents to take "costly and burdensome measures to protect the confidentiality of their communications."[220] The Court said that subjective chill through the existence of a surveillance program is not an adequate substitute for specific subjective harm or threat of future harm.[221] Instead, the injury must be "concrete, particularized, and actual or imminent, fairly traceable to the challenged action; and redressable by a favorable ruling" and "'certainly impending . . . allegations of possible future injury' are not sufficient."[222]

---

215 408 U.S. 1, 3 (1972).

216 *Id.* at 4–6.

217 *Id.* at 13.

218 *Id.* at 13–14. *But see* Slobogin, *supra* note 155, at 253–55 (noting limitations of the applicability of *Laird*).

219 568 U.S. 398 (2013).

220 *Id.* at 415.

221 *Id.* at 415–18.

222 *Id*. at 409.

This requirement for specificity and current injury is further complicated because it is incredibly difficult to find plaintiffs who have directly and concretely had their First Amendment rights to anonymous speech affected by FRT. With respect to infringements on the right to anonymous speech, plaintiffs must allege the system or ordinance has been applied to them.[223] This is particularly difficult with law enforcement and government agencies, who are not transparent when it comes to detailing what techniques or mechanisms were used in apprehending a suspect.[224] Simply showing that the government had a FRT system near a plaintiff's location is likely insufficient to make a pleading that satisfies the specificity requirements of *Twombly* and *Iqbal*.[225] And after making this showing, a plaintiff must also clearly show that the FRT not only destroyed their anonymity, but burdened their ability to speak or express themselves.[226]

On the other hand, potential plaintiffs could bring a chilling effects claim, which is likely less specific than traditional anonymous speech cases addressed in Part I.A. Unfortunately, it is even more difficult to bring these cases. The Court has stated that "'[c]hilling effect' allegations [are] insufficient to establish a case or controversy" unless the allegations are "much more specific."[227] Further, injunctive relief in these cases can be hard to come by without specific allegations of ongoing or imminent harm.[228] This is especially true with respect to state laws, which are a significant avenue for FRT implementation since most law enforcement agencies are local or state affiliated.[229] And as the Court ruled in *Clapper*, what

---

223 Ellis v. Dyson, 421 U.S. 426, 448–49 (1975).

224 *See, e.g.*, Ashcroft v. Iqbal, 556 U.S. 662, 667 (2009) (discussing the FBI's investigation to identify potential terrorists after 9/11, but not detailing the specific means of investigation).

225 For an account of the FBI's lack of transparency when it comes to the use of FRT, see Kade Crockford, *The FBI Is Tracking Our Faces in Secret. We're Suing.*, ACLU (Oct. 31, 2019), https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/ [https://perma.cc/XNQ9-2N62].

226 *See supra* Part I.A.

227 Socialist Workers Party v. Att'y Gen., 419 U.S. 1314, 1316, 1318–20 (1974).

228 Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013).

229 *See* Younger v. Harris, 401 U.S. 37, 51–52 (1971) ("Just as the incidental 'chilling effect' of such statutes does not automatically render them unconstitutional, so the chilling effect that admittedly can result from the very existence of certain laws on the statute books

adequately constitutes a sufficient allegation is a high bar that wades into providing evidence *prior* to knowing what the government's program looks like.[230] For example, respondents must have knowledge of the government's targeting practices in claiming they were targeted.[231] They must know whether methods under the alleged infringing statute were used or other methods were used.[232] They must know whether such methods were successful in acquiring communications.[233] And they must not speculate as to whether their own communications were impacted.[234] These barriers are not mere hurdles—they are mountains.

In contrast to *Clapper*, *Meese v. Keene* provides an example of what concretely satisfies the standing bar, and it is not a reassuring standard. In *Meese*, the Court considered whether the Department of Justice's labelling of the respondent's film as "political propaganda" violated the First Amendment.[235] The Court found that labelling the films "substantially harm[ed] [respondent's] chances for reelection and . . . adversely affect[ed] his reputation in the community," which was "more than a subjective chill" and satisfied the standing requirement.[236] This kind of concrete standing is not something FRT surveillance victims can adequately allege.[237]

Finally, a note about private actors. In *Thornley v. Clearview AI*, petitioners unexpectedly argued that they did not have Article III standing because they wanted to keep their litigation in Illinois state court, likely because the complaint alleged a violation of Illinois state law.[238] The Court found that because the complaint merely alleged a general regulatory violation and was not sufficiently

---

does not in itself justify prohibiting the state from carrying out the important and necessary task of enforcing these laws against socially harmful conduct that the state believes in good faith to be punishable under its laws and the Constitution.").

230 *Clapper*, 568 U.S. at 411–14.

231 *Id.* at 411.

232 *Id.* at 412–13.

233 *Id.* at 414.

234 *Id*.

