THE YALE LAW JOURNAL FORUM
OCTOBER 25, 2017

Why Rely on the Fourth Amendment To Do the Work of the First?

Alex Abdo

ABSTRACT. Modern surveillance threatens not only individual privacy but also the freedom to dissent. Yet for a variety of reasons, American courts almost always evaluate the lawfulness of government surveillance solely through the lens of the Fourth Amendment rather than the First Amendment. This Essay explains why we should not expect the Fourth Amendment to adequately protect First Amendment interests, and it briefly sets out how the First Amendment might once again become a bulwark against overreaching government surveillance.

Government surveillance implicates the freedom of speech as well as the right to privacy, and yet our courts usually evaluate the lawfulness of government surveillance solely through the lens of the Fourth Amendment rather than the First. Is that approach defensible?

This term in *Carpenter v. United States*, for example, the Supreme Court will consider whether the warrantless and long-term collection of an individual's "cell site location information," revealing the movements and locations of the user, violates the Fourth Amendment.[1] But the case has clear implications for First Amendment freedoms, too—particularly the ability to express dissent. Dissent's fragile lifecycle—from formulation to ferment—requires privacy and often confidential association to flourish. Warrantless location tracking threatens these conditions, exposing to the government both the participants that initiate and the private places that incubate dissent. And yet the legal fight in

1. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (mem.) (June 5, 2017) (No. 16-402).

Carpenter and many other surveillance cases is taking place almost entirely on Fourth Amendment grounds.

This trend is problematic because the Fourth Amendment is not up to the task of safeguarding dissent from the threat of new technology. As explored below, the Fourth Amendment differs from the First substantially in both its coverage and the strength of its protections. First, Fourth Amendment doctrine addresses invasions of privacy, not speech, and has been held to ignore a whole class of surveillance—the collection of third-party records—with significant implications for expression. Second, unlike the First Amendment, the Fourth Amendment is often blind to the cumulative effect of invasions of privacy that are small in isolation but substantial in combination. Third, and relatedly, the Fourth Amendment tends to focus narrowly on individual harms, not collective or societal ones. Fourth, even when it does apply, the Fourth Amendment offers much weaker protection than does the First, which requires a heightened government interest and means narrowly tailored to that interest. Finally, Fourth Amendment doctrine has been developed largely in the context of criminal prosecutions, in which both the claimants and the relief available tend to generate judicial antipathy.

In other words, we should not expect the Fourth Amendment to pull double constitutional duty, and yet courts routinely act as though it can. The result is that First Amendment freedoms are often at the mercy of a Fourth Amendment doctrine not designed to protect them. The time may have come to fully disentangle the two legal regimes to more fully recognize, as one court has said, that "the First Amendment requires a different analysis, applying different legal standards," than the Fourth.[2]

This Essay sketches out that argument. Part I describes the state of surveillance in the United States and its effect on dissent. Part II argues that we should not expect the Fourth Amendment to protect dissent and other First Amendment freedoms against the threat of modern surveillance. And Part III briefly describes how a First Amendment surveillance doctrine might differ from the current Fourth Amendment framework.

2. Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007) ("[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.").

I. SURVEILLANCE AND DISSENT

A. The State of Modern Surveillance

Government surveillance has always threatened the freedom of speech and dissent. As the Supreme Court has said: "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[3]

This risk is compounded by modern surveillance capabilities, which have reached a tipping point. Their recent evolution has been not incremental, but abrupt. The crucial advance of modern surveillance has been the development of inexpensive automation. Where before the government had to rely on human agents or informants to spy, today it spies through a proliferating network of unsleeping sensors. And where before agents had to manually review what they collected, today they use computers to make sense of their harvest.[4] The government's appetite for digitally collected data has grown in conjunction with its capabilities for collection and analysis. And, when law enforcement agencies cannot sate that appetite directly, they feast, instead, on data accumulated by private companies.[5]

The result of these advances is that, for the first time in human history, the government can now engage in nearly pervasive surveillance of the public. We have seen a glimpse of that reality already, through Edward Snowden's disclosures to the press of the breathtaking scope of surveillance by the National Security Agency[6] and recent reports on law enforcement's expanding use of new and invasive technologies like cell-site simulators,[7] automated license plate

3. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 320 (1972).

