COMMENT

SURVEILLING AND THEN SHOOTING THE MESSENGER: INTERMEDIARIES, GAG ORDERS, AND THE FIRST AMENDMENT

AMANDA R. SIMMONS†

"[We] see[k] policies of . . . freedom and privacy of expression in digital media. At first[,] we relied on such legal protections for speech as were provided by the First Amendment of the U.S. Constitution. But we soon we realized that, in Cyberspace, the First Amendment is a local ordinance."

– John Perry Barlow[1]

† J.D. 2019, University of Pennsylvania Law School; B.A. 2013, Wesleyan University.

1 JOHN PERRY BARLOW, LEAVING THE PHYSICAL WORLD (n.d.), https://www.eff.org/pages/leaving-physical-world [https://perma.cc/K8Y6-WVY6]. Barlow was a founding member of the Electronic Frontier Foundation and a former lyricist for the Grateful Dead. Sam Roberts, Obituary, *John Perry Barlow, 70, Dies; Championed an Unfettered Internet*, N.Y. TIMES (Feb. 8, 2018), https://www.nytimes.com/2018/02/08/obituaries/john-perry-barlow-internet-champion-dies.html [https://perma.cc/26QB-LPRT].

INTRODUCTION

In the context of domestic criminal surveillance, law enforcement agencies have historically relied on the practice of obtaining user information from traditional third-party intermediaries in order to uncover incriminating evidence on their true targets. For decades, those intermediaries were phone companies, and the actual targets were the individuals who used those companies' services to communicate.[2] Over time, this practice, which implicates both privacy and speech rights, has become more prevalent—and arguably more problematic—in the online world, where there are now a growing number of intermediaries collecting staggering amounts and kinds of user information.[3] But while it appears that the government can, at least for now,[4] constitutionally access communications held by intermediaries without probable cause thanks to the Fourth Amendment's controversial third-party doctrine,[5] the Stored Communications Act (SCA), which was enacted in 1986, attempts to restore by statute certain protections to individuals' right to privacy in their electronic communications.[6] Depending on factors like the type of information sought and the way that it is stored, the SCA outlines a convoluted graduated scale through which officials seeking an individual user's

2 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

3 *See* Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 896 (W.D. Wash. 2017) ("Government surveillance aided by service providers creates unique considerations because of the vast amount of data service providers have about their customers."); Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J.F. 444, 446 (2017) ("[M]odern surveillance capabilities . . . have reached a tipping point . . . . 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.").

4 *See* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2012), *cert. granted*, 137 S. Ct. 2211 (2017).

5 *See Smith*, 442 U.S. at 743-44.

6 18 U.S.C. §§ 2701–2712 (2012); *see also* S. REP. NO. 99-541, at 1 (1986) ("The bill . . . update[s] and clarif[ies] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

communications from a third-party provider must first obtain a court order, subpoena, or even the kind of traditional search warrant requiring probable cause originally envisioned by the Fourth Amendment.[7] Arguably detracting from those procedural protections, however, the Act also allows government entities requesting these various orders—including search warrants—to also ask that the issuing court "preclude notice" to parties other than the direct recipient in certain circumstances.[8] These so-called "gag" orders bar the third-party Internet intermediaries from disclosing to the actual subjects of an investigation and the public at large not only the contents of a government search warrant, but also its very existence. Consequentially, there is serious doubt about the constitutionality of gag orders under the First Amendment.

Part I of this Comment describes the process and pitfalls of government surveillance of individuals' speech via the intermediaries on which they rely to exchange information and ideas. This Part explores both the Fourth Amendment, in which the so-called third-party doctrine seemingly opens the floodgates to user communications held by intermediaries, and the SCA, which attempts—but, as I argue, ultimately fails—to reintroduce protections over this information when it is held in electronic storage. Because the surveillance in question targets people's communications, it implicates both privacy and speech concerns, though the latter is often improperly overlooked.

Part II introduces the SCA's problematic gag order provision and the various objections it has faced on First Amendment grounds, focusing on instances of government surveillance where the SCA requires a traditional search warrant with probable cause but the Fourth Amendment doctrine currently does not. Over the past few years, several online service providers that were served with warrants requiring them to turn over user communications to investigators have challenged individual notice-of-preclusion orders issued against them under the SCA, arguing that, as applied, they violate free speech principles. One company, Microsoft, went even further in 2016, directly suing the Department of Justice (DOJ) in federal court and alleging that the SCA's gag order provision on its face violates the First Amendment.[9] The earlier, particularized objections to specific gag orders have had varying degrees of success, resulting in a split among federal magistrate courts regarding the correct statutory interpretation of the SCA's gag-order provision, as well as its overall constitutionality under the First Amendment. Meanwhile, after surviving the

7 18 U.S.C. § 2703.

8 *Id.* § 2705(b).

9 *See* Kate Conger, *Microsoft Sues Justice Department for Transparency in Government Data Searches*, TECHCRUNCH (Apr. 14, 2016, 1:09 PM), https://techcrunch.com/2016/04/14/microsoft-sues-justice-department-for-transparency-in-government-data-searches/ [https://perma.cc/KH4E-R8Q7].

government's motion to dismiss its First Amendment claim in October 2017,[10] Microsoft volunteered to drop its lawsuit after the DOJ decided to adopt a new policy narrowing its guidelines on the circumstances under which its prosecutors requesting court-issued warrants should also pursue gag orders.[11] In assessing these various lawsuits, I also consider why these companies raised their claims in the first place, since online intermediaries have unique motives for challenging SCA-sanctioned gag orders on behalf of individual users and the public at large.

In Part III, I consider both the efficacy and effect of these legal challenges by Microsoft and other gagged Internet intermediaries. With respect to the merits of the tech companies' constitutional challenges to the SCA's nondisclosure provision, I argue that gag orders issued under the SCA run the serious risk of directly violating tech companies' First Amendment rights by acting as content-based[12] prior restraints[13] and therefore face a heavy presumption against their constitutionality. While the government does have a compelling interest in maintaining the integrity of its criminal investigations, the evidence indicates that in practice, gag orders issued under the SCA are typically far from "narrowly tailored" and therefore likely do not pass constitutional muster.[14] Here, a comparison to gag orders attached to National Security Letters (NSLs) sanctioned by the SCA and the ensuing legal challenges these orders have faced also contribute to my analysis. Furthermore, I consider in this Part whether gag orders under the SCA might amount to an indirect infringement on the First Amendment rights of other stakeholders—i.e., the true targets of the government surveillance at issue and perhaps even the public at large.

In terms of a potential solution to the constitutional problem of SCA-sanctioned gag orders, I conclude by assessing the impact of the 2017 DOJ guidelines that were announced in response to intermediaries' recent legal

---

10 Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017).

11 Cyrus Farivar, *DOJ Changes "Gag Order" Policy, Microsoft to Drop Lawsuit*, ARSTECHNICA (Oct. 24, 2017, 5:12 AM), https://arstechnica.com/tech-policy/2017/10/doj-changes-gag-order-policy-microsoft-to-drop-lawsuit/ [https://perma.cc/4ZQL-6XJT].

12 *See* R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 382, 387, 391 (1992) (holding that content-based regulations—government actions that restrict speech because of the subject matter or viewpoint that it conveys—are "presumptively invalid" and therefore subject to strict scrutiny).

13 *See* Neb. Press Ass'n v. Stuart, 427 U.S. 539, 556, 559 (1976) (holding that prior restraints, or orders that act to prevent speech before it occurs, "are the most serious and least tolerable infringement on First Amendment rights").

14 *See* First Amended Complaint for Declaratory Judgment ¶ 16, *Microsoft*, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 16-0538), 2016 WL 3381727 [hereinafter Microsoft Complaint] (claiming that over a twenty-month period ending in May, Microsoft received more than 3250 "secrecy orders" silencing the company from speaking about the government's attempts to compel disclosure of its customers' communications information, roughly 450 of which were attached to search warrants and of infinite duration).

challenges.[15] I argue that the new policy is a good start, as are nascent attempts to amend the SCA, but that a better reform would come from courts endeavoring to adjudicate the issue of gag orders imposed on intermediaries on First Amendment grounds. More broadly, a reinforcement of free-speech rights in the face of the growing prevalence of government surveillance and the use of constitutionally suspect gag orders on intermediaries could seemingly work to counteract the threat of shrinking privacy rights in the digital age, thereby fulfilling the initial promise of the SCA.

I. BACKGROUND: REACHING INTERMEDIARIES

As a general matter, the government's attempts to interfere with individuals' communications by targeting third-party intermediaries—the "weak links in the chain of communications"[16]—predate the Internet. *Lamont v. Postmaster General*, for example, concerned a federal statute's interference with individual speech (or at least individuals' ability to access speech) by dictating that the postal service—one of society's earliest and most prominent intermediation institutions with communications-privacy implications[17]—only deliver "communist political propaganda" to those who requested such material in writing.[18] *Bantam Books, Inc. v. Sullivan*, meanwhile, considered efforts by a state commission to disrupt the publishing of controversial literature by issuing notices to distributors of certain books and magazines stating that their contents were objectionable to its members.[19] Similarly, some three decades later, there was an attempt to reprimand a radio station for playing a tape of a conversation between labor officials in *Bartnicki v. Vopper*, even though the station had no role in making the secret recording (which might have violated federal wiretapping laws) and was merely sharing

15 Memorandum from Rod J. Rosenstein, Deputy Att'y Gen., to Heads of Dep't Law Enf't Components et al. (Oct. 19, 2017), https://assets.documentcloud.org/documents/4116326/Protective-Orders.pdf [https://perma.cc/ZM2C-7EN] [hereinafter Rosenstein Memo].

16 Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 70 (2006).

17 *See* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 553-54 (2007) (arguing that "the principle of communications privacy derives not from the Fourth Amendment or even from the Constitution at all," but rather from the 1792 Post Office Act and other eighteenth century statutes and customs).

18 372 U.S. 301, 307 (1965); *see also* Anuj C. Desai, *The Transformation of Statutes into Constitutional Law: How Early Post Office Policy Shaped Modern First Amendment Doctrine*, 58 HASTINGS L.J. 671, 718 (2007) (arguing that in *Lamont*, "the Court shaped an important principle of freedom-of-speech jurisprudence—the right to receive ideas—around the fact that the Post Office was the principal means of [meaning it had an effective monopoly over] long distance communication"). Note that this "right to receive" was articulated in Justice Brennan's concurrence in *Lamont*. 372 U.S. at 308 (Brennan, J., concurring).

19 372 U.S. 58, 58 (1963).

it with its listeners.[20] At issue in each of these three cases was speech that was effectively silenced not by directly pursuing the speakers and/or recipients, but instead by pressuring the third-party intermediaries on which they relied—here, post offices, book distributors, and radio stations—to pass along the communications in question. Here, the government attempted to indirectly reach and suppress the speech in question by imposing a so-called "chilling effect"[21] on the true targets.[22]

In some ways, the process of targeting intermediaries to disrupt the flow of information from publisher/speaker to reader/listener looks much the same in the twenty-first century, at a time when online communications are now at stake. In the 2015 circuit case *Backpages.com, LLC v. Dart*, for example, Judge Posner ridiculed an Illinois sheriff who, after failing in his ill-advised attempt to block Craigslist from listing "adult" services, tried to all but shut down a similar site called Backpage by sending notices to the third-party credit card companies it used that implied that he would prosecute these intermediaries if they continued to facilitate financial transactions for Backpage.[23] As *Lamont*, *Bantam Books*, *Bartnicki*, and eventually *Backpages.com* illustrated, however, such efforts to silence speech via intermediaries are not always successful. After all, the court in each case held that government officials' attempts to intimidate third parties into silencing speakers violated the First Amendment. Similarly, in cases involving the government's efforts to combat whistleblowing, courts typically protect the disseminators spreading leaks (at

---

20 532 U.S. 514, 518 (2001).

21 *See* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U. L. REV. 685, 693 (1978) ("A chilling effect occurs when individuals seeking to engage in activity protected by the [F]irst [A]mendment are deterred from so doing by governmental regulation not specifically directed at that protected activity.") Schauer notes that the Supreme Court first used the word "chill" in a First Amendment case in *Wieman v. Udegraff*, when Justice Frankfurter stated in his concurrence: "Such unwarranted inhibition . . . has an unmistakable tendency to *chill* that free play of the spirit which all teachers ought especially to cultivate and practice; it makes for caution and timidity in their associations by potential teachers." *Id.* at 685 & n.1 (quoting 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring) (emphasis added)). See Section III.B, *infra*, for discussion on the First Amendment's chilling effect doctrine.

22 As the *Bartnicki* Court explained,

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.

Bartnicki, 532 U.S. at 533 (quoting PRESIDENT'S COMM'N ON LAW ENF'T & ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967)).

23 807 F.3d 229, 231-33 (7th Cir. 2015).

least if the information being shared was determined to have been obtained through innocuous means).[24]

Elsewhere, however, where the government officials are not necessarily trying to take information offline but are rather seeking evidence related to a distinct domestic crime, they appear more capable of reaching third-party intermediaries in pursuit of surveillance that can be used to incriminate individuals who use these services to communicate. Here, the Fourth Amendment gives the government wide latitude to reach intermediaries, but the practice of targeting individual speech via its third-party disseminators arguably still has important First Amendment implications in terms of its chilling effect.[25] As described below, the overall ease with which the government was able to access information held by intermediaries under the Fourth Amendment, at a time when surveillance was becoming more invasive as intermediation technology and intelligence-gathering tactics were quickly advancing, led lawmakers to pass the Stored Communications Act.[26] This statute attempted to close the chasm of constitutional questions left open by the Fourth Amendment's third-party doctrine, in part by requiring that surveillance of certain online communications be accompanied by a warrant.[27]

---

24 *See, e.g.*, Butterworth v. Smith, 494 U.S. 624, 627-28, 636 (1990) (striking down on First Amendment grounds a state statute prohibiting grand jury witnesses from disclosing their own testimony in a case where the respondent sought to publish materials based on his grand jury testimony about misconduct by public officials); Fla. Star v. B.J.F., 491 U.S. 524, 527-28, 532 (1989) (holding that imposing civil sanctions on a newspaper pursuant to a state statute for publishing the name of a rape victim violated the First Amendment); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 105-06 (1979) (holding that a state court's writ of prohibition violated the First Amendment because it prevented newspapers from publishing the names of juvenile offenders without approval from the juvenile court); N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam) (reversing the decision to enjoin two newspapers from publishing a leaked classified study because the injunction served as a presumptively invalid prior restraint on speech). Sources, however, are much more likely to face prosecution over leaks. *See, e.g.*, United States v. Aguilar, 515 U.S. 593 (1995) (finding that a judge who disclosed information about a wiretap could not be prosecuted for obstruction of justice but could be subjected to criminal penalties for under a federal statute without violating the First Amendment); Haig v. Agee, 453 U.S. 280, 306, 309-10 (1982) (upholding the Secretary of State's decision to revoke the passport of a former CIA employee who leaked information about CIA agents and sources); Snepp v. United States, 444 U.S. 507, 512-13 (1980) (holding that a CIA agent's publication of book about the agency's activities in Vietnam without submitting it to the agency for prepublication review breached his fiduciary duty). High-profile examples of whistleblowers targeted by the government rather than the disseminators that spread the leaks include Daniel Ellsberg, Edward Snowden, Michael Flynn, and Reality Winner.