235 Meese v. Keene, 481 U.S. 465, 468–69 (1987).

236 *Id.* at 473–74.

237 Note that lower courts have noted that the chilling effect on anonymous speech might be better challenged through other rights that have more cognizable harms. *See, e.g.*, Hassan v. City of N.Y., 804 F.3d 277, 292 (3d Cir. 2015).

238 Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1243–44 (2021).

particularized, it did not satisfy Article III standing and must be heard in state court.[239] *Thornley* is a great example of strategic maneuvering to remain in state court where state statutory laws are violated or where state court might be friendlier than federal court. Unfortunately, claims grounded in the First Amendment or against the federal government cannot maneuver like this; by definition, such claims fulfill Article III standing because they allege a violation of federal law.

In conclusion, for claims that are not against private parties and allege First Amendment violations, potential plaintiffs will find it hard to satisfy standing because of *Clapper*'s specificity standard, creating a deterrent to litigation.

B. National Security Issues

FRT is used at the border and to prevent terrorism and similar national security threats.[240] By 2020, the DHS had scanned more than 43.7 million people at the border using FRT.[241] In addition, the federal government uses FRT to prevent terrorism[242] and track domestic terrorists.[243] These uses fall within the purview of border security and national security. Unfortunately, the Court—and courts

---

239 *Id.* at 1248–49.

240 Tau & Hackman, *supra* note 194 and accompanying text.

241 *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. (2020) (statement of John Wagner, Deputy Executive Assistant Comm'r, Office of Field Operations, U.S. CBP).

242 Bobby Allyn, *Amazon Halts Police Use of Its Facial Recognition Technology*, NPR (June 12, 2020, 12:55 PM), https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology [https://perma.cc/C65C-PVS4] ("American intelligence and military officials have long used facial recognition software in overseas anti-terrorist operations, but local and federal law enforcement agencies inside the U.S. have increasingly turned to the software as a crime-fighting tool.").

243 Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html [https://perma.cc/K3WM-E7AA] (noting that after the January 6th insurrection, "[t]here was a [twenty-six] percent increase of searches over [Clearview's] usual weekday search volume."). For a more thorough read of the federal government's use of FRT, see generally KRISTIN FINKLEA ET AL., CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY (2020), https://fas.org/sgp/crs/misc/R46586.pdf [https://perma.cc/3EX5-JA8H].

generally—are deferential to the government's claims that national security issues might require abridgements of First Amendment rights.

With respect to border security, the Court's deference to executive authority is impressive, despite the guarantees of the First Amendment. For example, *Kleindienst v. Mandel* addressed whether the government could prevent a foreigner seeking to participate in academic lectures about socialism from obtaining a non-immigrant visa.[244] The Court ruled that the respondent had no constitutional right of entry as a nonimmigrant.[245] Despite U.S. citizens' First Amendment right to receive information, Congress' "power to make rules for the admission of aliens and to exclude those who possess those characteristics which Congress has forbidden" took precedent.[246] The Court accepted Congress' facially legitimate reasoning, regardless of any First Amendment claim.[247] A similar principle was applied in *United States v. Ramsey*, this time noting the border search exception to the Fourth Amendment's warrant requirement in allowing border officers to search incoming international mail for drugs.[248] The Court permitted warrantless searches of international mail at the border despite any chill to First Amendment rights, which would be minimal and "wholly subjective."[249] In sum, where FRT is used at the border, it is unlikely that the underdeveloped right to anonymous speech would hold much water as compared to the risks to national security and the other branches' authority.

In addition to deference at the border, the Court generally defers to Congress and the Executive when it comes to national security issues. In *Humanitarian Law Project*, Chief Justice Roberts spent several paragraphs quoting Congress and the Executive's claims about terrorism findings, stating that:

---

244 408 U.S. 753, 756–57 (1972).

245 *Id.* at 762.

246 *Id.* at 762–66 (quoting Boutilier v. Immigr. & Naturalization Serv., 387 U.S. 118, 123 (1967)).

247 *Id*. at 767, 770–79; *see also* Timothy Zick, *Territoriality and the First Amendment: Free Speech at—and Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543, 1554–56 (2010) (describing additional statutes that Congress has passed that allow for barring nonimmigrants based on past speech).

248 431 U.S. 606, 616 (1977).

249 *Id.* at 624.