4. *See infra* notes 6-8 and accompanying text.

5. *See* American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* 28-29 (July 2013), http://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [http://perma.cc/K9CD-K9NF].

6. *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964 [http://perma.cc/F5VY-EJX6].

7. Cell-site simulators are devices that imitate cell towers to gather information on potentially thousands of nearby cellphones in order to locate a specific cellphone. *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), http://www.wsj.com/news/article_email/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533-lMyQjAxMTI0NTEwNDAxMTQwWj [http://perma.cc/8R5W-DMY8]; Nicky Woolf, *Stingray Documents Offer Rare Insight into Police and FBI Surveillance*, GUARDIAN (Aug. 26, 2016), http://www.theguardian.com/us-news/2016/aug/26/stingray-oakland-police-fbi-surveillance [http://perma.cc/SBA9-8CXR] ("[A]t least 66 state and federal agencies are now known to use the devices, including the IRS, as well as dozens of state and local police departments."); Kim Zetter, *California Police Used Stingrays in Planes to*

readers,[8] pervasive aerial surveillance systems,[9] and facial-recognition databases.[10]

The trend in technology is to reduce virtually everything we do to digital data. Our cellphones are livestreams of our locations; our internet-usage histories are unintended journals of our thoughts; our e-mails are often-permanent records of once-ephemeral conversations. Newer technologies digitize even more of our lives: smart watches, smart TVs, smart refrigerators, smart cars, and a host of other internet-connected devices have made *The Wizard of Oz*'s technicolor transition seem impossibly quaint.

Whether by warrant, subpoena, or some other demand, the government can access more data about us than ever before.

B. The Cost to Dissent

Many commentators have explained that this new surveillance state of affairs comes at considerable cost to the freedom to dissent.[11]

Spy on Phones, WIRED (Jan. 27, 2016), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones [http://perma.cc/69ST-P74S].

8. Automated license plate readers are cameras affixed to police cars or to roadside infrastructure that automatically scan every license plate they see and note the exact time and location of the scan. *See* American Civil Liberties Union, *supra* note 5, at 2 (reporting that automatic license plate readers "have been proliferating around the country at worrying speed"); *id.* at 20 (showing license plate information retention periods of various jurisdictions); *id.* at 25 ("The Wall Street Journal reported in 2012 that, over the past five years, the Department of Homeland Security distributed over $50 million in grants to fund the acquisition of license plate readers.").

9. One such surveillance system is capable of tracking the movements (although not identifying features) of every car and person in a thirty-square-mile area. *See* Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), http://www.bloomberg.com/features/2016-baltimore-secret-surveillance [http://perma.cc/JJW3-M7MS]; *see also* Andrea Peterson, *FBI Spy Planes Used Thermal Imaging Tech in Flights over Baltimore after Freddie Gray Unrest*, WASH. POST (Oct. 30, 2015), http://www.washingtonpost.com/news/the-switch/wp/2015/10/30/fbi-spy-planes-used-thermal-imaging-tech-in-flights-over-baltimore-after-freddie-gray-unrest [http://perma.cc/N2YZ-U73S] (discussing the use of thermal imaging cameras from surveillance aircraft to monitor protests).

10. The FBI and state and local agencies now routinely use facial-recognition technology as a "virtual, perpetual line-up" of the estimated 117 million Americans whose faces are in facial-recognition databases. Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), http://www.perpetuallineup.org [http://perma.cc/T3S7-W2NA].

11. BERNARD E. HARCOURT, EXPOSED (2015) (asserting that today's digital landscape and data collection apparatus is building an "expository state" that is breaking down boundaries between individuals and the state and encumbering our freedom); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1950 (2013).

Dissent requires breathing space: to formulate dissenting ideas, to test and debate those ideas with close associates, to expand the association into a movement, and finally to air grievances publicly, to convince fellow citizens, and to effect political change.

Expansive modern surveillance threatens this fragile process at each stage of development. The threats are most visible at the final stage, when dissidents take their message to the public. Modern surveillance empowers the government to identify and respond to that public outreach earlier and more quickly than ever before.