25 *See, e.g.*, United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms."); Abdo, *supra* note 3, at 447 ("[T]his new surveillance state of affairs comes at considerable cost to the freedom to dissent."). *Contra* Laird v. Tatum, 408 U.S. 1, 13-14 (1972) (holding that any chilling effect caused by the U.S. Army's surveillance of civilians' lawful political activity was an insufficient basis for standing).

26 *Infra* Section I.B.

27 *Infra* Section I.B.

But the SCA, put into effect decades before most of the ways people communicate today were invented, much less imagined, raises critical free-speech concerns of its own. In particular, where the SCA requires the government to acquire a traditional search warrant, its gag order provision still enables the silencing of speech that the speakers—here, Internet intermediaries—seem to have a constitutional right to express. Perhaps even more troubling, this speech arguably needs to be heard by the true surveillance targets seeking due process, as well as the public hoping to enjoy a healthy debate in Justice Oliver Wendell Holmes's "marketplace of ideas" over the current state of privacy rights.[28]

A. *Constitutional Gap: The Fourth Amendment's Third-Party Doctrine*

It is worth considering how the government is able to access individuals' communications via intermediaries, given that the Fourth Amendment protects against "unreasonable searches and seizures," thereby requiring law enforcement agencies to obtain warrants with probable cause.[29] In *Ex parte Jackson*, perhaps the first Supreme Court case to consider what protections, if any, should be afforded to communications held by intermediaries,[30] "the secrecy of letters [traveling through the postal service] and such sealed packages in the mail" was confirmed under the Fourth Amendment,[31] with further reference to the freedom of the press.[32] Despite the finding in *Jackson* that the Fourth Amendment protected sealed letters even when they were out of the home and in transit, some fifty years later the Court articulated in *Olmstead v. United States* a more formal approach, holding that violations of privacy only

---

28 *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . . ").

29 U.S. CONST. amend. IV.

30 Although *Jackson* might have been the first time the Supreme Court considered value of privacy over communications shared in the mail, this principle has been embedded in statutes and policies governing the U.S. postal service since the eighteenth century. *See* Desai, *supra* note 17, at 577 ("It was this congressional action [making it a crime for postal workers to "unlawfully" open sealed letters], not the adoption of the Fourth Amendment, that eventually led to the Fourth Amendment principle in *Ex parte Jackson*.").

31 96 U.S. 727, 733 (1877). The Court stated: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, *wherever they may be*." *Id.* (emphasis added). Note that while the Court ruled that the government would need a search warrant to access the content of sealed letters in the mail, it did not extend this protection to the routing information communicated on the envelope.

32 *See id.* ("Liberty of circulating is as essential to that freedom as liberty of publishing; indeed, without the circulation, the publication would be of little value."). Here, *Jackson* presciently underscores the interplay between the right to privacy and the freedom of expression.

occur where there are acts of physical trespass.[33] This reading of the Fourth Amendment notably ignored the warning in Justice Louis Brandeis's *Olmstead* dissent that because the framers of the Bill of Rights were unaware of new technologies that could eventually be used by the government to invade privacy, the Fourth Amendment's scope should be interpreted more flexibly, beyond an inquiry into a mere physical invasion of privacy.[34] Some forty years later, *Katz v. United States*, a case involving investigators bugging a public telephone booth, developed a more modern approach to the Fourth Amendment that addressed Justice Brandeis's criticisms by finding that the right to privacy "protects people, not places."[35] Justice Harlan's concurrence laid out a new, functional test that was eventually adopted by the Court: an unconstitutional search under the Fourth Amendment does not necessarily need to amount to a physical trespass, but rather must infringe on a reasonable expectation of privacy.[36]

Just how far this novel conception of privacy could reach was tested in *Smith v. Maryland*, a case that considered whether law enforcement's use of a pen register, a device that captures numbers dialed into a phone, constituted a search under the Fourth Amendment.[37] The Court found that this method of surveillance was not a search, and therefore did not require a warrant, because the caller "voluntarily conveyed numerical information to the telephone company," and therefore could not have a reasonable

---

33 *See* 277 U.S. 438, 466 (1928) (holding that evidence obtained by a wiretap without a warrant did not violate the Fourth Amendment because the wiretap, which was set up by placing equipment in the street and in the basement of a large office building near the defendant's house, did not involve an actual physical trespass of his home), *overruled in part*, Katz v. United States, 389 U.S. 347 (1967).

34 As Justice Brandeis warned in his dissent:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers . . . will be enabled to expose to a jury the most intimate occurrences of the home.

Id. at 474 (Brandeis, J., dissenting).

35 *See Katz*, 389 U.S. at 351 (holding that the FBI's bugging of a public telephone booth used by a criminal suspect violated the Fourth Amendment because although the communications took place outside of private property and without physical trespass, there was a reasonable expectation of privacy in such a space). Note that just before the Court ruled on *Katz*, that same year it invalidated a state law that allowed for electronic eavesdropping without obtaining a warrant under the Fourth Amendment. Berger v. New York, 388 U.S. 41 (1967). A few years after *Katz*, the Supreme Court in the *Keith* case similarly invalidated a wiretap obtained without a warrant and used to investigate a domesticated terror threat—but left open the possibility for warrantless searches related to terrorism as well as foreign powers and their agents. United States v. U.S. Dist. Court for the E. Dist. of Mich. (*Keith*), 407 U.S. 297, 308-09, 324 (1972).

36 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

37 442 U.S. 735, 742 (1979).

expectation of privacy over this information.[38] By the Court's rationale, when an individual shares information with a third party, be it in direct conversation with another human being (even one surreptitiously wearing a wire monitored by investigators[39]) or by indirectly dialing digits of a phone number relayed to a telephone company, he or she "assume[s] the risk that the information would be divulged to police."[40]

Justice Thurgood Marshall's dissent in *Smith* raises important challenges to *Smith*'s third-party doctrine, arguing that the majority's finding that the speaker voluntarily assumed the risk that the telephone company would relay his speech to the government presupposes a choice that might not have existed even in the 1970s, at a time when the use of telephones was already integral to participating in modern society.[41] This rebuttal seems to ring all the more true today in the digital age. Can individuals seeking to keep their communications private and out of the hands (or ears) of government surveillance realistically make a choice to avoid interacting with third parties in the twenty-first century?[42] If even plausible, since these days all communications seem to necessarily flow through some kind of intermediation, the result would arguably look like the effective silencing of speakers ruled unconstitutional under the First Amendment in cases like *Lamont* and *Bartnicki*. Indeed, Justice Marshall, dissenting in *Smith*, touched on the chilling effect that he feared the Fourth Amendment's third-party doctrine would have on free speech rights: "The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of

---

38 *Id.* at 744; *see also* United States v. Miller, 425 U.S. 435, 442 (1976) (holding that a bank customer similarly had no reasonable expectation of privacy in cancelled checks and other transactional information held by his bank—even though the records in question were "voluntarily conveyed . . . in the ordinary course of business" to the bank in compliance with a federal statute compelling their disclosure).

39 *See* United States v. White, 401 U.S. 745, 745 (1971) (holding that under the Fourth Amendment there is no distinction between the voluntary sharing of information with a third party who then either reports to the police or who allows law enforcement agents to listen in with an eavesdropping device). *But see id.* at 759 (Brennan, J., dissenting) ("The risk of being overheard by an eavesdropper . . . . is the kind of risk we necessarily assume whenever we speak. But as soon as electronic surveillance comes into play, the risk changes crucially.").

40 *Smith*, 442 U.S. at 745.

41 *Id.* at 751 (Marshall, J., dissenting) ("To hold [that the defendant assumed the risk by choosing to place a phone call] ignores the vital role telephonic communication plays in our personal and professional relationships.").

42 *See, e.g.*, Tim Fernolz, *More People Around the World Have Cell Phones Than Ever Had Land-Lines*, QUARTZ (Feb. 25, 2014), https://qz.com/179897/more-people-around-the-world-have-cell-phones-than-ever-had-land-lines/ [https://perma.cc/U3CQ-498P] ("There are almost as many cell-phone subscriptions . . . as there are people on this earth . . . . Shouting is likely the next-most widespread communications technique . . . .").

unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts."[43]

Furthermore, the fact that the defendant in *Smith* "conveyed" to the phone company the numbers he dialed—rather than the actual contents of his call (or even confirmation that he did in fact place a call)—exacerbates the tension between privacy law's third-party doctrine and modern-day technology that individuals use to communicate and express themselves. In *Smith*, the Court found that the defendant knew or should have known he was passing this metadata-type information along to a third party,[44] but it is less clear if individuals today fully recognize the scope of the noncontent information they share with modern-day third-party intermediaries.[45] Unique to twenty-first century surveillance is the convergence of 1) "[t]he exploding collection of consumer information by private sector actors[,] . . . produc[ing] enormous pools of information which can be adapted to domestic surveillance"; 2) law enforcement agencies' increasingly powerful data aggregation techniques for obtaining and "adapting" this data; and 3) the willingness of these different agencies to share with one another the information they gather.[46] As Professor Kreimer notes, together, these modern trends are not only "able to transcend the practical obscurity"[47] that "previously attended the size and difficulty of accessing large amounts of data . . . but they are able as well to engage in 'data mining' to discover information that was previously only implicit in available data."[48] As a result, not only are the contents of communications susceptible to government surveillance under *Smith*'s third-

43 *Smith*, 42 U.S. at 751 (Marshall, J., dissenting) (citing NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 463 (1958)).

44 *Id.* at 742.

45 Stewart Baker, Smith v. Maryland *as a Good First-Order Estimate of Reasonable Privacy Expectations*, WASH. POST: THE VOLOKH CONSPIRACY (May 4, 2014, 3:15 PM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/04/smith-v-maryland-as-a-good-first-order-estimate-of-reasonable-privacy-expectations/ [https://perma.cc/XC65-FP4L] ("By now everyone understands the social media business model; we're getting the service because we are giving up the data. And most of us have been occasionally surprised and disconcerted by the ways in which the data has been used.").

46 Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 157 (2004) (comparing the political surveillance in the 1970s—citing, among other cases, *Lamont v. Postmaster General*, 381 U.S. 301 (1965), *Laird v. Tatum*, 408 U.S. 1 (1972), and *United States v. U.S. Dist. Court for the E. Dist. of Mich.* (*Keith*), 407 U.S. 297 (1972)—to the enhanced techniques available to government actors in the post-9/11 era).

47 *Id.* at 161; *see also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762 (1989) (holding that even though bits of "practical[ly] obscure[d]" information about individuals' criminal history were publicly available, rap sheets that aggregated these records into comprehensive reports were deserving of protection under the Fourth Amendment because the information was not easily accessible in the initial isolated format).

48 Kreimer, *supra* note 46, at 161; *see also* Abdo, *supra* note 3, at 446 ("The crucial advance of modern surveillance has been the development of inexpensive automation. . . . The government's appetite for digitally collected data has grown in conjunction with its capabilities for collection and analysis.").

party doctrine, but so too are the bits of contextual noncontent information that accompany those communications, which, when aggregated, can reveal a surprising amount about individual communications. This effectively makes speech all the more vulnerable in the age of Internet intermediation and high-tech government surveillance.

In terms of free speech implications, these modern-day concerns are perhaps the reason some have argued that phone numbers, location information, and other forms of noncontent metadata can be construed as speech deserving direct protection under the First Amendment.[49] Alternatively, and perhaps more persuasively, Justice Sonia Sotomayor recently revived Justice Marshall's First Amendment-based concerns over the third-party doctrine's chilling effect on speech in her concurring opinion in *United States v. Jones*.[50] There, the Court held that a GPS tracking device placed by investigators on a criminal suspect's vehicle constituted a search under the Fourth Amendment—not necessarily based on a *Katz*-like reasonable expectation of privacy inquiry, but instead because there was a physical trespass akin to the old *Olmstead* standard.[51] Inviting the Court to reconsider *Smith*'s third-party doctrine, Justice Sotomayor questioned "whether people *reasonably expect* that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[52] Here, Justice Sotomayor touched on what Professor Kerr calls "the mosaic theory,"[53] which stands in opposition to old notions of "practical obscurity" that suggest

---

49 *See, e.g.*, Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 61, 63 (2014) ("If the dissemination of mechanical recordings receives First Amendment protection (which it does), then the creation of those same recordings must have First Amendment significance, too." (footnote omitted) (citing Bartnicki v. Vopper, 532 U.S. 514, 527 (2001)); Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record,* 159 U. PA. L. REV. 335, 339 (2011) (questioning the distinction between mechanically recorded information and protected speech in the context of personal image capture); Andrew Crocker, Note, *Trackers That Make Phone Calls: Considering First Amendment Protection for Location Data*, 26 HARV. J.L. & TECH. 619, 623 (2013) ("[T]he collection of location data can be highly revealing of political activity and, under certain circumstances, can even constitute speech under the First Amendment.").

50 565 U.S. 400, 413-19 (2012) (Sotomayor, J., concurring).

51 *Id.* at 406 n.3 (2012) (majority opinion) ("Whatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment"). By reviving the physical trespass rule, the Court was able to issue a narrow holding and avoid a reassessment of *Katz*'s reasonable expectation of privacy test and *Smith*'s third-party doctrine.