> [The] evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference. This litigation implicates sensitive and weighty interests of national security . . . neither the Members of this Court nor most federal judges begin the day with briefings that may describe new and serious threats to our Nation and its people.[250]

Additional examples of such deference include *Ziglar v. Abbasi*, where the court declined to extend *Bivens* jurisprudence[251] in a case where foreigners who overstayed their visas were detained after 9/11 and were kept under a maximum security unit, strip searched, and subjected to verbal and physical abuse.[252] The Court emphasized the long line of cases discussing separation of powers principles and Congress' desire for the Judiciary not to interfere so as to not expand *Bivens* jurisprudence.[253] Additionally, the Court noted that discovery and litigation would require disclosure of Executive discussion and deliberations, so instead the Court should defer to the Executive in matters of national security.[254] Similarly, in *Hernandez v. Mesa*, the Court considered whether to extend *Bivens* to Fifth Amendment claims in a case where a border patrol agent fatally shot a Mexican child on Mexican soil.[255] Because the shooting was a cross-border incident and because the Executive plays the "lead role in foreign policy," the Court deferred to the Executive to prevent inconsistent government decision-making that might be embarrassing.[256]

---

250 Holder v. Humanitarian L. Project, 561 U.S. 1, 33–34 (2010).

251 A *Bivens* claim allows plaintiffs to sue the federal government for violations of their constitutional rights. The Court permits *Bivens* claims for violations of the Fourth and Eighth Amendments and the Fifth Amendment's Equal Protection Clause. *See* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 390 (1971) (covering Fourth Amendment violations); Carlson v. Green, 446 U.S. 14, 15 (1980) (covering Eighth Amendment violations); Davis v. Passman, 442 U.S. 228, 229–30 (1979) (covering Fifth Amendment Equal Protection Clause violations).

252 137 S. Ct. 1843, 1847, 1869 (2017).

253 *Id.* at 1858.

254 *Id*. at 1861.

255 140 S. Ct. 735, 740–42 (2020).

256 *Id.* at 744–45 (quoting Medellin v. Texas, 552 U.S. 491, 524 (2008)).

While all three cases deal with issues of national security that intersect with foreign policy, the Court's message is clear: in such cases, the federal government's authority is nearly unquestionable, and the Court should defer maximally. Because FRT is currently used to track violent criminals, insurrectionists, drug smugglers, prisoners,[257] and foreigners who have overstayed their visas,[258] it is especially unlikely that the Court will muster the strength to override Congress and the Executive's policies. Finally, where probable cause, investigatory powers, or seizure authority exists, First Amendment claims can be defeated.[259] Thus, the mountain becomes steeper if the technology or techniques questioned implicate national security, border issues, or crime-fighting.

C. Right to Collect and Disseminate Information, and Government Databases

As noted in Part I.I.B, other parties' rights to collect and disseminate information may prevent their First Amendment right to anonymous speech claims against private actors. Both because the jurisprudence is currently evolving, and because a deep analysis is beyond the scope of this Article, this Section briefly addresses two issues. First, whether private actors' right to collect and disseminate information supersedes other First Amendment rights. Second, whether the government's collection and compilation of data through third parties—though not directly under the purview of the right to collect and receive information—has been successfully challenged in the past.

---

[257] *See* Matt Field, *The Alarming Face of Facial Recognition*, BULL. OF ATOMIC SCIENTISTS (June 24, 2019), https://thebulletin.org/2019/06/the-alarming-face-of-facial-recognition/ [https://perma.cc/S2TC-JZN6] (describing the use of FRT in building cases against local drug dealers).

[258] HOMELAND SEC. ADVISORY COUNCIL, FINAL REPORT OF THE BIOMETRICS SUBCOMMITTEE 39 (2020), https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf [https://perma.cc/8FW6-PN5P] ("[A facial recognition system] has been credited with identifying several hundred known or suspected terrorists, in addition to criminals, drug smugglers, human traffickers, murderers, child predators and gangs like MS-13.").

[259] *See, e.g.*, Nieves v. Bartlett, 139 S. Ct. 1715, 1727 (2019) (noting that because probable cause existed to arrest respondent, it did not matter that the police may have been retaliating to respondent's taunts and speech, which fell under his First Amendment rights).

Generally, given facial data's wide availability and many permissible uses, it is unlikely that plaintiffs could plausibly complain of its use by private parties under *Sorrell*.[260] *Branzburg*, *Rhinehart*, and *Humanitarian Law Project* indicate that some statutory and legal interests can precede the right to collect and disseminate information.[261] However, it is unclear what right a potential plaintiff would have here that would be able to trump a collecting company's First Amendment right to speech (as expressed through code[262] and, thus, the creation of facial recognition software), given the lack of statutory protections. This is problematic given examples like Clearview AI, where data upon which the software relies has been acquired legally.[263] The ability to speak anonymously is a right citizens hold against the *government* in preventing registration or tracking *when conducting specific expressive speech*.[264] The right to privacy under the penumbra of the First and Fourth Amendments applies against the government and is unlikely to abridge a third party's right to speech.