As the government's surveillance capabilities grow, the threat to dissent reaches earlier into its lifecycle. John Milton described the prior restraint of publication as the abortion of one's "intellectual[] off-spring."[12] Pervasive surveillance can have the same abortive effect. When people are watched or fear that they might be watched, they change their behavior. This is why we close our curtains, password-protect our emails, and clear our internet browsing history. But because we cannot guard against all forms of modern surveillance (most digital "curtains" require technical savvy to use), some amount of self-censorship is inevitable.[13]

The most insidious threat that expansive surveillance poses reaches even earlier into the lifecycle of dissent. For a thought to be birthed in a Miltonian sense, it must first be conceived, and here pervasive surveillance has a contraceptive effect. Those watched change not only their behavior; they change their thinking, too, so that they do not even conceive the thoughts that would become their "intellectual offspring." This is what Neil Richards calls the "normalizing gaze of surveillance,"[14] and it is perhaps analogous to the "observer

12. JOHN MILTON, *Areopagitica: A Speech of Mr. John Milton for the Liberty of Unlicenc'd Printing, to the Parliament of England*, *reprinted in* AREOPAGITICA AND OTHER POLITICAL WRITINGS OF JOHN MILTON 3, 13 (Liberty Fund ed., 1999) (1644) ("Till then Books were ever as freely admitted into the world as any other birth; the issue of the brain was no more stifl[e]d than the issue of the womb: no envious *Juno* sat cross-leg[ge]d over the nativity of any man's intellectual[] off-spring . . . .").

13. *See, e.g.*, *Americans' Privacy Strategy Post-Snowden*, PEW RES. CTR. 4 (Mar. 16, 2015), http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf [http://perma.cc/D54F-G343] (finding that that 22% percent of American adults—about 54 million people—have changed their online behavior "a great deal" or "somewhat" after learning of the scope of U.S. government surveillance, with those most informed changing their behavior most); *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AM. CTR. 6 (Nov. 12, 2013), http://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf [http://perma.cc/WXP6-HNPL] (finding that 28% of American writers had curtailed their use of social media and, more troublingly, that 24% had "deliberately avoided certain topics in phone or email conversations" and that 16% had avoided "writing or speaking about a particular topic").

14. Richards, *supra* note 11.

effect" in physics. Unobserved, a citizen's thoughts—like particles—follow their own path. But the more closely watched they become, the more their possible paths are determined by the very act of observation.[15]

II. THE FOURTH AMENDMENT'S INADEQUATE PROTECTION OF FIRST AMENDMENT INTERESTS

Though expansive surveillance threatens free speech and dissent, courts typically evaluate the constitutionality of surveillance solely with reference to Fourth Amendment doctrine.

This is not categorically the case. In the late 1950s and early 1960s, the Supreme Court issued a string of seminal decisions rejecting subpoenas or other compulsory disclosures that would have exposed the membership of organizations central to the civil rights movement. The decisions invoked the First Amendment, finding the chilling effect of disclosure obvious and unconstitutional.[16] Since that time, many lower courts have questioned and sometimes invalidated subpoenas on similar grounds where they would expose and chill protected associations.[17]

---

15. *See, e.g.*, Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 161 (2016) (finding, in a sophisticated study of self-censorship following the Snowden disclosures, a "large, statistically significant, and immediate drop in total views" of certain politically controversial Wikipedia articles, as well as a "broad and statistically significant shift in the overall trend in the data" that "suggests any chilling effects observed may be substantial and long-term"); *Americans' Privacy Strategy Post-Snowden*, *supra* note 13, at 4 (finding that that about 17% of American adults who are aware of government surveillance programs had changed their use of internet search engines); *Chilling Effects*, *supra* note 13, at 6 (finding that 16% of the American authors polled had "refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious" and that another 12% had "seriously considered" doing the same).

16. *See* Shelton v. Tucker, 364 U.S. 479, 485-86 (1960) ("[T]o compel a teacher to disclose his every associational tie is to impair that teacher's right of free association, a right closely allied to freedom of speech and a right which, like free speech, lies at the foundation of a free society."); NAACP v. Alabama, 357 U.S. 449, 462-63 (1958) ("[W]e think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."); *see also* Bates v. City of Little Rock, 361 U.S. 516 (1960) (holding the same, in Arkansas).