52 *Id.* at 416 (Sotomayor, J., concurring) (emphasis added).

53 "[I]ndividual pieces of the puzzle that seemed small in isolation could be assembled together like a mosaic to reveal the full picture of a person's life." Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 325 (2012). Note that Kerr criticizes the mosaic approach and argues that questions about the Fourth Amendment's protection over the use of new technologies would be better addressed by a *Katz*-based reasonable expectation of privacy analysis. *Id.* at 343-52.

there is an inherent privacy value in large amounts of data because of the difficulty in finding the proverbial needle in a haystack.[54] The mosaic theory, on the other hand, stresses that today, the aggregating of information into one cohesive dataset that is otherwise disparately available has the power to significantly transform the nature and value of the information and reveal a "big picture" that was otherwise once hidden in plain sight.[55] Justice Sotomayor also indirectly addressed the chilling effect that surveillance of intermediaries can have on individual speakers under the First Amendment, noting that "[a]wareness that the government may be watching chills associational and expressive freedoms."[56] This finding underscores the often overlooked interplay and tension between the First and Fourth Amendments in the context of the government surveilling individual communications.

The Supreme Court has since taken Justice Sotomayor up on her invitation to review the third-party doctrine in the digital age, and this Term will decide *United States v. Carpenter*,[57] yet another Fourth Amendment phone metadata surveillance case that, like *Smith* and, more recently, *Jones*, "has clear implications for First Amendment freedoms, too—particularly the ability to express dissent . . . [which] requires privacy and often confidential association to flourish."[58] In *Carpenter*, investigators obtained from a cell phone company[59] a criminal suspect's cell site location information (CSLI)[60] over a period of four months which, when aggregated, helped triangulate the defendant's location and show that he was consistently in the same area

54 *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762 (1989).

55 Kerr, *supra* note 53, at 325; *see also* Kreimer, *supra* note 46, at 160-62 ("[T]he exponential increase in the capacity to aggregate and analyze information obtained by noncoercive and non-surreptitious measures gives government the opportunity to acquire vastly more extensive and penetrating oversight . . . .").

56 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Note that the Court appears somewhat divided on the role a chilling effect should play in First Amendment jurisprudence. Whereas *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), *Shelton v. Tucker*, 364 U.S. 479 (1960), and *Lamont v. Postmaster General*, 381 U.S. 301 (1965), among other key First Amendment cases, all expressed concern with the chilling effect of government surveillance, the Court held in *Laird v. Tatum*, 408 U.S. 1 (1972), that such "subjective" effects do not amount to standing to challenge such surveillance on First Amendment grounds.

57 819 F.3d 880 (6th Cir. 2012), *cert. granted*, 137 S. Ct. 2211 (2017).

58 Abdo, *supra*, note 3, at 444 (arguing that a First Amendment-based analysis could better protect against overreaching government surveillance than the current application of Forth Amendment doctrine).

59 The suspect was accused of stealing cell phones and was somewhat ironically incriminated by his own. *Carpenter*, 819 F.3d at 884.

60 CSLI is the metadata produced from a cellphone constantly sending signals to nearby towers to find service. *Id.* at 885. This information shows how the call was made, but not the content of the communication itself. It is unique in that it is much more exposing than the phone numbers picked up from the pen register device in *Smith* (which was determined to be a *constitutional* search) but less revealing than the GPS data tracked in *Jones*, which could have unveiled a much more concrete location point (and which was found to be an *unconstitutional* search).

where a series of armed robberies took place.[61] The Sixth Circuit held that no search warrant was required under the third-party doctrine,[62] although critics—and Justice Sotomayor's "mosaic theory"-based concurrence in *Jones*—warn that law enforcement agencies' cutting-edge data aggregation techniques[63] make the surveillance methods like the one used in *Carpenter* reveal much more about communications than could be picked up from a person overhearing the contents of a conversation or even a pen register device tracking digits dialed.[64] In light of the emergence of new communications and surveillance technologies, *Carpenter* will present the Supreme Court with an opportunity to shift the current trajectory of privacy claims concerning speech and communications. One approach might argue that, with privacy rights under threat by the Fourth Amendment's third-party doctrine, a reinforcement of First Amendment freedoms could serve as a kind of shield in an age where intermediaries are all but necessary for individuals to communicate, both in terms of direct speech and the contextual information that is passed along incidentally.[65]

---

61 *Id.* at 888 (holding that *Smith*'s third-party doctrine applies to the location data at issue here because "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."). The CSLI collected by the government over those four months also revealed lots of personal details about Carpenter's daily life, such as the days on which he attended church. *See Planet Money: Your Cellphone's a Snitch*, NPR (Nov. 8, 2017), https://www.npr.org/sections/money/2017/11/08/562888974/episode-804-your-cell-phones-a-snitch [https://perma.cc/MEB6-LLTJ] [hereinafter *Planet Money*].

62 *Carpenter*, 819 F.3d at 888-90. Note that the criminal law enforcement agents here did obtain a court order for the data under the Stored Communications Act, *id.* at 886, which only requires a showing of "reasonable grounds" for believing that the records sought were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d) (2012); *see also* subsection I.B.i (discussing the Stored Communications Act).

63 In an interview, Carpenter's lawyer noted that in the course of discovery, government investigators turned over a scan of a PDF of a spreadsheet, which meant that the defense team had to manually recreate the 7000 rows of location data before they could run their own aggregation analysis on the information collected by the government which, in its raw form, was essentially meaningless. *Planet Money*, *supra* note 61.

64 *See, e.g.*, James G. McLeod, *All Things in Aggregation: Reassessing the Fourth Amendment's Third-Party Doctrine and the Fourth Circuit's Approach to Cell Site Location Information in* United States v. Graham, 96 N.C. L. REV. 1203 (2018) (discussing the privacy-related consequences of allowing aggregate third-party data like CSLI under the third-party doctrine); Paul Rosenzweig, *In Defense of the Mosaic Theory*, LAWFARE (Nov. 29, 2017, 3:18 PM), https://www.lawfareblog.com/defense-mosaic-theory [https://perma.cc/2TP2-MLK2] ("The fundamental idea [behind the "mosaic theory"] is that aggregations of data create information beyond their individual value. 1+1+1 equals 17, not just 3.").

65 Alex Abdo argued that the Court should approach *Carpenter* with a First Amendment analysis, which

> 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. . . .

Until then, however, the Fourth Amendment's third-party doctrine articulated by *Smith* can still be viewed as opening the floodgates to government surveillance of individual communications.

B. *Statutory Rebuttal: The Electronic Communications Privacy Act*

In response to this chasm created by *Smith*, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986, not to necessarily altogether stop, but to at least better control the third-party doctrine's flow of information to government investigators and its chilling effect.[66] The statute's scope is broad, simultaneously amending and adding to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the original wiretap statute).[67] A complex law organized into three titles, ECPA sets different standards under which the government can obtain user electronic communications in the context of domestic criminal investigations, establishing a kind of graduated scale of procedural protections.[68] Crucially, ECPA protections apply even where there is no recognized reasonable expectation of privacy under the Fourth Amendment.[69] Its stated purpose is to find a balance that "protect[s] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."[70]

To this end, Title I of ECPA—directly responding to eavesdropping-related cases like *Olmstead*, *Katz*, and *Berger v. New York*—amended the Wiretap Act to strengthen statutory regulations related to the interception of communications in transit.[71] Here, to receive a court's authorization to use a

> 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.

Abdo, *supra* note 3, at 456.

66 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2511–2522 (2012)).

67 S. REP. 99-541, at 3 (1986); *see also* Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1701, 1704 (2004) ("At a very general level, the law of electronic surveillance recognizes two things: that government surveillance is good and that it is bad.").

68 18 U.S.C. §§ 2511–2522; *see also* Solove, *supra* note 67, at 1279. The scale ranges from "administrative subpoenas" that do not require court involvement, to "court orders" that typically require certification that there is "reason to believe" the information sought is related to a criminal investigation, Fourth Amendment-like search warrants requiring probable cause and finally, on the other end of the spectrum, "super" search warrants that require a showing more burdensome than traditional probable cause. *Id*.

69 Baker, *supra* note 45 ("ECPA is remarkably fine-tuned, setting several different standards for government access to different kinds of private communications, all of them higher than the default that *Smith* offers.").

70 S. REP. 99-541, at 3.

71 Electronic Communications Privacy Act of 1986, tit. I, §§ 101, 106 (codified as amended at 18 U.S.C. § 2518).

wiretap for the purpose of a criminal investigation, the government must meet certain standards that are actually much more burdensome than those imposed by a traditional search warrant requiring probable cause under the Fourth Amendment.[72] Applications for these so-called "'super' search warrants"[73] must contain details justifying the interception of communications in transit, information about how the interception will occur, and the duration of the wiretap.[74] They can only be sought by high-level government prosecutors and are limited to certain crimes (i.e., felonies).[75] The granting judge, meanwhile, must find probable cause for the belief that an individual "is committing, has committed, or is about to commit a particular offense"; that "particular communications concerning that offense will be obtained through such interception"; and that there are no reasonable alternatives in terms of investigative procedures.[76] The surveillance of communications in transit must also be "conducted in such a way as to minimize the interception of communications" outside the scope of the court order.[77] Lastly, the amended Wiretap Act requires that reports on the surveillance it permits and denies be published and made available to Congress and the public, a boon to the marketplace of ideas.[78]

On the other end of ECPA's spectrum of privacy protections, Title III established the Pen Register Act (PRA), which requires law enforcement agents seeking the use of a pen register device in a criminal investigation to first obtain a court order from a judge by merely certifying that "the information likely to be obtained by such installation and use is *relevant to an ongoing criminal investigation*."[79] The threshold for meeting this standard is significantly lower than that of a traditional search warrant requiring probable cause under the Fourth Amendment—and in fact, of ECPA's three titles, it is the lowest standard required for obtaining any kind of order granting an

---

72 *Id.* In other ways, however, court orders under the Wiretap Act are broader than warrants under the Fourth Amendment. For example, with Title I, courts can authorize continuing surveillance, whereas under the Fourth Amendment, search warrants generally authorize a single entry. *Id.*

73 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1232 (2004).

74 18 U.S.C. § 2518(1)(b)–(e).

75 18 U.S.C. § 2516.

76 18 U.S.C. § 2518(3)(a)–(c).

77 18 U.S.C. § 2518(5).

78 18 U.S.C. § 2519; *see also, e.g.*, *Wiretap Reports 2016*, U.S. COURTS (Dec. 31, 2016), http://www.uscourts.gov/statistics-reports/wiretap-report-2016 [https://perma.cc/9PUV-VL43].

79 18 U.S.C. § 3123(a)(1) (emphasis added). The statute specifically covers pen registers (which capture *outgoing* phone numbers) as well as trap-and-trace devices (which show *incoming* phone numbers), but Section 214 of the PATRIOT Act broadened its scope to cover similar devices monitoring the addressing of online communications, such as email headers. Pub. L. No. 107-56, § 214, 115 Stat. 286-87 (2001).

interception of communications.[80] Nonetheless, the PRA imposes at the very least a *degree* of privacy protections over the information obtained through the use of a pen register device—and therefore, this statute is clearly designed to undercut *Smith*, in which the Court, only six years prior, ruled that law enforcement agencies' use of such a device did not need to meet *any* procedural safeguards under the Fourth Amendment.[81]

The distinction between ECPA's standards regulating the government's ability to access a wiretap versus a pen register signifies that in 1986, Congress viewed interceptions of the actual content of communications to be much more revealing—and therefore more threatening to personal liberty under the First and Fourth Amendments—than the noncontent information inherent to those communications. This assumption, which was recently questioned by Justice Sotomayor's concurrence in *Jones* and is now before the Supreme Court in *Carpenter*, also informs ECPA's approach to stored communications, as discussed below. As communications intermediaries become more sophisticated in their ability to capture both content and noncontent information simultaneously and in myriad ways, today this discrepancy seems arbitrary and informs much criticism of the statute.[82] But regardless of their distinct approaches to regulating different aspects of communications, Titles I and III of ECPA more broadly illustrate Congress's willingness to rebut and rework past judicial interpretations of the constitutional protections (or lack thereof) afforded to individuals' speech that flows through third-party intermediaries.

1. The Stored Communications Act and its Discontents

With Title II of ECPA, or the Stored Communications Act, as it is referred to herein, Congress ventured even further in its cause to undercut the Fourth Amendment's third-party doctrine by applying (or eliminating) certain safeguards to electronic communications held in storage by intermediaries. Like the other titles of ECPA, this law attempts to enhance privacy protections over communications where the Fourth Amendment appears to have stripped them away. In particular, the SCA addresses the rise of new communications technologies that had not been considered by the Supreme Court in *Katz*, *Smith*, or the other 1960s- and 1970s-era Fourth Amendment doctrine cases and that would not necessarily be subject to either

80 18 U.S.C. §§ 2510–2522.

81 Smith v. Maryland, 442 U.S. 735, 742 (1979); *see also supra* notes 37-47 and accompanying text (discussing *Smith*).

82 *See, e.g.*, Orin S. Kerr, *The Next Generation Communications Act*, 162 U. PA. L. REV. 373, 386-90 (2014) (describing the Digital Due Process Coalition's criticisms of the ECPA and its proposals to change parts of the statute).

Title I's Wiretap Act or Title III's PRA. At the time of ECPA's passage into law, Congress was seemingly aware of the fact that:

> Our most private information ends up being sent to private third parties and held far away on remote network servers. This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all.[83]

Here, the SCA's drafters deserve credit for presciently recognizing that as new communications technologies emerged, they would continue to rely on third-party intermediation, thereby effectively missing out on constitutional protections under the Fourth Amendment. The legislative history, as well as the actual substance of the law, indicates that Congress intended to right this perceived wrong by ensuring that "the law . . . advance[s] with the technology to ensure the continued vitality of the Fourth Amendment . . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right."[84] Whereas the Fourth Amendment's third-party doctrine seems stagnant and agnostic toward new technology, the SCA's approach is forward-looking, anticipating new modes of communication at a time when the Internet was barely in its infancy and the World Wide Web had not yet been invented.[85] Indeed, many of the ways in which people consistently communicate today had not even been conceived of in 1986.