More generally, the broad First Amendment right to speech of *private actors* collecting data likely cannot be overcome by an *individual's* right to privacy. This is because laws that protect individual privacy rights will do so by preventing companies from collecting specific types of content (such as facial data), which is subject to the high bar of strict scrutiny.[265] In addition, individual privacy interests generally "fade once information already appears on the public record," while the private entity using that information is protected by the First Amendment.[266] Further, the underlying assumption in

---

260 564 U.S. 552, 573 (2011); *see also supra* note 67 and accompanying text.

261 *See supra* notes 73–77 and accompanying text.

262 Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Ca. 1996) ("For the purposes of First Amendment analysis . . . source code is speech.").

263 *See* Fla. Star v. B.J.F., 491 U.S. 524, 526–28 (1989).

264 *See supra* Part I.A.

265 *See, e.g.*, Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1113 (1999) (noting that anti-paparazzi laws are content-based laws that are presumably unconstitutional). See generally Bambauer, *supra* note 67, for a maximalist view of the First Amendment right to collect and disseminate and how this right trumps privacy rights.

266 *Fla. Star*, 491 U.S. at 532 n.7; *see also* Time, Inc. v. Firestone, 424 U.S. 448, 471–72 (1976) (Brennan, J., dissenting) ("[W]e have held that laws governing harm incurred by individuals through defamation or invasion of privacy . . . must be measured and limited

challenging the use of FRT is that a subject's facial data is either collected in public, on the internet where it is collected through a third party,[267] or in a private space like a store where the private entity's rules and regulations apply. In all three instances, the individual's privacy interests are different from situations in which the individual's information is held purely privately, such as keeping information in a personal journal.[268] In sum, any anonymity or privacy rights generated under the First and Fourth Amendments are weak enough that they would likely be defeated by private entities' own First Amendment rights.

Although not directly related to the right to collect and disseminate information, a further confounding factor is that the government often compiles fingerprint and DNA databases; these may also affect the right to anonymous speech and privacy. Yet, neither type of database has been challenged. For example, the Court held DNA collection and analysis from arrested persons who are not convicted as constitutional because the legitimate law enforcement governmental interest outweighed the minimally invasive privacy intrusion of a cheek swab.[269] Similarly, lower courts have generally accepted maintaining collections of photographs and fingerprints based on a Fourth Amendment balancing analysis, finding that the value of establishing the identity of an individual outweighs liberty and privacy concerns.[270] Further, the Supreme Court has noted that the collection of fingerprint data, even outside the criminal context, is minimally constrained by constitutional issues.[271]

---

by constitutional constraints assuring the maintenance and well-being of the system of free expression."); Anne E. Crane, *Unsealing Adoption Records: The Right to Know Versus the Right to Privacy*, 1986 ANN. SURV. AM. L. 645, 654–55 (1986) (discussing how First Amendment rights often defeat requirements for sealed records in adoption cases).

[267] However, note that it is unclear whether this constitutes "the public record." *See* Crane, *supra* note 266.

[268] See Zhu, *supra* note 36, at 2397, for a discussion of the private-public dichotomy. Specifically, Zhu notes that under the secrecy paradigm, individuals lack a privacy interest in data available from third parties or public records, at least when it comes to bringing a privacy tort. *Id.* A similar analysis would apply here.

[269] Maryland v. King, 569 U.S. 435, 449–61 (2013).

[270] David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095, 1097–98 (2013).

[271] *See, e.g.*, Davis v. Mississippi, 394 U.S. 721, 727 (1969) ("[B]ecause of the unique nature of the fingerprinting process, [detentions for the purpose of fingerprinting] might,

Thus, it is unlikely that a potential plaintiff's right to anonymous speech would defeat a private party's First Amendment right to collect and disseminate information. And the government's extant biometric databases indicate that a facial recognition system, though far more invasive, is unlikely to succeed. Given this futile state of affairs, potential solutions must go through legislation and regulation.

IV. SOLUTIONS

This Article presents three avenues to protect the right to anonymous speech outside of litigation. The first is local and federal government legislation that prevents or pauses the government's use of facial recognition. Second are regulations against private actors. Finally, slowing the creation of facial recognition systems might also be effective in preventing technological expansion until lawmakers, ethicists, and technologists have a better framework to regulate the technology.

A. Legislation and Norm-Setting Against the Government's Use of Facial Recognition

Prophylactic legislation is one approach to protecting rights. This is not a novel concept, even within the realm of FRT. While the right to anonymous speech is enshrined under the Bill of Rights, Congress "bears a responsibility to enforce the Bill of Rights and it has been particularly likely to act in the arena of surveillance regulation."[272] Even so, that may not be the case in a post-9/11, post-bipartisanship world.