17. *See, e.g.*, FEC v. Larouche Campaign, 817 F.2d 233, 234-45 (2d Cir. 1987) (quashing a subpoena for campaign records that would "compromise the privacy of individual political associations"); Local 1814 v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 270-71 (2d Cir. 1981) (approving of a subpoena for union members' names, after substantial narrowing to

Nevertheless, judicial application of the First Amendment to state surveillance demands has generally been narrow. The courts have analyzed more traditional surveillance challenges—those involving physical or electronic searches and seizures, rather than compelled disclosure—primarily in Fourth Amendment terms.

In *Zurcher v. Stanford Daily*, for example, the Supreme Court recognized the free speech implications of a warrant authorizing the seizure of photographs directly from a newspaper's offices, but it held that those concerns were addressed by the application of the Fourth Amendment's requirements with "scrupulous exactitude."[18] Congress responded by enacting the Privacy Protection Act of 1980, which insulates journalists from certain searches and seizures, but the statute's protections are narrow, and they are, of course, statutory rather than constitutional.[19]

A few years later, the Supreme Court distilled its jurisprudence concerning the seizure of books and films, holding that while the First Amendment requires scrupulous application of certain procedural protections, the seizures "should be evaluated under the same standard of probable cause used to review warrant applications generally."[20] About the same time, the Sixth Circuit broadly stated that "physical surveillance consistent with Fourth Amendment protections in connection with a good faith law enforcement investigation does not violate First Amendment rights, even though it may be directed at communicative or associative activities."[21]

---

accommodate First Amendment concerns); *see also In re* Grand Jury Subpoena to First Nat'l Bank, 701 F.2d 115 (10th Cir. 1983) (remanding for consideration of a First Amendment challenge to a subpoena for bank records of tax-protest groups).

18. 436 U.S. 547, 564 (1978) (quoting Stanford v. Texas, 379 U. S. 476, 485 (1965)).

19. *See* 42 U.S.C. §§ 2000aa, 2000aa-5 to 2000aa-7. The Act is limited in important respects. For instance, it does not apply if there is cause to believe that the journalist in question has committed an offense involving the "receipt, possession, or communication of information relating to the national defense, classified information, or restricted data." *Id.* § 2000aa(a)(1), (b)(1).

20. New York v. P.J. Video, Inc., 475 U.S. 868, 875 (1986); *see also id.* at 873 (collecting cases).

21. Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983) (citations omitted); *see also* United States v. Mohamud, 843 F.3d 420, 444 n.28 (9th Cir. 2016) ("Finally, the district court correctly rejected Mohamud's First Amendment challenge, as motions to suppress based on First Amendment violations are analyzed under the Fourth Amendment."); Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 37, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *rev'd*, 785 F.3d 787 (2d Cir. 2015) (No. 13 Civ. 3994 (WHP)), 2013 WL 5221584 ("The law is clear that governmental investigations conducted in observance of Fourth Amendment requirements, without purpose to deter or penalize protected expression or association, do not violate the First Amendment.").

Even in these contexts, the Supreme Court has recognized the overlapping concerns of the First and Fourth Amendments.[22] But when it comes to actually analyzing the constitutionality of more traditional surveillance, courts tend to apply a traditional Fourth Amendment framework, asking whether the surveillance constitutes a search or seizure within the meaning of the Fourth Amendment and, if so, whether that search or seizure is reasonable.[23]

The result is that the First Amendment freedoms of speech and of the press are often at the mercy of Fourth Amendment doctrine. It is critical to ask, then, whether current Fourth Amendment doctrine adequately protects those First Amendment rights. It does not.

First, the Fourth Amendment protects against intrusions into privacy, not free speech. This is obvious, of course, given the substance of the Fourth Amendment, but it contradicts a seemingly necessary predicate of judicial decisions analyzing First Amendment harms in exclusively Fourth Amendment terms. If the coverage of the two differs, why should we expect defense of one to replace defense of the other? Why, in other words, should an amendment historically focused on the sanctity of the home and other personal effects displace application of an amendment directed at expression?