But therein lies the problem, and the arguable failure, of the SCA today: because Congress could not have predicted many of the advancements in electronic intermediation that have taken place over the last few decades, the key distinctions it draws between certain kinds of government surveillance actions and types of communications storage forms are seemingly arbitrary and largely unworkable in a modern-day context.[86] In fact, as written in 1986 (granted, with considerable amendments) and employed in the twenty-first century, the SCA arguably impairs rather than protects individuals' privacy rights related to online communications through third-party intermediaries. Perhaps most problematic are the gag orders the statute permits, which, as discussed below, raise serious doubt as to their constitutionality under the First Amendment.

---

83 Kerr, *supra* note 73, at 1209-10.

84 S. REP. 99-541, *supra* note 67, at 5. This is an interesting justification for ECPA, given the Supreme Court's recent return to *Olmstead*'s physical trespass standard in *Jones*.

85 *See* CHRISTOPHER S. YOO, THE DYNAMIC INTERNET 21 fig.2-2 (2012) (charting "Annual Growth Rates for U.S. Internet Traffic" from 1990–2009).

86 *See* Kerr, *supra* note 82, at 396 ("ECPA was an impressive achievement in its day. A quarter century later, however, it has become commonplace to recognize that ECPA is outdated.").

In terms of substance, broadly speaking the SCA, under 18 U.S.C. § 2703, covers communications in "electronic storage," meaning "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[87] The statute "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."[88] In particular, these regulated intermediaries are electronic communication service providers (ECS)—i.e., Internet service providers and telecommunications companies that carry Internet traffic—or remote computing services providers (RCS)—i.e., cloud computing systems.[89] The SCA treats communications stored with these intermediaries slightly differently, but today, in the age of constant and ubiquitous Internet access and seemingly unlimited cloud computing capacity, any subtle differences between the two are likely meaningless to the average Internet user.

Like with the overall ECPA statute, embedded in the SCA itself is a graduated scale of procedural standards that law enforcement officials must meet in order to access these communications for the purposes of criminal surveillance.[90] At the bottom rung, the government can compel an ECS or RCS provider to disclose basic subscriber information related to a user's identity through a simple subpoena, which does not even require so much as a judge's approval.[91] To access other forms of subscriber information, investigators must obtain a court order oftentimes referred to as a "§ 2703(d) order," by showing "reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." [92] Note that here, the SCA echoes the PRA's—and apparently the Fourth Amendment's—relatively lax privacy protections afforded to noncontent information as compared to the actual contents of communications. This distinction might have made sense in 1986 and before, when the contextual information surrounding communications was likely not

87 18 U.S.C. § 2510 (2012).

88 Kerr, *supra* note 73, at 1212.

89 18 U.S.C. § 2703.

90 *See* Kerr, *supra* note 73, at 1222 ("The rules for compelled disclosure operate like an upside-down pyramid. . . . The higher up the pyramid you go, the more information the government can obtain.").

91 18 U.S.C. § 2703(c)(2). These subscriber records include noncontent customer data held by Internet service providers, such as name, address, length of service, means of payment. *Id.*

92 18 U.S.C. § 2703(d); *accord* Kerr, *supra* note 73, at 1219.

as revealing in a world without commercial email, social media networks, etc.[93] Today, however, the low procedural protections afforded to online subscriber records are particularly troublesome in terms of free speech and expression rights, in part because this information can easily be used to "identify people using screen names or pseudonyms on the Internet. Thus, a person's First Amendment right to speak anonymously is implicated."[94]

As for the actual contents of communications (for example, the text of an email), the SCA confusingly provides different levels of protection against government surveillance depending in part on the age of the communication. Government officials seeking access to contents in electronic storage on a RCS or an ECS for *more* than 180 days only need a 2703(d) order or even a mere low-threshold subpoena, so long as there is prior notice (although that can be delayed in certain circumstances).[95] To compel emails in storage on an ECS provider for 180 days or *fewer*, law enforcement agents must apply for a regular search warrant with probable cause under the Federal Rules of Criminal Procedure (or under state procedures, as applicable), which comports with the Fourth Amendment.[96] As the highest level of protection provided to any communications under the SCA, here the statute essentially extends the reach of the Fourth Amendment to cover by statute government searches of certain electronically stored communications.

It is worth noting, however, that these distinctions are notoriously difficult to apply to today's stored communications and seemingly undermine the enhanced protections that the SCA set out to provide in response to the Fourth Amendment's perceived shortcomings. Consider the case of email, a mode of communication that was at best nascent in 1986 but today is arguably necessary to use in order to participate in modern society. Twenty-first century RCS providers can store essentially limitless amounts of email, casting further doubt on the need for the SCA's various standards of protection. Nevertheless, the statute treats emails stored under slightly different circumstances in starkly distinct ways. Under the SCA, the government can obtain an

---

93 *See, e.g.*, *Ex parte* Jackson, 96 U.S. 727 (1877) (finding a simple and logical distinction between the contents of sealed letters, which were protected from government surveillance under the Fourth Amendment, and the routing information contained on the outside of the envelope, which was, of course, not).

94 Solove, *supra* note 67, at 1724 (citing Talley v. California, 362 U.S. 60, 65 (1960)); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 374 (1995) (holding that a state statute banning anonymous campaign literature violates the First Amendment in part because the interest in having anonymous speech enter the marketplace of ideas outweighs the public interest in disclosure). *But see* Doe v. Reed, 561 U.S. 186, 201-02 (2010) (upholding state procedures requiring disclosure of signatures on a referendum against a First Amendment challenge because the government's interest in preserving the integrity of the electoral process outweighed the benefits of anonymous speech).

95 18 U.S.C. § 2703(b); Kerr, *supra* note 73, at 1219.

96 18 U.S.C. § 2703(a).

individual's basic subscriber information listed in § 2703(c)(2) with only a subpoena.[97] Other noncontent records require a court order under § 2703(d) based on a reasonable belief that the information sought is simply relevant in some way to "an ongoing criminal investigation."[98] Investigators seeking access to unopened email in electronic storage for more than 180 days must issue a subpoena with notice to the target.[99] Only for unopened email in electronic storage for 180 days or fewer must law enforcement agents seek a standard warrant requiring probable cause.[100] Still, questions on how to treat other types of email linger. For example, courts are split on whether opened email held in remote storage is considered a stored communications for the purposes of SCA,[101] and it is unclear if email in transit across a network is covered by the statute.[102] With this confusion in mind, the Sixth Circuit held in a 2010 case, *United States v. Warshak*, that all government interceptions of email first required a search warrant—not under the SCA, but rather under the Fourth Amendment because individuals have a "reasonable expectation of privacy" over their emails.[103] In fact, the *Warshak* court held that SCA provisions requiring anything less than a search warrant were unconstitutional.[104] But *Warshak* is not followed in other jurisdictions and the Supreme Court—which is responsible for the third-party doctrine that the SCA attempts to combat—has yet to address the issue.[105] In the interim, then, the SCA controls the surveillance of stored communications, even if it is near-impossible to apply to modern-day situations. This means that, despite Congress's apparent attempt to circumvent the third-party doctrine and restore privacy protections over individual communications, under the resulting statute, the government need only obtain a traditional search warrant requiring probable cause in cases where emails are stored by a third-party intermediary for 180 days or fewer.

---

97 Kerr, *supra* note 73, at 1223 tbl.1.

98 *Id.*

99 *Id.*

100 *Id.*

101 *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) (holding that email that has already been opened is still in storage for the purposes of the SCA). *But see* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (finding that once email has been opened, it has reached its final destination and is no longer stored for "backup" purposes under the SCA).

102 *See* United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (holding that interception of email in transit to its intended recipient is a violation of the Wiretap Act rather than the SCA because the "electronic communication" covered by the former statute includes transient electronic storage that is intrinsic to the communication process).

103 631 F.3d 266, 287 (6th Cir. 2010).

104 *Id.* at 288.

105 *Jones* and *Carpenter* did not concern email specifically but did provide the Supreme Court with an opportunity to broadly consider SCA's effect on the right to privacy and the freedom of expression.

The rest of this Comment will focus on this specific kind of circumstance, where the SCA imposes protections akin to the Fourth Amendment by requiring the government to obtain a traditional search warrant before reaching certain communications held by third-party intermediaries. Particular attention is paid to these warrants because they are the only instance where the SCA attempts to fully restore the constitutional privacy protections that were in place before the development of the third-party doctrine. Furthermore, SCA-sanctioned search warrants are especially noteworthy in terms of the privacy and speech rights they implicate, since in this context the government is required to comply with the most demanding process that the statute provides. Here, the SCA's gag order provision, discussed below, raises important free-speech concerns that ultimately undermine its attempt to close the third-party doctrine's gap, allowing government surveillance to seep into individuals' communications.

II. A PROBLEM IN PRACTICE: GAGGING INTERMEDIARIES

While the SCA faces numerous criticisms related to privacy and speech concerns, perhaps its provision most deserving of reproach is that which authorizes gag orders on the third-party intermediaries that are the recipients of the government search warrants required by the statute. This provision, which is constitutionally suspect under the First Amendment, is arguably responsible for the SCA's ultimate inability to achieve its goal of protecting individual communications in the face of the Fourth Amendment's third-party doctrine. Before touching on gag orders, the SCA, under § 2705(a), first outlines the circumstances under which law enforcement agencies seeking access to individuals' communications can delay notifying others of their pursuit.[106] Where a court order or administrative subpoena is sought, the requesting government entity can delay notification "for a period not to exceed ninety days," if, respectively, either the granting court determines or the supervisory official certifies "that there is reason to believe that notification of the existence of the [court order or subpoena] may have an adverse result."[107] "Adverse results" justifying delayed notification include "endangering the life or physical safety of an individual; . . . flight from prosecution; . . . destruction or tampering with evidence; . . . intimidation of potential witnesses"—a somewhat narrow list, with the exception of a catchall for circumstances "otherwise seriously jeopardizing an investigation or unduly delaying a trial."[108] If granted, such periods of delayed notification can be extended for ninety days at a time.[109]

106 18 U.S.C. § 2705(a)(1) (2012).
107 *Id.*
108 *Id.* § 2705(a)(2).
109 *Id.* § 2705(a)(4).

Under the SCA, there are no restrictions limiting law enforcement agents' ability to delay notification of search warrants.

Meanwhile, § 2705(b), the statute's gag order provision—which affects the ability of the intermediary-recipients of SCA-sanctioned court orders, subpoenas, and warrants to notify others of their existence—is keyed to its rules on notification delay by authorities. Here, a government entity can apply for a notice-of-preclusion order, under which the granting court can bar an ECS or RCS intermediary from speaking to anyone else about the disclosure it is compelled to reveal to investigators under § 2703, "to the extent that it may delay such notice" under § 2705(a).[110] Within those confines, the court "*shall*" impose what essentially is a gag order if "it determines there is mere "*reason to believe*" that notification will lead to one of the "adverse results" contemplated in § 2705(a): "endangering the life or physical safety of an individual; . . . flight from prosecution; . . . destruction or tampering with evidence; . . . intimidation of potential witnesses; . . . or otherwise seriously jeopardizing an investigation or unduly delaying a trial."[111] As discussed above, the catchall factor ensures that the scope of this provision is broad, as is the duty (rather than discretion) seemingly imposed on the court requiring it to bar disclosure if there is reason to believe one of the "adverse results" will follow.[112] Furthermore, as for the duration of these gag orders imposed on intermediaries, a granting court can issue them "for *such period* as [it] deems appropriate"—perhaps indefinitely, it seems, in instances where notices of preclusion are applied to search warrants.[113] As a result, "individuals targeted by electronic surveillance are kept unaware by the presence of gag orders silencing their search providers, and . . . law-abiding citizens never charged with a crime are prevented from ever learning of government intrusions into their electronic lives."[114]

The legal challenges to § 2705(b) described below suggest that many gag orders accompanying search warrants issued under the SCA are likely unconstitutional under the First Amendment. Furthermore, they also appear to undermine the statute's attempts to strengthen Fourth Amendment-like protections for communications via intermediaries, thereby highlighting the difficult interplay between privacy and speech rights today. Faced with the threat of shrinking privacy rights via increasingly sophisticated government

110 *Id.* § 2705(b).

111 *Id.* (emphasis added).

112 *Id.*; *see also* Al-Amyn Sumar, *Prior Restraints and Digital Surveillance: The Constitutionality of Gag Orders Issued Under the Stored Communications Act*, 20 YALE J.L. & TECH. 74, 86 (2018) ("The statute has a clearly broad sweep.").

113 18 U.S.C. § 2705(b) (emphasis added).

114 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 332 (2012).

surveillance under the outdated SCA, free speech rights in this context should be strengthened rather than restrained in order to protect individual speakers and the general public, whose communications are essentially at stake.

Similar arguments have been advanced against the SCA's gag order provision in recent years—not by individual targets of government surveillance or the public at large, but rather by the gagged third-party intermediaries themselves, who argue that their own First Amendment rights are directly infringed by § 2705(b). Whereas the development of the Fourth Amendment's third-party doctrine and the ensuing statutory response were shaped by the true targets of surveillance challenging government investigations in court, as well as public discourse concerning privacy rights and new modes of communications, in the context of gag orders issued under the SCA, the legal fight takes a very different form. Why the distinction? When intermediaries are barred from speaking about the search warrants issued on them under the SCA, speakers, listeners and any other parties interested in the targeted communications are unable to learn about the very existence of the surveillance in question, much less the details of the surveillance. It is virtually impossible for other stakeholders affected by the SCA's gag order provision to object to the surveillance practices and accompanying silencing orders when they have no way of knowing about them in the first place. Left in the dark, they instead must rely on the intermediaries to fight their free speech battles for them.

This Section introduces these legal challenges to a clear First Amendment issue embedded in Congress's statutory approach to privacy. It considers both as-applied challenges to specific SCA-sanctioned gag orders issued under particular circumstances, as well as a single facial challenge raising doubt as to the overall constitutionality of the statute's gag order provision. The unique motives driving Internet intermediaries to bring suit on behalf of others are also contemplated. But regardless of why U.S. tech companies are challenging § 2705(b), they are in effect arguing that as privacy rights continue to shrink in the digital age, free speech rights should be reinforced to fill the gap and restore the SCA's stated purpose: to provide measured protections against government surveillance of online communications.