Local and state governments have led the way, approaching the issue of facial recognition with the enthusiasm expected of the

---

under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense."); Schmerber v. California, 383 U.S. 757, 764 (1966) ("[B]oth federal and state courts have usually held that [Fifth Amendment privilege] offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."). *See generally* John D. Woodward, Jr. et al., *Appendix C: Legal Assessment: Legal Concerns Raised by the U.S. Army's Use of Biometrics*, *in* ARMY BIOMETRIC APPLICATIONS: IDENTIFYING & ADDRESSING SOCIOCULTURAL CONCERNS 111, 111–66 (RAND 2001).

272 Strandburg, *supra* note 8, at 816.

laboratories of democracy—which may be a blueprint for how the federal government should react. So far, many cities, including Berkeley,[273] Boston,[274] Cambridge,[275] Minneapolis,[276] New Orleans,[277] Oakland,[278] Pittsburgh,[279] Portland,[280] and San Francisco[281] have all banned their respective cities from using FRT. Within these bans, some do the minimum: preventing the city from using the technology.[282] Others—like Berkeley, Boston, Minneapolis, and Pittsburgh—prevent law enforcement from using such technology as well.[283] Cambridge goes further, preventing the collection and use of information obtained through such systems.[284] New Orleans has

---

[273] Levi Sumagaysay, *Berkeley Bans Facial Recognition*, MERCURY NEWS (Oct. 16, 2019, 4:23 PM), https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/ [https://perma.cc/D38W-H2JM].

[274] Ally Jarmanning, *Boston Bans Use of Facial Recognition Technology. It's The 2nd-Largest City to Do So*, WBUR (June 24, 2020), https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban [https://perma.cc/C8DS-NT4K].

[275] Stefan Geller, *Cambridge City Council Bans Face Surveillance Technology*, BOS. HERALD (Jan. 14, 2020, 8:37 PM), https://www.bostonherald.com/2020/01/14/cambridge-city-council-bans-face-surveillance-technology/ [https://perma.cc/R5MH-SQ5H].

[276] Kim Lyons, *Minneapolis Prohibits Use of Facial Recognition Software by its Police Department*, VERGE (Feb. 13, 2021, 9:48 AM), https://www.theverge.com/2021/2/13/22281523/minneapolis-prohibits-facial-recognition-software-police-privacy [https://perma.cc/9NS8-DDW4].

[277] Michael Isaac Stein, *New Orleans City Council Bans Facial Recognition, Predictive Policing and Other Surveillance Tech*, LENS (Dec. 18, 2020), https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech/ [https://perma.cc/RQN3-U2Z6].

[278] Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRONICLE (July 17, 2019, 8:33 AM), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php [https://perma.cc/ZJ5N-SF25].

[279] Juliette Rihl, *Pittsburgh City Council Votes to Regulate Facial Recognition and Predictive Policing*, PUB. SOURCE (Sept. 22, 2020), https://www.publicsource.org/pittsburgh-city-council-vote-regulate-facial-recognition/ [https://perma.cc/P6RB-DU55].

[280] Tom Simonite, *Portland's Face-Recognition Ban Is a New Twist on 'Smart Cities*,*'* WIRED (Sept. 21, 2020, 9:00 AM), https://www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities/ [https://perma.cc/R2LT-PGLP].

[281] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/WYW5-FF6L].

[282] *See, e.g.*, Jarmanning, *supra* note 274.

[283] *Supra* notes 273–74, 276, 279 respectively.

[284] Geller, *supra* note 275.

banned such technologies from propagating predictive policing.[285] And Portland has gone the full distance, banning even private businesses from implementing such technologies.[286] This movement isn't limited to local governments: Vermont has banned law enforcement from using such technology.[287]

The benefits of enacting local and state legislation are numerous. They are not hindered by congressional gridlock and are more closely linked with local law enforcement organizations. Where Congress is constitutionally limited in what prophylactic federal legislation it may pass, state and local governments are not.[288] State and local officials are also less insulated from public pressure and do not generally capture the spotlight of national politics.[289] More importantly, they serve as a measure of forward-thinking, more proactive legislation that can inform the Supreme Court and Congress about what laws work and are constitutionally viable.[290] And because state and local legislators do not have to deal with congressional gridlock, they can react quickly to technological developments, both in creating and reducing restrictions on the use of FRT. Finally, these avenues are useful in resisting sharing information

---

285 Stein, *supra* note 277.

286 Simonite, *supra* note 280.

287 *Vermont Lawmakers Approve Ban on Facial Recognition Technology*, WCAX (Oct. 13, 2020), https://www.wcax.com/2020/10/13/vermont-lawmakers-approve-ban-on-facial-recognition-technology/ [https://perma.cc/YDJ8-2KZ3].

288 City of Boerne v. Flores, 521 U.S. 507, 518 (1997) (stating that "[l]egislation which deters or remedies constitutional violations *can* fall within the sweep of Congress' enforcement power even if in the process it prohibits conduct which is not itself unconstitutional and intrudes into 'legislative spheres of autonomy previously reserved to the States.'") (emphasis added).