One glaring example of this mismatch in coverage is the third-party doctrine, through which courts have interpreted the Fourth Amendment to be blind to the seizure of data held by third parties. There is no obvious reason why the First Amendment should be similarly indifferent, and historically, it has not been. The seminal Supreme Court cases quashing subpoenas directed at identifying civil rights activists were, after all, First Amendment cases. But there are signs that the third-party doctrine is now distorting First Amendment doctrine, too. A district court considering a challenge to the NSA's bulk collection of call records held both that the Fourth Amendment does not apply because of the third-party doctrine *and* that the government's argument that the First Amendment should not apply either was "well-supported."[24] The court ultimately dodged the question, but it appeared persuaded that the First

22. *See, e.g.*, United States v. U.S. Dist. Court *(Keith)*. 407 U.S. 297, 313 (1972) ("National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime."); *id.* at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.").

23. *But see* Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007) ("[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.").

24. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

Amendment does not have force independent of the Fourth, thus suggesting that third-party possession eliminates First *and* Fourth Amendment protections.[25]

The Supreme Court may revisit the third-party doctrine this term in *Carpenter*, but the general point remains that the First and Fourth Amendments differ in their coverage.

Second, courts have sometimes taken a divide-and-conquer approach to privacy that is foreign to the First Amendment. Fourth Amendment doctrine tends to focus narrowly on individual harms, whereas First Amendment doctrine accounts for collective or societal ones. The Supreme Court has said many times that Fourth Amendment rights are "personal rights which, like some other constitutional rights, may not be vicariously asserted."[26] On this theory, courts have resisted aggregating "reasonable" invasions of the privacy of many individuals to find the invasions "unreasonable" in their totality.[27] For example, the Foreign Intelligence Surveillance Court has held that an individual challenge to the NSA's bulk collection of call records is not strengthened by the fact that the NSA collected everyone else's call records as well. In that court's words, "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[28]

In contrast, courts applying the First Amendment give significant weight to the collective chilling effect on third parties not before the court. In *Local 1814 v. Waterfront Commission of N.Y. Harbor*, for instance, the Second Circuit slashed the number of longshoremen's names that a state regulatory agency could subpoena in an investigation into union coercion out of concern that a broader

---

25. *Id.*

26. Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (quoting Brown v. United States, 411 U.S. 223, 230 (1973)).

27. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 13 (1973) ("It does not follow that each witness may resist a subpoena on the ground that too many witnesses have been called."); *In re* Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 305 (8th Cir. 1987) ("Western Union's overbreadth argument is based on its fear that the subpoena may make available to the grand jury records involving hundreds of innocent people. But the fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation."); Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 37-40, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 1:13-cv-03994).

28. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], BR 13-109, at 9 (FISA Ct. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf [http://perma.cc/ZTF2-DCM8].

subpoena for more names "may have the practical effect of discouraging" union membership.[29]

Third, and relatedly, courts have taken a similar divide-and-conquer approach to privacy even with respect to multiple privacy invasions of a single individual. In several cases around the country, courts have held that because individuals do not have an expectation of privacy in the address of a single website they have visited online, they do not have any expectation of privacy in a list of *all* websites they have visited.[30] Proponents of that logic say that "zero plus zero equals zero."[31]

The First Amendment, by contrast, is more attentive to the cumulative effect of even individually insubstantial invasions. In *Clark v. Library of Congress*, the D.C. Circuit held that a government employee could pursue a First Amendment claim based on the understandable chill of his expressive activities caused by a "full field investigation" into his association with the Young Socialist Alliance.[32] The investigation consisted of interviewing his coworkers, neighbors, and teachers and of obtaining his school, credit, and other records.[33] A more limited investigation, involving perhaps only a single interview of a coworker, would likely have produced a different outcome. The constitutional harm, then, flowed from the investigation's cumulative effect.