A. *As-Applied Challenges: The District Court Split*

In recent years, some holders of users' electronic communications have decided to rise to the occasion, objecting in court to specific and seemingly indefinite notices of preclusion issued against them under the SCA in connection with a particular domestic criminal investigation and arguing that these individual gag orders violate their First Amendment rights. These cases, like the other "tens of thousands of secret cases every year . . . . classified

as 'warrant-type applications,'" are decided by federal magistrate judges who, as U.S. Magistrate Judge Stephen W. Smith readily admits, "are given no guidance in how to interpret or apply ECPA's complex provisions, and law enforcement is given free rein to push its surveillance power to whatever limits it chooses to recognize."[115] Under this regime,

> temporary sealing orders almost always become permanent. More often than not, judges set no expiration dates on these orders, but merely direct that they be sealed and not disclosed "until further order of the court." The reality is that magistrate judges almost never . . . revisit these cases, so the "further order" lifting the seal rarely arrives.[116]

Furthermore, "remarkably few appellate court opinions delve into ECPA's complexities as a matter of ordinary statutory interpretation."[117] As described below, the as-applied challenges to the SCA's gag order provision have had varying degrees of success, resulting in a split among district court magistrate judges regarding the correct statutory interpretation of the SCA's gag order provision, as well as its overall constitutionality under the First Amendment.

For example, in 2014, law enforcement agents in the Northern District of California sought not only a search warrant under § 2703 for certain emails held on Microsoft's servers, but also a notice of preclusion under § 2705(b) that did not specify an expiration date.[118] Raising claims under both the SCA itself and the First Amendment, Microsoft challenged the gag order, which, without an expiration date, appeared to bar the technology company from ever disclosing the existence of the warrant to any other party.[119] In *In re Search Warrant For: [Redacted]@hotmail.com* (*[Redacted]@hotmail.com*), the magistrate judge first acknowledged that the government had a compelling reason to issue a gag order of some kind, given that there was, under § 2705(b), reason to believe that disclosure of the warrant might "seriously jeopardize" the criminal investigation in question.[120] At issue, however, were the parameters of such an order, and in particular whether investigators could

---

115 *Id.* at 313, 315.

116 Smith, *supra* note 114, at 325 (footnoted omitted).

117 *Id.* at 326.

118 *[Redacted]@hotmail.com*, 74 F. Supp. 3d at 1185. Note that as discussed below, Microsoft has since made a separate facial challenge to the SCA's gag order provision. The company has also challenged the government's attempt to issue SCA-sanctioned search warrants on emails held on its foreign servers; the Supreme Court heard oral arguments on the SCA's reach in 2018 but did not decide the merits of the case. *See infra* note 176177 and accompanying text.

119 *Id.*

120 *Id.* Recall the catchall justification for the issuing of a gag order under § 2705(b). 18 U.S.C. § 2705(b) (2012). The government must only assert a "reason to believe" that disclosure would "seriously jeopardize" its investigation and does not need to show any particular facts to support this belief. *Id.*

gag Microsoft "well, forever."[121] The court held that under a "common sense" approach, the SCA's gag order provision, which enables courts to grant notices of preclusion "for such *period* as [they] deem appropriate,"[122] "clearly requires the court to define some kind of end. . . . Forever is by definition without an end."[123] Because the court held that the SCA did not in fact permit the government's indefinite gag order attached to a traditional search warrant in this particular case, the court conveniently did not have to consider the company's free speech claim, although it did note the importance of "the First Amendment rights of both Microsoft and the public, to say nothing of the rights of the target."[124]

Elsewhere, however, courts have found that § 2705(b) does not require an "end" or expiration date, thereby appearing to leave the matter of duration to the courts' discretion. Consider the challenge brought by Adobe to a seemingly indefinite order in 2017 in the Central District of California.[125] This case resulted from a warrant issued on Adobe, along with a notice of preclusion barring the company from disclosing the warrant's existence to the true target of the investigation or the public at large, all without "specify[ing] a duration" for the disclosure bar.[126] Adobe argued that this gag order undermined its policies of (1) notifying its subscribers whenever a third party requested their information (unless legally prohibited from doing so) and (2) disclosing to the public information about the government surveillance orders it receives by publishing a "Government Requests Transparency Report."[127] Furthermore, in terms of the gag order's duration, Adobe claimed that "an 'indeterminate' [notice of preclusion] has no time period at all."[128] As a matter of statutory interpretation, however, the court diverged from the holding in *[Redacted]@hotmail.com*, and found that the language of the SCA did not

121 *[Redacted]@hotmail.com*, 74 F. Supp. 3d at 1185.

122 18 U.S.C. § 2705(b) (emphasis added).

123 *[Redacted]@hotmail.com*, 74 F. Supp. 3d at 1186.

124 *Id.*

125 *In re* Search Warrant for [Redacted].com (*[Redacted].com*), 248 F. Supp. 3d 970, 973 (C.D. Cal. 2017).

126 *Id. See generally* Smith, *supra* note 114, at 325 ("The SCA does authorize the court to issue a gag order (called 'preclusion of notice') on service providers, commanding them not to notify any other person of the existence of the court order." (internal citation omitted)).

127 *Id.* at 973-74. Adobe's report from fiscal year 2016 indicates that of the forty-eight subpoenas, court orders, search warrants, etc., it received targeting user communications information, thirty of those came with delayed notice orders barring disclosure to others for some period of time. *Government Requests Transparency Report*, ADOBE (Dec. 13, 2016), https://www.adobe.com/legal/lawenforcementrequests/transparency-2016.html [https://perma.cc/9LC2-9A4E].

128 *[Redacted]@hotmail.com*, 74 F. Supp. 3d at 976.

require that the warrant issued against Adobe to be limited in duration by an expiration date.[129]

The federal magistrate judge in *[Redacted].com* was, however, persuaded by Adobe's argument that the gag order at issue, as applied indefinitely, violated the company's First Amendment rights.[130] The court held that gag orders are content-based prior restraints subject to strict scrutiny judicial review, which the indefinite notice of preclusion in this case did not satisfy because it was not narrowly tailored.[131] While the court reiterated that the government has a legitimate interest protecting the integrity of its criminal investigation, it found that, as applied, the gag order "at issue herein effectively bars Adobe's speech in perpetuity," despite the availability of less restrictive alternatives, such as setting a certain expiration date for the gag order and then applying for extensions as needed.[132] Ultimately, the court found that the indefinite gag order issued on Adobe did not violate the SCA, but still infringed on the affected intermediary's First Amendment rights, meaning that the government had to modify the order to include an end date.[133] Nonetheless, the court construed its holding narrowly, noting that it was not suggesting that *all* indefinite gag orders issued under § 2705(b) inherently violate the First Amendment.[134]

Finally, contrary to both the *[Redacted]@hotmail.com* and *[Redacted].com* courts, a district court in New Jersey recently held that a gag order attached to an SCA-sanctioned search warrant issued on Google survived *both* statutory and constitutional objections. Initially indefinite, the gag order at issue in *United States v. Search Warrant*, as amended, would expire if and when one of two possible events occurred: 1) the government concluded its investigation or 2) an indictment was returned and unsealed (although even if either of these conditions were triggered, law enforcement agents could petition the court to extend the order's duration).[135] Note that this event-based, rather than time-dependent, expiration, still seems to take the burden

---

129 *Id.* at 976–77. Here, the court relied on a dictionary definition of "period" provided in Webster's Third New International Dictionary, which states that a period is "a time often of indefinite length but of distinctive or specified character." *Id.* at 977 (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (2002)). The court also reasoned that because the SCA spelled out specific time limits on gag orders attached to subpoenas and court orders, principles of statutory construction suggest that the phrase "period," as applied to warrants, should not be interpreted so narrowly. *Id.*

130 *Id.* at 978-83.

131 *Id.* at 980-83 (citing, inter alia, *Alexander v. United States*, 509 U.S. 544 (1993), and *Ward v. Rock Against Racism*, 491 U.S. 781 (1989)).

132 *Id.* Note that the DOJ's new guidelines for prosecutors seeking gag orders requires them to apply for this "alternative" gag order that includes a clear expiration date. *See* Rosenstein Memo, *supra* note 15, at 2.

133 *[Redacted].com*, 248 F. Supp. 3d at 984.

134 *Id.* at 983.

135 No. 16-4116, 2017 U.S. Dist. LEXIS 148393, at *4 (D.N.J. Aug. 10, 2017).

off the government in terms of either narrowing the gag order's scope or justifying its breadth. Further, if the investigation continued indefinitely or no arrest was made, any surveillance targets found to be law-abiding citizens would likely never learn that their communications were accessed by the government.[136] Nevertheless, in response to Google's claim that this particular gag order violated the SCA's notice-of-preclusion rules by not including a time-based end, the court echoed the first part of the holding in *[Redacted].com*, concluding that "[t]he plain language of § 2705(b) makes clear that it does not require a fixed period."[137] The magistrate judge then held that this particular gag order also survived strict scrutiny under the First Amendment, because the government had a compelling interest in protecting its ongoing criminal investigation and the means through which it achieved this interest—essentially barring Google from notifying the target until the criminal investigation ended—was narrowly tailored.[138]

Overall, this split among federal magistrate courts is hard to make sense of and does little for the intermediaries seeking to assert their First Amendment rights against oppressive gag orders. Of course, it also hurts the true targets of government surveillance and the public, both of whose own privacy and speech rights are dependent on third-party legal challenges in this context.

B. *A Facial Challenge: The Microsoft Case*

As the cases above illustrate, the outcome of an as-applied challenge to an indefinite gag order attached to a search warrant under the SCA is unpredictable. Moreover, the process of objecting to individual, indefinite notices of preclusion can be taxing on even the largest and most resourceful online intermediaries, as measured by the sheer volume of orders issued against them. For instance, cloud computing services provider Microsoft stated that over a twenty-month period ending in May 2016, it received more than 3250 "secrecy orders" silencing the company from speaking about the government's attempts to compel disclosure of its customers' communications information.[139] According to Microsoft, at least 450 of those gag orders accompanied search warrants "and roughly 70 percent of those orders [attached to warrants] were of indefinite duration."[140] This data suggests that the practice of gagging intermediaries under the SCA has become the rule rather than the exception it should apparently be according to the stated purpose of

136 Smith, *supra* note 114, at 332.

137 *Search Warrant*, 2017 U.S. Dist. LEXIS 148393, at *6.

138 *Id.* at *13-15.

139 Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 897 (W.D. Wash. 2017).

140 Microsoft Complaint, *supra* note 14, ¶ 5.

the statute. It also partially explains the motivation behind Microsoft's recent facial challenge to § 2705(b) on constitutional grounds.

In 2016, Microsoft sued the DOJ in federal court, alleging that the SCA's gag order provision generally violates the First and Fourth Amendments.[141] In particular, the company claimed that § 2705(b) infringed on its First Amendment right to inform its customers about how "the government conducts its investigations" and its customers' Fourth Amendment right to know about the issuance of search warrants targeting individual communications held on its servers.[142] The DOJ, meanwhile, filed a motion to dismiss Microsoft's claims.[143] The district court dismissed Microsoft's Fourth Amendment claim after finding that the company lacked standing to raise claims about privacy rights on behalf of its users.[144] As the court acknowledged, this holding underscores the problematic relationship between privacy and speech rights of intermediaries and individuals:

> As Microsoft alleges, the indefinite nondisclosure orders allowed under Section 2705(b) mean that some customers may never know that the government has obtained information in which those customers have a reasonable expectation of privacy. . . . For this reason, some of Microsoft's customers will be practically unable to vindicate their own Fourth Amendment rights.[145]

This seemingly paradoxical aspect of *Microsoft* reveals a key distinction between legal challenges to government surveillance attempts to reach intermediaries that have been gagged and those that have not been gagged. In *Lamont*, *Bantam Books*, *Bartnicki*, and *Backpages*, the true targets of government surveillance were able to raise their own constitutional claims because they had standing; here, evidently no affected party other than the intermediary can sue, simply because no one else knows that there is a potential invasion of privacy to taking place. And yet in *Microsoft*, the intermediary was blocked from raising Fourth Amendment claims. This holding, then, might comport with the rules of civil procedure, but it undermines the SCA's intent: to better protect individual speech in the face of new modes of communication and increasingly sophisticated methods of government surveillance.

This unresolved tension might partially explain why, on the other hand, the *Microsoft* court upheld Microsoft's First Amendment claims against the DOJ's motion to dismiss. The court found that the company did have the

141 *Microsoft*, 233 F. Supp. 3d at 896.
142 *Id.* at 897.
143 *Id.*
144 *Id.* at 916.
145 *Id.*

requisite standing to raise a facial challenge to § 2705(b) on free speech grounds because "Microsoft ha[d] sufficiently alleged an injury-in-fact and a likelihood of future injury."[146] The court recognized that Microsoft had sufficiently stated a particularized claim by "alleg[ing] 'an invasion of' its 'legally protected interest' in speaking about government investigations."[147] It found that Microsoft had alleged a "concrete and particularized injury," based on its claim that it had "personally been subjected to thousands of indefinite non-disclosure orders that implicate its First Amendment Rights" and that there was no indication that the DOJ would cease seeking indefinite gag orders without the impacted intermediary raising specific challenges to each individual order.[148] These claims could proceed because the court held that they were related to Microsoft's personal constitutional right to speak about the search warrants it receives in connection with specific criminal investigations, and the claims did not represent generalized grievances on behalf of the public at large.[149]

In terms of substance, the court found that Microsoft sufficiently alleged that gag orders issued under § 2705(b) were content-based prior restraints.[150] In particular, Microsoft's claims against this provision of the statute— "that the gag orders can be of prolonged duration, that the 'reason to believe' standard is too permissive, and the statute is otherwise deficient"—survived the DOJ's motion to dismiss.[151] The company persuaded the court to treat these alleged infringements on its First Amendment rights with strict scrutiny because although "Microsoft acknowledged that gag orders might be permissible in exceptional circumstances, . . . the SCA's sweep, as effectuated by the government, had been obviously overbroad."[152] In other words, the government might at times have a compelling interest in issuing a gag order on intermediaries, but in practice, its nondisclosure orders, which at least when issued against Microsoft were mostly indefinite, were not narrowly tailored. The court described these indefinite gag orders as "analogous to permanent injunctions preventing speech from taking place before it occurs" and suggested that the government's procedural safeguards in place, if any, evidently did not do enough, since Microsoft was often silenced even after

146 *Id.* at 899.