289 *See* Megan Brenan, *Americans' Trust in Government Remains Low*, GALLUP (Sept. 30, 2021), https://news.gallup.com/poll/355124/americans-trust-government-remains-low.aspx [https://perma.cc/5BEZ-SSN2] ("Americans' trust in their state and local governments' ability to handle problems under their purview continues to be higher than trust in the federal government and its three individual branches. As has been the case in recent years, confidence in local government ([sixty-six percent]) remains higher than it is for state government ([fifty-seven percent]).").

290 *See, e.g.*, Alabama v. Shelton, 535 U.S. 654, 668–69 (2002) (finding that most states already provide a right to appointed counsel "more generous than that afforded by the Federal Constitution," thus informing the Court's decision on the right to counsel). For a state-by-state account of pending legislation on FRT, see *State Facial Recognition Technology*, ELEC. PRIV. INFO. CTR., https://epic.org/state-policy/facialrecognition/ [https://perma.cc/PE26-PNP9].

with federal agencies engaged in suspicious, but not unconstitutional activities.[291]

Congressional regulation is more difficult, but two approaches may work. First, pushing the federal government for a temporary moratorium on the use of such technology may be successful. Given that the FBI, DHS, and the military are some of the most dangerous users of FRT, a moratorium could be propagated through an Executive Order, which is comparatively easy to pass. If the government wanted to regulate states' use of FRT, then Congress would have to exert its Fourteenth Amendment enforcement authority[292] or Commerce Clause powers,[293] though either approach would need the right framing. And while Congress is gridlocked, lawmakers on both sides of the aisle have shown interest in implementing at least some restrictions on FRT use.[294] In addition, Congress could include regulation providing best practices for the use and implementation of FRT, including acceptable error thresholds, discrimination and algorithmic biases, types of data permissible in facial recognition databases, and permissible acquisition of data from private companies.[295] Finally, Congress could more broadly consider developing intellectual privacy norms that go beyond a warrant requirement just for emails and toward warrant requirements for "intellectual records

---

[291] *See* Erin Baldassari, *BART Adopts Transparency, Accountability Policy for Surveillance Technology*, MERCURY NEWS (Sept. 14, 2018, 4:02 AM), https://www.mercurynews.com/2018/09/13/bart-adopts-transparency-accountability-policy-for-surveillance-technology/ [https://perma.cc/A3GL-SNTB] (noting that Bay Area Rapid Transit created transparency measures after concerns that the organization's facial recognition data was being shared with DHS or other national databases. The measure did not ban facial recognition, however).

[292] U.S. CONST. amend. XIV, § 5 (giving Congress the power to enforce the Fourteenth Amendment against states).

[293] *See generally* Katzenbach v. McClung, 379 U.S. 294 (1964) (recognizing Title II of the Civil Rights Act of 1964's reach on intrastate commerce because preventing Black people from eating in certain restaurants would impact interstate travel and commerce).

[294] *See* Tom Simonite, *Congress Is Eyeing Face Recognition, and Companies Want a Say*, WIRED (Nov. 23, 2020, 7:00 AM), https://www.wired.com/story/congress-eyeing-face-recognition-companies-want-say/ [https://perma.cc/F82N-J6Q7] (noting that some Republicans and most Democrats want to regulate FRT); *see also* National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020).

[295] For an example of model language, see generally *Ban on Government Use of Face Surveillance: A Model Bill*, ELEC. FRONTIER FOUND., https://www.eff.org/document/ban-government-use-face-surveillance-model-bill-0 [https://perma.cc/5XMT-6JHC].

more generally."[296] This could include "heightened certification requirements" when requesting certain kinds of records, notice to those whose facial information is accessed, and intellectual privacy norms within institutions.[297]

B. Regulating Private Actors

While regulating government agencies is one avenue to protect anonymous speech rights, any solution is incomplete without regulating the ways in which private actors collect data for FRT, how the technology is developed, and when the data is sold to certain parties. For example, the Illinois Biometric Information Privacy Act ("BIPA") regulates the collection, retention, disclosure, and destruction of biometric identifiers and information by private entities.[298] BIPA also creates a cause of action against entities that violate it.[299] Since such a cause of action depends on the creation of legislation, this kind of law is nearly necessary to regulate private actors, given private actors' own First Amendment rights discussed in Part II.B.2.

In addition to regulating the technology itself, governments could regulate the source of data in the facial recognition database so companies like Clearview AI would not be able to access information available online without explicit consent from the data subject. For example, the California Consumer Privacy Act requires notice and consent to sell or share data.[300] Such a regulation could prevent nonconsensual use of data in facial recognition databases. Additionally, consumer rights to access their own data profiles and information collected about them in a private company's database[301]—and similar rights to correct[302] and delete[303] such data—might help curb development of such technology from the consumer's end, or at least reduce wrongful identification that harm

---

296 *See* Richards, *supra* note 163, at 440–41.