Fourth, the two Amendments also differ in the strength of their legal protections. Significant burdens on free speech must be narrowly tailored to serve heightened state interests.[34] Searches and seizures under the Fourth Amend-

---

29. 667 F.2d 267, 270 (2d Cir. 1981); *see also* Broadrick v. Oklahoma, 413 U.S. 601 (1973) ("Litigants, therefore, are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression.").

30. United States v. Ulbricht, 858 F.3d 71, 97-98 (2d Cir. 2017) (holding that one does not have an expectation of privacy in IP address routing information and collecting cases stating the same); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) (stating that there is no expectation of privacy in "e-mail to/from addresses and IP addresses"); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *13-14 (D. Ariz. May 8, 2013) (reiterating that there is no expectation of privacy in 1.8 million IP addresses of websites visited).

31. There are many reasons to criticize the approach, and the Supreme Court has already signaled it may reverse the trend itself. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *id.* at 429-31 (Alito, J., concurring).

32. 750 F.2d 89, 92-95 (D.C. Cir. 1984).

33. *Id.* at 91.

34. Az. Free Enter. Club's Freedom Club PAC v. Bennett, 564 U.S. 721, 734 (2011); *Clark*, 750 F.2d 89.

ment, by contrast, need only be reasonable.[35] The Supreme Court has said that, to be reasonable, searches and seizures must generally be supported by a warrant based on probable cause.[36] But the interest that a search or seizure serves need not be heightened, and the search or seizure need not serve that interest in as narrow a means as possible. The reasonableness and particularity requirements of the Fourth Amendment require some tailoring of the government's searches and seizures, but the Supreme Court has held that they do not require the government to choose the least-intrusive means available to achieve its interests.[37]

Finally, Fourth Amendment doctrine has been developed largely in the context of criminal prosecutions, in which both the claimants (criminal defendants) and the relief available for violations (suppression of evidence) tend to generate judicial antipathy. Judicial anguish at the prospect of awarding criminal defendants the perceived windfall of suppression is often palpable. In a recent and oft-cited decision, the Supreme Court explained that suppression "exacts a heavy toll on both the judicial system and society at large," because "its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment."[38]

In contrast, courts often pride themselves on preserving and expanding the promises of the First Amendment. In 1964, the Supreme Court said that the First Amendment reflects "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[39] That principle has been a rallying cry of free speech ever since, invoked in nearly every major free speech opinion, and defended against efforts to regulate even the most hateful speech.[40] Though it may be impossible to prove, the differing judicial attitudes toward the First and Fourth Amendments may have promoted the growth of the one while stunting the growth of the other.

---

35. Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'").

36. Katz v. United States, 389 U.S. 347, 357 (1967) ("searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment").

37. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989) (collecting cases holding that searches and seizures need only be reasonable, not the least-intrusive means available).

38. Davis v. United States, 564 U.S. 229, 237 (2011).

39. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

40. *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 452 (2011).

III. A FIRST AMENDMENT FRAMEWORK FOR SURVEILLANCE

If the Fourth Amendment is, for these reasons, an inadequate guarantor of First Amendment rights against overreaching surveillance, what is the alternative? The obvious candidate is the First Amendment itself. Courts could simply apply the First Amendment independently of the Fourth to surveillance that substantially burdens free speech and dissent.

There would be at least three obvious differences in that regime.

First, courts would undertake a First Amendment analysis in circumstances where the Fourth Amendment might not apply at all. For instance, courts that currently find no constitutional restraint on the government's collection of the list of websites someone has visited might recognize that such surveillance burdens free inquiry and dissent. This would not require much legal innovation. The Supreme Court has already recognized the First Amendment harms of the compelled disclosure of organizational membership lists.[41] All that remains is to extend that logic to other forms of surveillance.

Second, where the First Amendment applies, it would require the government to demonstrate a heightened interest to justify its surveillance. The Fourth Amendment generally imposes no such requirement, at least in practice: courts generally do not require the government to defend its interest in executing a warrant, except by establishing probable cause to believe the search or seizure would turn up evidence of a crime. The First Amendment framework would be more fine-grained and might, for example, forbid particularly invasive surveillance predicated on minor offenses or on token showings of cause. For example, whereas the Fourth Amendment might permit officers to track the cellphones of protesters to gather evidence of jaywalking, the First Amendment might prohibit that surveillance as too invasive to be used to investigate an offense so minor.