147 *Id.* at 887.

148 *Id.* at 901.

149 *Id.*

150 *Id.* at 905. Furthermore, the court held that Microsoft's argument that "indefinite nondisclosure orders impermissibly burden [its] First Amendment rights" could survive even if the government was correct that a standard of judicial review lower than strict scrutiny should apply. *Id.* at 908.

151 Sumar, *supra* note 112, at 88 (citing *Microsoft*, 233 F. Supp. 3d. at 907-08).

152 *Id.* at 87; *accord Microsoft*, 233 F. Supp. 3d at 896.

"secrecy [was] no longer required to satisfy" the government's interest in protecting the integrity of its criminal investigations.[153]

Although the court's ruling at the pleadings stage did appear to look favorably on Microsoft's First Amendment claims, the merits of the case never had a chance to be assessed. In October 2017, less than two years after Microsoft first sued over the government's use of gag orders attached to search warrants under the SCA, the DOJ issued new guidelines limiting the role prosecutors should play in preventing intermediaries from telling users and the public about search warrants compelling disclosure of their communications and related information through gagging.[154] In response, Microsoft volunteered to drop its lawsuit.[155]

Below, I consider the motives driving Internet intermediaries like Microsoft to challenge the SCA's gag order provision in the first place, the merits of the would-be substantive lawsuit, and the effect of the DOJ guidelines on the speech and privacy rights of intermediaries, individuals, and the public at large.

1. Why Bother? Considering Internet Intermediaries' Motivations

For now, it is uncertain how effective the DOJ's guidelines will be in curbing the use and scope of gag orders issued on Internet intermediaries under the SCA. This means that for the time being, true targets of government surveillance and the public at large remain dependent on intermediaries to fight for their rights and to keep them informed on the progress. This is a precarious position to be in for those impacted parties unable to assert their own rights in the face of potential government overreach.[156]

Consider, for example, Facebook's recent challenge to a gag order prohibiting it from disclosing the existence of three search warrants targeting information from three Facebook user accounts.[157] While fighting the order

---

153 *Microsoft*, 233 F. Supp. 3d at 906-07.

154 *See generally* Rosenstein Memo, *supra* note 15.

155 *See* Ellen Nakashima, *Justice Department Moves to End Routine Gag Orders on Tech Firms*, WASH. POST (Oct. 24, 2017), https://www.washingtonpost.com/world/national-security/justice-department-moves-to-end-routine-gag-orders-on-tech-firms/2017/10/23/df8300bc-b848-11e7-9e58-e6288544af98_story.html?utm_term=.3138665ab3a4 [https://perma.cc/V276-43JV].

156 *See In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) ("Of course, the burden of the gag order probably falls more heavily upon the target of the surveillance rather than the service provider, whose business interests are arguably unaffected by non-disclosure.").

157 *See generally* Brief of Amici Curiae The American Civil Liberties Union, The American Civil Liberties Union of the District of Columbia, and Public Citizen, Inc. In Support of Appellant and Reversal, Facebook Inc. v. United States, Nos. 17-0388, 17-0389, 17-0390 (D.C. Cir. 2017), https://www.aclu.org/sites/default/files/field_document/in_re_facebook_brief_of_amici_aclu_aclu-dc_and_public_citizen.pdf [https://perma.cc/8RMU-FU4F].

in court, the social media company revealed what little information it legally could: that "the events underlying the government's investigation are generally known to the public"—which would seemingly undermine the need to gag the Internet intermediary in the first place.[158] Observers of the case pieced together the scraps of available information concerning the investigation in question and surmised that the warrants, along with the accompanying gag orders issued on Facebook, concerned felony charges stemming from "riots that erupted in D.C. amid President Donald Trump's inauguration."[159] Only after public outcry did federal prosecutors move to vacate the nondisclosure orders—the day before oral arguments were to begin.[160] The Electronic Frontier Foundation (EFF), a nonprofit legal advocacy organization focused on user privacy and free expression, criticized the government's case over the gag order, stating: "While we applaud the government's about-face, we question why they ever took such a ridiculous position in the first place."[161] In December 2017, the first six defendants from the inauguration day arrests—including a journalist who was apprehended while covering the protests and faced up to sixty-one years in prison—were found not guilty of all charges against them, including conspiracy to riot and destruction of property.[162]

In another apparent example of government overreach in the context of secret surveillance via third-party intermediaries, a 2012 New York criminal case over the alleged disorderly conduct of an Occupy Wall Street protestor led prosecutors to send an SCA-sanctioned subpoena[163] for all of the

158 Bryan Koenig, *Feds Drop Gag Order on Facebook Over Warrants*, LAW360 (Sept. 14, 2017), http://www.law360.com/articles/964060/feds-drop-gag-order-on-facebook-over-warrants [https://perma.cc/53RE-DB9L].

159 *Id*.

160 *Id*.

161 Andrew Crocker & Nate Cardozo, *VICTORY: DOJ Backs Down from Facebook Gag Orders in Not-So-Secret Investigation*, ELECTRONIC FRONTIER FOUND. (Sept. 13, 2017), https://www.eff.org/ deeplinks/2017/09/victory-doj-backs-down-facebook-gag-orders-not-so-secret-investigation [https://perma.cc/378D-ASEM].

162 *See* Jaclyn Peiser, *Journalist Charged with Rioting at Inauguration Day Protest Goes Free*, N.Y. TIMES (Dec. 21, 2017), https://www.nytimes.com/2017/12/21/business/media/journalist-inauguration-day-protest-not-guilty-rioting.html?_r=0 [https://perma.cc/FH5Z-9VCM]. It is unclear if the search warrants issued to Facebook in the fall of 2017 concerned these defendants in particular, but both the prosecution and defense made use of the livestream the journalist had shared on his Facebook feed at the time of the protests. *Id*.

163 The court ruled, however, that because one day's worth of the tweets sought by the prosecution were less than 180 days old, that information would have to be compelled by a *search warrant*, rather than a *subpoena*, pursuant to 18 U.S.C. § 2703. People v. Harris (*Harris II*), 949 N.Y.S.2d 590, 596 (Crim. Ct. 2012).

defendant's tweets and noncontent user data[164] over a three-month period—not to the protestor on trial, but rather to Twitter, a third-party intermediary.[165] Harris, the protester and tweeter, first tried to quash the subpoena himself, but the court held that he had no proprietary interest in the user information on his Twitter account and therefore lacked the necessary standing to intervene in what was viewed as a separate legal proceeding concerning Twitter.[166] It was then that Twitter further involved itself in what was otherwise a local misdemeanor case, filing its own motion to quash the subpoena, although its challenge was also mostly denied, on the much-criticized theory that Harris had "no reasonable expectation of privacy in a tweet sent around the world."[167] I wrote about the case as an undergraduate in the summer of 2012, when Paul Alan Levy, an attorney with Public Citizen who contributed to Harris's defense, told me that in criminal contexts like this one, "it takes a little more backbone" for intermediaries like Twitter to object to arguably overbroad government surveillance on behalf of its users.[168]

The Facebook and Twitter cases underscore individuals' and the public's heavy reliance on Internet intermediaries in the face of shrinking privacy rights and the specter of unchecked government overreach, given that "there may be no recourse for unconstitutional surveillance unless companies can speak about it."[169] But these interested yet effectively powerless parties should recognize that their interests are not necessarily aligned with those of the intermediaries raising objections on their behalf. For one thing: "To hear tech companies explain it, challenging these gag orders is in large part a matter of constitutional principle. . . . [But] compliance with such [gag] orders can create unease in many privacy-minded consumers and business clients."[170]

---

164 According to Andrew Crocker, this case shows that in certain circumstances, "the collection of location data can be highly revealing of political activity and, under certain circumstances, can even constitute speech under the First Amendment." Crocker, *supra* note 49, at 623.

165 People v. Harris (*Harris I*), 945 N.Y.S.2d 505, 506 (Crim. Ct. 2012).

166 *Id.* at 507-10.

167 *Harris II*, 949 N.Y.S.2d at 593. This holding "failed to acknowledge that Twitter can collect an accrual of public statements, unlike passersby who might witness an isolated incident," which paints a much bigger picture than a single public tweet. Amanda Simmons, *A Subpoena that Has Everyone A-Twitter*, REPORTERS COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-summer-2012/subpoena-has-everyone-twitt [https://perma.cc/8H7M-3LKG] (last visited Jan. 1, 2018).

168 Simmons, *supra* note 167.

169 Sumar, *supra* note 112, at 94 ("Companies likely lack standing to challenge the search itself, and the gag order prevents the only persons who could have standing—the targets of the search—from ever knowing about it." (footnote omitted)).

170 Rhys Dipshan, *Do Business, Regulatory Realities Trump Constitutional Principle in Gag Orders Fight*, LEGALTECHNEWS (May 9, 2017, 1:22 PM), https://www.law.com/legaltechnews/almID/1202785585774/do-business-regulatory-realities-trump-constitutional-principle-in-gag-orders-fight/ [https://perma.cc/7FEJ-JW39].

Consider, for example, the EFF's "Who Has Your Back" annual comparative report.[171] The study ranks large technology companies based on how hard they push back on government data requests, thereby pressuring these intermediaries to challenge SCA-sanctioned gag orders and other procedural tools used by law enforcement agencies to secretly surveil.[172]

Further, the motivation driving certain tech companies to push back on SCA-sanctioned gag orders appears to go beyond keeping commercial consumers in the United States satisfied. Looking beyond the impact that gag orders have even on their customers, U.S.-based Internet intermediaries might be challenging these orders on *American free speech* grounds albeit more so to comply with *foreign privacy* regulations, namely the European Union's demanding new General Data Protection Regulation (GDPR), which will become enforceable in May 2018.[173] Europe's reinvigoration of its privacy laws—and American online intermediaries' willingness to comply—was arguably spurred by Edward Snowden's revelations that these companies were complying with the NSA's shockingly invasive "PRISM" data collection surveillance program with virtually no pushback.[174] Today, rigorous privacy protection regimes like the GDPR, coupled with the uncertain scope of foreign jurisdictions' reach, have the effect of putting Internet intermediaries in a difficult position where compliance with one country's privacy law might violate that of another. One strategy evidently adopted by certain data "processor[s],"[175] as companies like Microsoft are called under the European privacy law scheme, involves making a public showing—perhaps through as-applied or facial challenges—that at least attempts to comply with the GDPR's new regulations.[176] This distinct motivation behind U.S. tech companies' strategy of raising legal challenges to the SCA's § 2705(b) gag order provision

171 Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, ELECTRONIC FRONTIER FOUND. (July 10, 2017), https://www.eff.org/who-has-your-back-2017 [https://perma.cc/RW5F-H6YB].

172 *Id.*; *see also* Dipshan, *supra* note 170.

173 *See id.* ("Section 2705 gag orders, for instance, may violate the EU-U.S. Privacy Shield—the approved legal framework for transferring data between the EU and the U.S.").

174 *See, e.g.*, Klint Finley, *Thank (or Blame) Snowden for Europe's Big Privacy Ruling*, WIRED (Oct. 6, 2015, 9:06 PM), https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/ [https://perma.cc/3R6K-7WEH].

175 Commission Regulation 2016/679 art. 4(8), 2016 O.J. (L 119) 33 (EU).

176 The GDPR is considered much more rigorous than the SCA and other privacy law statutes in that the required compliance is much more burdensome for Internet intermediaries that handle individuals' online data. Perhaps for that reason, Microsoft, which has led in challenging the jurisdictional bounds of the SCA to attempt compliance with GDPR, recently sued the U.S. federal government over a search warrant issued under the U.S. statute compelling it to disclose email stored overseas, in Ireland. The U.S. Supreme Court heard oral arguments but dropped the case in April 2018, after Congress amended the SCA via the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which states that emails and other data stored on servers located abroad can be reached by U.S. search warrants. United States v. Microsoft Corp., 138 S. Ct. 1186, 1187-88 (2018).

highlights the strange interplay between the right to privacy and the freedom of speech, and its effects on individual communications in the digital age.

III. ASSESSING THE MERITS: THE CASE AGAINST GAG ORDERS

Although the DOJ's new policy for prosecutors seeking gag orders that barred intermediaries from speaking about the search warrants issued in domestic criminal investigations apparently obviated the need for Microsoft to continue pursuing its lawsuit,[177] it is nonetheless worthwhile to consider the merits of the arguments against the general practice. After all, the EFF says it would "go so far as to say that challenging gag orders imposed alongside government data requests is one of the key digital civil liberties issues of our time."[178] To urge popular Internet intermediaries to continue raising such objections, the EFF even rates intermediaries' willingness and effectiveness in fighting against instances of government surveillance and accompanying gag orders in terms of the companies' corporate policies and legal challenges.[179] Ultimately, as illustrated in third-party intermediaries' as-applied and facial challenges to gag orders attached to search warrants under the SCA, there is a strong argument to be made that these orders run the serious risk of directly violating their recipients' First Amendment rights as content-based prior restraints, which generally face a heavy presumption against their constitutionality. Here, a useful comparison can be made to how courts treat gag orders attached to National Security Letters (NSLs), which are low-threshold administrative subpoenas authorized in part by the SCA and issued to Internet intermediaries for the purpose of furthering national security investigations (as opposed to traditional search warrants and other orders permitting surveillance that pertains to domestic criminal law). One court described a gag order attached to an NSL as "not a typical prior restraint or a typical content-based restriction warranting the most rigorous First Amendment scrutiny."[180] Furthermore, in terms of the merits of lawsuits challenging gag orders on constitutional grounds, one should consider if SCA-sanctioned gag orders indirectly infringe on the First Amendment rights of

177 Perhaps this is because the DOJ's response satisfied Microsoft's own motives for bringing its suit in the first place, even if it did not necessarily result in the DOJ admitting the alleged violations of the First Amendment rights of Microsoft, its individual users, and the general public.

178 Andrew Crocker, *A Step Forward in Microsoft's Legal Battle for Transparency About Government Data Requests*, ELECTRONIC FRONTIER FOUND. (Feb. 17, 2017), https://www.eff.org/deeplinks/2017/02/step-forward-microsofts-legal-battle-transparency-about-government-data-requests [https://perma.cc/TB7C-CPCP].