297 *Id*.

298 740 ILL. COMP. STAT. 14/10 (2008).

299 740 ILL. COMP. STAT. 14/20 (2008).

300 45 C.F.R. § 164.508(a)(4)(i) (2018).

301 *See, e.g.*, CAL. CIV. CODE § 1798.100(d) (West 2021).

302 The European Union's General Data Protection Regulation (or "GDPR") has a right to rectification that could serve as a model. *See* Council Regulation 2016/679, art. 16, General Data Protection Regulation, 2016 O.J. (L 119) 1.

303 *See, e.g.*, Cal. Civ. Code § 1798.105(a).

minority groups. Similarly, a data minimization principle may also serve to limit the kind of data collected by companies, limiting the data's use to specific purposes provided in their notice and consent, or limiting the data collected to provide a specific service requested by a consumer.[304] This way, if a company like Clearview AI collects information from social media companies, the data may not be sufficiently valuable or meaningful for Clearview AI to use in its facial recognition database.

Finally, legislation can prevent surreptitious data collection by companies and subsequent transfer to the government. Such legislation could survive heightened scrutiny if framed in a manner where the right to privacy is a legitimate governmental interest protected by well-written, narrow legislation.[305] The content of this legislation should create conditions for FRT's development and implementation. If legislation creates notice and consent requirements by FRT's developers such that those companies must notify individuals whose faces are included in a database, consumers may have adequate notice. Alternatively, legislation could create a Freedom of Information Access-like requirement for companies developing such technology so consumers could investigate whether their identity exists within a company's database.

Legislation could also require transparency reports that detail companies' interactions with the government, including government demands to share and remove content; currently, such transparency reports are voluntary.[306] Most importantly, however, banning the government from accessing private companies' systems or using such systems may be necessary given that government agencies own and maintain "public forums, like parks and sidewalks, that private [individuals] use for their own expressive activities, like protests and

---

[304] *See, e.g.*, Council Regulation 2016/679, art. 25(2), General Data Protection Regulation, 2016 O.J. (L 119) 1.

[305] *See* Kaminski, *supra* note 72, at 1116–17.

[306] *See* Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, ELEC. FRONTIER FOUND. (July 10, 2017), https://www.eff.org/who-has-your-back-2017#govt-requests [https://perma.cc/ZFQ3-U6M3]; *see also* Jake Laperruque, *How Companies Can Help Make Police Facial Recognition Systems More Transparent*, LAWFARE (Sept. 24, 2019, 9:33 AM), https://www.lawfareblog.com/how-companies-can-help-make-police-facial-recognition-systems-more-transparent [https://perma.cc/V3YW-TEE6].

festivals" which greatly expands the impact of the government's use of FRT's impacts on speech in public spaces.[307] At the very least, regulating transparency around what technologies the government acquires and uses might help shed light on whether First Amendment rights are truly being impacted and whether potential plaintiffs have standing.[308]

A possible challenge to such legislation is that companies have a First Amendment right to regulate speech within their domains as they see fit.[309] But such legislation could also escape this problem and the issues posed by *Sorrell*'s overly pro-collection and pro-dissemination approach to the First Amendment if the legislation defines data as a commodity, rather than speech.[310] Combined with *Bartnicki*'s dicta—that if the content of communication might inform future speech, that does not necessarily constitute current speech—carefully written legislation could survive judicial scrutiny.[311] But private actors may also come around to the notion of procedural norms which might protect the right to anonymity, if users begin to demand such norms.[312]

C. Slowing the Creation of Facial Recognition Systems

Finally, a drastic method to prevent facial recognition systems from proliferating is slowing or regulating the *development* of such technology.

---

[307] Adam Schwartz & Nathan Sheard, *Why EFF Doesn't Support Bans on Private Use of Facial Recognition*, ELEC. FRONTIER FOUND. (Jan. 20, 2021), https://www.eff.org/deeplinks/2021/01/why-eff-doesnt-support-bans-private-use-face-recognition [https://perma.cc/4SST-W4FJ].

[308] *See supra* Part III.A.

[309] *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1195–96 (2018) (describing the legal basis and contours for how private companies can regulate speech).

[310] This is because a commodity does not have expressive import to those involved in data exchanges. For a detailed discussion of this proposal, see Shaun B. Spencer, *Two First Amendment Futures: Consumer Privacy Law and the Deregulatory First Amendment*, 2020 MICH. ST. L. REV. 897, 923 (2020).

[311] *Id.* at 926.

[312] *See* Balkin, *supra* note 309, at 1198 (discussing how private actors, as they begin to resemble public squares, might begin to conform to the speech standards held against the government, due to user expectation and pressure).