Finally, where the First Amendment applies, it would require narrow tailoring of the surveillance to the government's interests. Under current Fourth Amendment doctrine, the government need not select the least-invasive surveillance that would accomplish its goals; the First Amendment would require just that. To take one example, courts often permit government investigators to collect extraordinary volumes of a suspect's digital data, on the view that the investigators are best positioned to review the data to determine what is relevant to the investigation and what is not.[42] Where that overbroad collection

---

41. *See supra* notes 16-17 and accompanying text.

42. *See, e.g.*, United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (approving investigator's search of several hard drives for incriminating images and rejecting Ninth Circuit's proposed guidelines addressing the over-collection of digital data).

would burden free speech and dissent, the First Amendment might require narrow tailoring of the collection.

Consider, again, the *Carpenter* case. The government argues that individuals have no expectation of privacy in their "cell site location information," because they voluntarily share that information with their cell phone providers. The result, according to the argument, is that the Fourth Amendment simply does not apply to the government's monitoring of the movements of its citizens using cellular location data. That principle would apply whether the government collected two days' or two years' worth of location data; whether the collection related to an investigation into recreational marijuana use or murder; and whether the government had used the least invasive or most invasive means of pursuing its investigation.

A First Amendment analysis would proceed differently. It would first ask whether the unchecked tracking of the suspect, particularly for long periods of time, burdened the freedoms of speech and association. The analysis would account not only for the chilling effect on the actual surveillance target, but also for the systemic chilling effect imposed by the availability and use of that power. If a court determined that the proposed location tracking would substantially burden First Amendment freedoms, it would ask whether, in the case before it, the tracking nonetheless served heightened government interests and was narrowly tailored to those interests. Even if held to be reasonable under the Fourth Amendment, pervasive and judicially unsupervised tracking of individuals suspected of minor crimes might not pass First Amendment muster. Judicially overseen tracking of individuals suspected of serious felonies for a short period might. In the former case, the government's interests are more minor and its means less measured. In the latter, its interests are stronger and its tactics tailored.

One objection to this approach might be to its administrability. The Fourth Amendment generally provides a predictable roadmap to police officers. The First Amendment framework set out here may appear more freeform. In practice, however, I suspect courts would apply it, much like Fourth Amendment analysis, in a categorical fashion. That is, courts would consider the free speech implications of categories of surveillance, much as courts now consider the privacy implications of categories of government investigation.

The requirement of narrow tailoring under the First Amendment framework might not, however, be as easily generalizable. The Fourth Amendment's focus on reasonableness gives law enforcement great leeway in using surveillance tools that are generally considered constitutional. A requirement that law enforcement narrowly tailor its use of certain surveillance tools might introduce some uncertainty into the constitutionality of using those same tools, as it would require a more searching inquiry. Again, I suspect courts would fashion

rules to provide for predictability. For instance, the federal wiretapping law requires police officers to attest in their surveillance applications that other investigative procedures have failed or would fail.[43] A similar test of narrow tailoring could be imposed under the First Amendment framework for especially intrusive practices.

* * *

Modern surveillance threatens First Amendment freedoms in obvious ways. The time may have come to dispense with the legal fiction that the Fourth Amendment adequately safeguards those freedoms.

Alex Abdo is a senior staff attorney at the Knight First Amendment Institute at Columbia University. Prior to joining the Institute, he was a senior staff attorney at the American Civil Liberties Union's Speech, Privacy, and Technology Project. *He is grateful for thoughtful feedback on drafts of this essay from Jameel Jaffer, Lincoln Caplan, Patrick Toomey, Brett Max Kaufman, and the staff of the* Yale Law Journal Forum*, including Lauren Hobby, Meenakshi Krishnan, Arjun Ramamurti, Erin van Wesenbeeck, and Kyle Victor.*

Preferred Citation: Alex Abdo, *Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 YALE L.J. F. 444 (2017), http://www.yalelawjournal.org/forum/why-rely-on-the-fourth-amendment-to-do-the-work-of-the-first.

43. 18 U.S.C. § 2518(1)(c) (2012).