179 Reitman, *supra* note 171, at 10 (explaining that the EFF assigns technology companies a positive rating on their willingness to resist gag orders only if they "publicly commit to invoking the available statutory procedures to have a judge review every indefinite NSL gag order [they] receive[]").

180 Doe v. Mukasey (*Doe III*), 549 F.3d 861, 877 (2d Cir. 2008).

constituents—i.e., the true targets of the surveillance and the public at large. This would suggest that where individuals' privacy rights are seemingly under siege, protections provided by the First Amendment should accordingly be expanded and strengthened.

A. *A Direct Infringement on Intermediaries' First Amendment Rights*

The specific as-applied challenges to individual gag orders attached to SCA-sanctioned warrants, as well as Microsoft's facial challenge to the statute, make an overall convincing case for why these orders violate intermediaries' First Amendment rights. As a general matter, it is understood that third-party institutions have a First Amendment right to circulate communications that flow through their intermediation. Recall, for example, *Bartnicki v. Vopper*, where the Supreme Court held that although a secret recording of a conversation between labor officials about a teacher strike might have violated Title I of ECPA (the Wiretap Act), the radio station that aired the tape was protected by the First Amendment.[181] More specifically, the Court reasoned that "[i]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category . . . ."[182] Furthermore, the type of speech that gagged intermediaries are prevented from discussing under the SCA—i.e., information about the scope and effect of government surveillance—had procedural protections in the Alien and Sedition Acts of 1798, which essentially criminalized the act of criticizing the government.[183] It's exactly the kind of speech James Madison would want available, and so too would Justice Holmes in his "marketplace of ideas," so that individuals can assert their due process and other constitutional rights and the public can enjoy healthy debate about its government's approach to privacy.[184] Today, too, the

---

181 532 U.S. 514, 516 (2001).

182 *Id.* at 527 (alteration in original) (quoting Bartnicki v. Vopper, 200 F.3d 109, 120 (3d Cir. 1999)).

183 *See* Sedition Act § 3, 2 Stat. 596, 597 (1798) (providing for a jury trial process for those prosecuted for libel against the United States).

184 As James Madison explained:

> Let it be recollected, lastly, that the right of electing the members of the Government constitutes more particularly the essence of a free and responsible government. The value and efficacy of this right depends on the knowledge of the comparative merits and demerits of the candidates for public trust, and on the equal freedom, consequently, of examining and discussing these merits and demerits of the candidates respectively . . . .

James Madison, *Report of 1799*, *in* THE VIRGINIA REPORT OF 1799–1800, at 227 (Richmond, J.W. Randolph 1850); *see also* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . .").

Supreme Court has recognized that there must be "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[185]

Gag orders are often challenged, both in the context of the SCA and in other circumstances, as content-based prior restraints. Content-based restrictions, the first tack intermediaries have taken to challenge gag orders prohibiting them from disclosing the existence of search warrants to the true targets or the public, are not on their face unconstitutional, but are carefully scrutinized under the First Amendment. In *Turner Broadcasting System v. FCC*, the Supreme Court held that content-based regulations, or government actions that restrict speech because of the subject matter or viewpoint that it conveys, are "presumptively invalid" and therefore subject to strict scrutiny.[186] According to Erwin Chemerinsky, "Court[-]issued gag orders are content-based because their application depends entirely on the topic of the speech."[187] Here, SCA-sanctioned gag orders are seemingly content-based because they prohibit disclosure of an entire subject matter of speech—i.e., the issuance and scope a search warrant in connection with a domestic criminal investigation. The Court has recognized a narrow exception, however, for government regulations of speech that are seemingly content-based, but that can be "*justified* without reference to the content of the regulated speech."[188] With respect to gag orders, it is difficult to see how the government could possibly justify their use without reference to the content such orders are designed to silence.[189] Moreover, current First Amendment

185 N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964); *see also* Landmark Commons Inc. v. Virginia, 435 U.S. 829, 838 (1978) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of government affairs." (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966)).

186 512 U.S. 622, 640-41 (1994); *see also id.* ("[Content-based] [l]aws of this sort pose the inherent risk that the Government seeks not to advance a legitimate regulatory goal, but to suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion.") *But see* Ward v. Rock Against Racism, 491 U.S. 781, 798 (1989) ("[A] regulation of the time, place, or manner of protected speech must be narrowly tailored to serve the government's legitimate, *content-neutral* interest but . . . need not be the least restrictive or least intrusive means of doing so." (emphasis added)).

187 Erwin Chemerinsky, *Lawyers Have Free Speech Rights, Too: Why Gag Orders on Trial Participants Are Almost Always Unconstitutional*, 17 LOY. L.A. ENT. L.J. 311, 320-21 (1997) (citing Simon & Schuster v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105 (1991), which held that a state law that prevented criminals from selling their stories to the press for their own profit was unconstitutional as a content-based restriction).

188 City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 48 (1986).

189 *Accord* Boos v. Berry, 485 U.S. 312, 329 (1988) (holding that a government regulation barring certain political speech near foreign embassies could not be justified on non-speech-related grounds and was therefore an unconstitutional content-based restriction).

doctrine somewhat controversially holds that strict scrutiny should *always* apply to laws that are content-based on their face, meaning that any plausible justifications that the government might have that are unrelated to the speech they restrict will not even be considered by the court.[190] Assuming, then, that gag orders issued in accordance with the SCA are content-based restrictions in that they "appl[y] to particular speech because of the topic discussed or the idea or message expressed,"[191] a court would then consider whether, on their face (as argued in the case of *Microsoft*) or as applied (as contemplated by the federal magistrate court split), they are narrowly tailored to further a compelling interest. Here, the government arguably has a legitimate interest in protecting the integrity of its criminal investigations, but its apparently overbroad means of furthering this interest—gag orders on third parties barring a particular kind of speech (often permanent in practice)—indicates that the SCA's § 2705(b) gag order provision would likely fail the content-based restrictions' strict scrutiny test, in violation of the First Amendment.

Gag orders, furthermore, are considered a classic form of prior restraint, a kind of "administrative and judicial order[] forbidding certain communications when issued in advance of the time that such communications are to occur."[192] This constitutes the second prong of intermediaries' First Amendment claims against SCA-sanctioned notices of preclusion. Prior restraints "are the most serious and the least tolerable infringement on First Amendment rights" and like content-based restrictions on speech, they face a heavy presumption against their constitutionality.[193] Here, the rationale behind the First Amendment's generally tough stance on prior restraints is in part based on the fact that they silence communication *before* it takes place, thereby preventing certain speech from ever occurring.[194] Moreover, a prior restraint cannot be challenged by disobeying the bar on speech—i.e., by merely speaking about the restraint—even when the speaker believes it was issued improperly or unconstitutionally.[195] In *Nebraska Press Ass'n v. Stuart*, the Supreme Court held

---

190 Reed v. Town of Gilbert, 576 U.S. 155, 165 (2015). As Justice Thomas's opinion for the majority explained: "A law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of 'animus toward the ideas contained' in the regulated speech." *Id.* Note that Justice Thomas's opinion holds that strict scrutiny should also apply to content-*neutral* regulations of speech, like the ordinance at issue in *Ward v. Rock*.

191 *Id.* at 163.

192 Alexander v. United States, 509 U.S. 544, 550 (1993) (emphasis removed) (quoting MELVILLE NIMMER, NIMMER ON FREEDOM OF SPEECH § 4.03 (1984)). Gag orders, after all, are imposed *before* their recipients have a chance to speak about the search warrants they accompany.

193 Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

194 *See* Near v. Minnesota, 283 U.S. 697, 720 (1931) ("*Subsequent* punishment for such abuses as may exist is the appropriate remedy . . . ." (emphasis added)).

195 *See* Walker v. City of Birmingham, 388 U.S. 307, 321 (1967) (holding that Dr. Martin Luther King, Jr. and some of his contemporaries could not challenge a court order preventing them from protesting without a permit simply because they had violated the order).

that a gag order issued on the press to protect a defendant's right to a fair trial would be permissible only if it could be shown that 1) extensive publicity would jeopardize the jury's impartiality; 2) there were no effective alternative measures; and 3) the prior restraint would be effective in protecting the trial.[196] This demanding test arguably goes beyond even strict scrutiny, "virtually preclud[ing] gag orders on the press as a way of preventing prejudicial pretrial publicity."[197] If intermediary-recipients of SCA-sanctioned search warrants with attached gag orders were likened to the press, and the domestic criminal investigations at issue analogized to a fair trial under the Sixth Amendment, one could argue that § 2705(b) would clearly fail the constitutionality threshold test in *Nebraska Press*.

Unfortunately for the intermediaries like Microsoft raising these claims (and the customers who are relying on them to do so), not all cases dealing with prior restraints in other relevant contexts are as cut and dry. Consider the case of *Near v. Minnesota*, where the Court ruled unconstitutional a state law barring, ex ante, the publication of "malicious, scandalous, and defamatory" newspaper articles—here applied to a newspaper's anti-Semitic pieces—but left open the possibility, in dictum, that such a prior restraint might be found valid in rare circumstances, such as the dissemination of Army troops' location points.[198] The Court addressed this very issue in the seminal case, *New York Times v. United States* (also known as the "Pentagon Papers" case), which struck down a court order barring publication of the top-secret government files on the Vietnam War, but offered little explanation as to why the order was found to violate the First Amendment.[199] Concurring opinions by Justice Black and Justice Douglas, respectively, held that prior restraints are effectively always unconstitutional.[200] In a separate concurrence, Justice Brennan took a similar approach but, echoing *Near*, found an exception that "may arise only when the

196 *Neb. Press*, 427 U.S. at 562-63, 565. Note that while *Nebraska Press* only considered gag orders issued on the press, Chemerinsky argues that the same test should apply to court-ordered gags on lawyers and trial participants. *See* Chemerinsky, *supra* note 187, at 314. Third-party intermediary-recipients of warrants targeting individual communications could arguably fit this expanded interpretation of *Near* as well.

197 Chemerinsky, *supra* note 187, at 312.

198 *Near*, 283 U.S. at 701; *see also id.* at 716 ("No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.").

199 403 U.S. 713, 714 (1971) (per curiam).

200 *See id.* at 715 (Black, J., concurring) ("[E]very moment's continuance of the injunctions against these newspapers amounts to a flagrant, indefensible, and continuing violation of the First Amendment."); *id.* at 723-74 (Douglas, J., concurring) ("The dominant purpose of the First Amendment was to prohibit the widespread practice of governmental suppression of embarrassing information. . . . The present case[] will, I think, go down in history as the most dramatic illustration of that principle.")

Nation 'is at war.'"[201] Under these interpretations of the First Amendment's treatment of prior restraints, the gag orders permitted under the SCA in connection with government surveillance related to domestic criminal investigations would likely be struck down as an infringement on the First Amendment because the government's justification for such orders—that they protect the integrity of criminal investigations—are seemingly insufficient. Justice White and Justice Marshall, meanwhile, authored separate concurring opinions taking issue with the fact that the court order in *New York Times* was not based on any express statutory authority.[202] The gag orders at issue here, on the other hand, are indeed authorized by the SCA's § 2705(b), and so would apparently be deemed constitutional by Justices White and Marshall, respectively. The last relevant take from *New York Times*, Justice Blackmun's dissent, expressed concern:

> I hope that damage has not already been done. If, however, damage has been done, and if, with the Court's action today, these newspapers proceed to publish the critical documents and there results therefrom "the death of soldiers, the destruction of alliances, the greatly increased difficulty of negotiation with our enemies, the inability of our diplomats to negotiate," to which list I might add the factors of prolongation of the war and of further delay in the freeing of United States prisoners, then the Nation's people will know where the responsibility for these sad consequences rests.[203]

Here, the constitutionality of the SCA's gag order provision would ostensibly turn on how grave a particular instance of government surveillance seemed compared with "the death of soldiers [and] the destruction of alliances."[204] However, given the overall outcome of *New York Times*, and the principle it has come to symbolize in terms of First Amendment doctrine and, more broadly, American history, it seems likely that in its wake, the Court today would treat gag orders attached to search warrants issued to third-party intermediaries under the SCA—particularly those that seemingly silence the tech company-recipients from speaking about the government surveillance in question indefinitely—like "any system of prior restraints of expression . . . [with] a heavy presumption against its constitutional validity."[205]

---

201 *Id.* at 726 (Brennan, J., concurring) (quoting Schenck v. United States, 249 U.S. 47, 52 (1919)).

202 *Id.* at 731 (White, J., concurring); *id.* at 747 (Marshall, J., concurring).

203 *Id.* at 763 (Blackmun, J., dissenting).

204 *Id.*

205 *Id.* at 714 (per curiam) (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963); Near v. Minnesota, 283 U.S. 697 (1931)).

1. A Point of Comparison: Litigating National Security Letters

The long, still-developing legal framework governing secret NSLs serves as an interesting point of comparison to gag orders attached to traditional search warrants under the SCA. Courts' treatment of gag orders in the context of NSLs can provide useful guidance for assessing the constitutionality of similar orders issued in connection with traditional search warrants under 18 U.S.C. § 2705(b). An NSL is a kind of administrative subpoena authorized, like search warrants issued to Internet intermediaries, in part by the SCA, or Title II or ECPA, that allows the FBI to compel electronic communications service providers to disclose subscriber information and other noncontent user data[206] without requiring court approval.[207] Here, these orders are distinct from SCA-sanctioned search warrants, which the government must obtain from a court of law for the purpose of surveilling of the actual contents of communication held by third-party intermediaries.[208] Instead, to obtain an NSL, FBI officials must merely certify to the intermediary-recipient (versus an overseeing court) that the information sought is related to "an authorized investigation to protect against international terrorism or clandestine intelligence activities."[209] This is of course an extremely low-threshold procedural protection. Furthermore, like with SCA-sanctioned warrants, here, the government can attach gag orders to these NSLs, barring the intermediary-recipients from disclosing their existence to the targets of the surveillance or the public at large.[210]

The original iteration of the NSL enabling statute, first enacted in 1986 with the rest of ECPA, went much further, generally imposing a blanket gag

---

206 This includes the customer's name, address, and length of service. The FBI is typically seeking information related to an individual user's telephone or Internet activity.

207 18 U.S.C. § 2709 (2012) (authorizing counterintelligence access to telephone toll and transactional records).

208 *Id.* § 2705(b).