In the wake of publicity regarding DHS and law enforcement's use of FRT, various companies unilaterally halted selling and developing these systems.[313] Unilaterally pausing such developments might be useful since this technology rests on iterative mechanisms and algorithms that improve accuracy as more data is provided and processed.[314] Something like an AI winter, which puts a pause on the development of a technology (in this case, AI),[315] might provide the government, lawyers, scholars, and ethicists with adequate time to develop a framework to regulate this technology before it becomes invasively accurate to the point where any regulation is rendered futile. However, a unilateral pause might be hard to achieve given the market's competitive nature and the inherent collective action problem with such a pause.

An alternative mechanism may be for the government to strictly regulate the technology and prevent it from being shared or developed altogether. A model framework for this approach might be the government's regulation of cryptography during the 1990s, when lawmakers feared it would stymie law enforcement or aid foreign adversaries.[316] While this approach generally failed as the internet and associated technologies proliferated,[317] it exemplifies an approach that might be useful in the near-term. Governmental regulation and development of nuclear energy may provide another framework. While private companies still develop nuclear reactors, there

---

[313] Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/E447-NRXR]. While Microsoft only paused its development and sale of such systems, IBM stopped developing their systems altogether and is considering an exit from the market. Matt O'Brien, *IBM Quits Facial Recognition, Joins Call for Police Reforms*, ASSOCIATED PRESS (June 9, 2020), https://apnews.com/article/5ee4450df46d2d96bf85d7db683bb0a6 (last visited Mar. 24, 2022).

[314] *See* Sara Brown, *Machine Learning, Explained*, MIT SLOAN (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained [https://perma.cc/JG48-5YA4] ("The more data, the better the program.").

[315] DANIEL CREVIER, AI: THE TUMULTUOUS SEARCH FOR ARTIFICIAL INTELLIGENCE 203 (1993).

[316] *See generally* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE DIGITAL AGE (2001).

[317] Jack Karsten & Darrell M. West, *A Brief History of U.S. Encryption Policy*, BROOKINGS (Apr. 19, 2016), https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/ [https://perma.cc/4EQY-LDT5].

are significant safety, national security, and supply chain regulations that ensure the government has a strong say in how the technology is developed and used.[318]

However, this approach may ultimately benefit the government. While it would prevent technology from expanding, it might also grant the government a monopoly on FRT and prevent adequate reporting and transparency. Further, all FRT is not bad: consumers use the same technology in their iPhones and when logging into their computers. The key is ensuring that FRT is used in a rights-protective manner. Nonetheless, in the near-term, this might be a valuable approach that gives legislators and technologists space to develop an adequate legal framework.

CONCLUSION

FRT has only seen the tip of the iceberg in its development. The exponential growth of this technology is unlikely to stop, considering the proliferation of AI, social media, computers, smartphones, and cameras. Such technology will likely impact the ability to speak freely in the public square, even if not protected by the First Amendments right to anonymous speech because of its constrained disclosure-based jurisprudence. Part of the problem is FRT's nebulous impact on speech: chilling conversations and imposing *implicit* associations between who and what is said. This implicit registration system is far removed from the kinds of formal registration systems in *McIntyre*[319] and the long line of cases preceding it.

In addition, the right to anonymous speech is underdeveloped and conflicts with other rights. The Court's jurisprudence has become more constrained in recent years, creating hurdles to standing and providing deference to the government's national security and policing responsibilities, no matter how erroneous. But the Court has left the door ajar in the face of new technologies. Even so, litigation may not be the most effective avenue to promote freedom of anonymous speech. This is especially so given that private actors are

---

318 *See generally* J. SAMUEL WALKER & THOMAS R. WELLOCK, A SHORT HISTORY OF NUCLEAR REGULATION (2010).

319 *See generally* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

major users and developers of such technologies, and their own First Amendment rights—which are more broadly recognized—might conflict with the right to anonymous speech.

Instead, the ideal solution is legislation and regulation that ensures transparency and confines the use of such technology, if it does not outright ban it. Greater FRT regulation will likely improve the First Amendment's ability to engender a marketplace of ideas, encourage democratic self-governance, bolster cultural democracy, and help realize self-actualization and autonomy.[320] While this Article only briefly evaluates such solutions, these are the fastest and most efficient ways to prevent broad First Amendment rights from being chipped away. In addition to these challenges and solutions, lawyers and scholars should consider how the First and Fourth Amendments intersect and how the penumbral right to privacy, in combination with the right to anonymous speech and regulations on searches and seizures, might protect civil liberties from being impacted.

There is still time before facial recognition systems become permanent, tracking our unchangeable faces. The law must deliberately move to ensure these challenges are adequately handled and, with that, burnish one of our most cherished civil liberties.

---

[320] Kaminski & Witnov, *supra* note 9, at 512–14.