209 *Id.* § 2709(b)(1)–(2).

210 Anecdotal evidence suggests that the government's motives for pursuing gag orders in the context of traditional warrants are different than its rationale for seeking such orders in connection with NSLs. With search warrants, the government seems to want to keep its investigation secret from the true target(s) of the surveillance. But in the case of NSLs sent to intermediaries, the FBI generally attaches gag orders in order to cloak from the public at large the extent of its surveillance and data collection programs. This FBI practice is more problematic from the perspective of First Amendment doctrine. *See, e.g.*, Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J.F. 158, 159 (2014) (describing tech companies' "self-help" remedies for circumventing NSL gag orders in the name of transparency, including issuing "warrant canaries" or regularly published reports stating that an intermediary has *not* received an NSL; when they do receive such an order with a gag attached, they "kill" the canary by removing the statement).

order whenever intermediaries were served with such an order.[211] In 2004, an anonymous[212] recipient of an NSL seeking information associated with a Connecticut library's computers challenged this broad gag order under the First Amendment.[213] The district court held that gag orders under the original NSL law were unconstitutional as content-based restrictions and prior restraints, neither of which were narrowly tailored.[214] The government appealed, but in the interim Congress amended the statute. First, the amendment required nondisclosure on the part of intermediary-recipients only when the requesting FBI official certified that without a gag, there was a belief that certain "enumerated harms" could occur—i.e., "a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."[215] These harms are similar to § 2705(b)'s list of possible reasons justifying the use of a gag order with a search warrant (including its catchall, "or . . . otherwise seriously jeopardizing an investigation or unduly delaying a trial").[216] In a more dramatic change, the NSL amendment also included a provision for judicial review, whereby a recipient of an NSL could petition a court to modify or rescind the order and/or accompanying gag order.[217] A request to modify or set aside the gag order could be granted if the reviewing court found "that there is no reason to believe that disclosure may endanger the national security of the United States" or cause other certain harms very similar to the list from the first amended provision, § 2709(c).[218] However, under this amendment, certification by a federal prosecutor or other senior government official that disclosure could endanger national security would be treated as "conclusive" unless it was determined by a court to have been made in "bad faith."[219] Section 2705(b), on the other hand, gives courts nearly all the authority in determining whether a gag order

211 *See* 18 U.S.C. § 2709(c) (2000), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 115, 120 Stat. 192, 212 (2006) ("No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.").

212 The plaintiff was anonymous so as to comply with the gag order he was challenging. As noted above, prior restraints are typically treated with exacting scrutiny because they cannot be challenged by simply disobeying the bar on speech. *See supra* note 195 and accompanying text.

213 Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 511 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales (*Doe II*), 449 F.3d 415 (2d Cir. 2006).

214 *Id.* at 516, 527.

215 USA PATRIOT Improvement and Reauthorization Act of 2005, § 115 (codified at 18 § 2709(c) (2012)).

216 *Id.* (codified at 18 U.S.C. § 2705(b)).

217 *Id.* (codified at 18 U.S.C. § 3511(a)).

218 *Id.* (codified at 18 U.S.C. § 3511(b)(2)).

219 *Id.* (codified at 18 U.S.C. § 3511(b)(2))

attached to a search warrant should be imposed, modified or rescinded in response to an objection from the recipient. Despite these changes to certain NSL statute provisions, which were clearly designed to improve the government's defense to constitutional challenges, the appellate court found that the gag order provisions still did not comport with the First Amendment because they remained content-based prior restraints.[220] More specifically, the court held that the new NSL gag order provision was unconstitutional because it improperly put the burden of initiating judicial review on the intermediary-recipient; provided for a judicial review procedure that was not as rigorous as the First Amendment required and upset the separation of powers; and permitted the FBI to require nondisclosure under circumstances that were not narrowly tailored.[221]

On appeal, a Second Circuit court panel seemed to underplay the threat that NSL gag orders under the 2005 amendment posed to intermediary-recipients' First Amendment rights in several respects. First, the court in *John Doe Inc. v. Mukasey* questioned whether gag orders of this sort should be classified as certain potential types of infringements of the First Amendment that elsewhere had traditionally faced a heavy presumption against their constitutionality:

> Although the nondisclosure requirement is in some sense a prior restraint, . . . it is not a typical example of [a prior restraint] for it is not a restraint imposed on those who customarily wish to exercise rights of free expression, such as speakers in public fora, distributors of literature, or exhibitors of movies. . . . And although the nondisclosure requirement is triggered by the content of a category of information, that category . . . is far more limited than the broad categories of information that have been at issue with respect to typical content-based restrictions.[222]

Such an analysis—that a gag order attached to NSL "is not a typical prior restraint or a typical content-based restriction warranting the most rigorous First Amendment scrutiny"[223]—could arguably apply to similar nondisclosure orders accompanying search warrants under the SCA. This would have the effect of subjecting SCA-sanctioned gag orders to a more permissive standard of judicial scrutiny than that contemplated in *Turner* (calling for strict scrutiny in cases of prior restraint) and *Nebraska Press* (arguably establishing an exacting standard beyond strict scrutiny for instances of prior restraint).[224] Note, however, that the district court in *Microsoft* found that gag orders attached to

220 Doe v. Gonzales (*Doe II*), 449 F. 3d 415, 386 (2d Cir. 2006).
221 *Id*.
222 John Doe Inc. v. Mukasey (*Doe III*), 549 F.3d 861, 876 (2d Cir. 2008) (emphasis added).
223 *Id*. at 877.
224 *See supra* Section III.A.

search warrants under the SCA are *not* the "atypical" content-based prior restraints that effectively silence NSL recipients.[225]

Further insulating the NSL gag order provision from scrutiny under the First Amendment, the *Doe III* court engaged in what would most generously be described as a liberal reinterpretation of certain problematic provisions—if not an effective rewriting of the statute—"thereby at least narrowing, though not eliminating, the First Amendment issues."[226] Here, the court noted that under the language of § 2709(c) that enabled FBI agents to issue gag orders with an NSL if there was a belief that certain "enumerated harms" would otherwise ensue, that issuance was not tied to the broader requirement that the NSL itself be pursuant to an investigation related to national security.[227] However, per the government-defendant's urging, the court circumvented this problem "by construing the scope of the enumerated harms in light of the purposes for which an NSL is issued."[228] This reading requires that the government's justifications for pursuing a gag order also be in connection to a national security investigation, much like how the reasons for issuing a NSL in the first place must be under 18 U.S.C. § 2709(a). Similarly, the panel was persuaded to broadly interpret the provision—which allowed a reviewing court to reconsider an NSL gag order only "if it finds that there is *no reason* to believe" that disclosure would lead to enumerated harms—to mean that the court could consider whether the government's justification for a gag constituted a "*good reason*."[229]

In considering the *Doe III* court's approach to NSL gag orders in relation to the SCA's gag order provision regarding traditional search warrants and its First Amendment implications, Al-Amyn Sumar suggests that a court can similarly read 18 U.S.C. § 2705(b) liberally to avoid problems under the First

---

225 The *Microsoft* Court was

> not persuaded to apply the same logic here. First, the Second Circuit [in *Doe III*] based its conclusion in large part on the national security context in which Section 2709(c) operated. . . . Second, the statutory provision at issue in [*Doe III*] imposed temporal limits on the nondisclosure orders. . . . Such temporal limitations are not required under Section 2705(b), and according to Microsoft's amended complaint, are frequently absent from orders issued pursuant to that statute.

Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 906 n.7 (W.D. Wash. 2017).

226 *Doe III*, 549 F.3d at 875.

227 *Id.*

228 *Id.*

229 *Id.* (emphasis added). Here, the panel held that courts can require a government official seeking a gag order in connection with an NSL to show that there would otherwise be a risk of harm that is "more than a conceivable possibility." *Id.*

Amendment.[230] For example, Sumar argues that the provision allowing courts to attach gag orders to search warrants "for such period as the court deems appropriate"—i.e., seemingly indefinitely—can instead be interpreted to have a "reasonable temporal limit," as the federal magistrate court did in *[Redacted]@hotmail.com*.[231] Similarly, where § 2705(b) requires that the government have "a reason to believe" that certain kinds of potential harm might occur without a gag order accompanying a warrant, a court can find that Congress meant that prosecutors must have "a *good* reason."[232] This suggestion mirrors the approach taken in *Doe III* and has the effect of implying that a nonindefinite gag order justified by a "good reason" is inherently narrowly tailored,[233] and therefore survives the strict judicial scrutiny that would likely apply to SCA-sanctioned gag orders attached to search warrants, given that the court in *Microsoft* rejected *Doe III*'s finding that nondisclosure orders related to NSLs are "atypical" content-based restrictions.

In *Doe III*, however, the circuit court panel could not agree on what standard of judicial scrutiny to use to review NSL gag orders.[234] Nonetheless, the court ultimately held that these orders—despite not being "typical" constitutional infringements—violate the First Amendment under either traditional strict scrutiny or a less rigorous standard of judicial review.[235] This is a remarkable ruling, given that the court went to great lengths to interpret the NSL gag order provisions in a liberal manner that better comported with the First Amendment. Here, the court held that there is "no governmental interest . . . more compelling than the security of the Nation"[236] but regardless, the statute could not be upheld given the lack of government-

230 *See* Sumar, *supra* note 112, at 99 ("*Doe* took that canon of construction close to its limit—perhaps too close. But it is nonetheless useful to consider how the statute might be read as constitutionally compliant."). This solution is arguably what the DOJ's new guidelines stemming from *Microsoft* attempt to achieve, but they of course are not binding on the courts that have the discretion to issue gag orders, whereas with NSLs, it is FBI agents that have the power to directly order nondisclosure. *See* Conclusion, *infra*.

231 Sumar, *supra* note 112, at 99-100; *see also In re* Search Warrant For: [Redacted]@hotmail.com (*[Redacted]@hotmail.com*), 74 F. Supp. 3d 1184, 1186 (N.D. Cal. 2014) ("Section 2705(b) clearly requires the court to define some end."). *Contra In re* Search Warrant for [Redacted].com (*[Redacted].com*), 248 F. Supp. 3d 970, 977 (C.D. Cal. 2017) ("Section 2705(b) is concerned with the portion of time characterized by the adverse result or results that will occur if the government's warrant or other process is disclosed. . . . [T]hat portion of time may be 'indefinite.'"); United States v. Search Warrant, No. 16-4116, 1027 U.S. Dist. LEXIS 148393, at *6 (D.N.J. Aug. 10, 2017) ("The plain language of § 2705(b) makes clear that it does not require a fixed period.").

232 Sumar, *supra* note 112, at 99-100.

233 *Id.* ("[I]f a court has a *good* reason to believe some enumerated harm would follow from disclosure, that suggests proper grounding for a gag order.").

234 *Doe III*, 549 F.3d at 878.

235 *Id.*

236 *Id.* (internal quotation marks omitted).

initiated judicial review under § 3511.[237] The court's main point of contention with § 3511, as amended in 2005, is that it gave FBI officials all the discretion in issuing gag orders with NSLs, unless an intermediary-recipient like the unnamed plaintiff in *Doe III* decided to take on the burden of petitioning the court for judicial review. Here, the court was arguably more troubled by the balance-of-powers issues than any specific First Amendment violations that the NSL gag orders raised.

Doe III did not end the saga of gag orders accompanying NSLs. Two tech companies, CREDO Mobile and Cloudfare, next initiated challenges to NSL gag orders under the 2006 version of the authorizing statutes.[238] As the case made its way through the courts, the statutory provisions governing NSLs and their nondisclosure orders were amended even further by the 2015 USA FREEDOM Act.[239] In one key change to the law, the Attorney General was tasked with periodically reviewing and terminating any nondisclosure requirements issued in connection with an NSL.[240] In 2015, the DOJ accordingly set up "Termination Procedures," which require any nondisclosure order to terminate when the underlying investigation is closed or "on the three-year anniversary of the initiation" of the investigation, unless the FBI determines that the gag is still warranted.[241] The second major component of the 2015 amendments allowed NSL recipients, even when gagged by a nondisclosure order, to report "aggregate data regarding the number of NSLs (in specific ranges or 'bands') that [they have] received."[242] The lowest "band" that can be reported (most likely for the purpose of transparency reports shared with the public and advocacy groups like the EFF) is confirmation that an intermediary has received "0 to 99" gag orders attached to NSLs.[243] In *National Security Letter v. Sessions*, the Ninth Circuit decided to use the occasion of CREDO and Cloudfare's lawsuit to assess the constitutionality of the amended NSL laws on their face.[244]

In July 2017, the *Sessions* court held that as amended, the statutes authorizing NSL gag orders still constituted a content-based restriction—but that here, the relevant provisions survived the strict scrutiny standard of review articulated in *Reed* and were therefore constitutional under the First

237 *Id.* at 881.

238 Nat'l Sec. Letter v. Sessions, 863 F.3d 1110, 1119-20 (9th Cir. 2017).

239 *Id.*

240 12 U.S.C. § 3414 (2012).

241 FED. BUREAU OF INVESTIGATION, TERMINATION PROCEDURES FOR NATIONAL SECURITY LETTER NONDISCLOSURE REQUIREMENT 2 (2015), https://www.fbi.gov/file-repository/nsl-ndp-procedures.pdf [https://perma.cc/RTR8-XFNT].

242 *Sessions*, 863 F.3d at 1119-20.

243 *Id.*

244 *Id.*

Amendment.[245] The challenging intermediaries had argued that gag orders attached to NSLs were still overbroad and overinclusive. For example, they claimed that the new "Termination Procedures" do not resolve the duration issue entirely: "where the government determines that the nondisclosure requirement remains necessary at the close of an investigation, the Termination Procedures do not require any subsequent review."[246] Similarly, they took issue with the provision allowing "aggregate reporting" in bands, arguing that it was not the least restrictive alternative because "recipients who receive fewer than 500 NSLs are forced to make the false assertion that they might have received no NSLs."[247] The court conceded these shortcomings in the statute's revised "tailoring," but was not persuaded simply because national security is an uncontested compelling interest since "[t]his granular focus cannot be reconciled with the Supreme Court's direction that narrow tailoring is not perfect tailoring."[248]

In terms of the prior restraint prong of the tech companies' First Amendment challenge, the *Sessions* court, like the Second Circuit panel in *Doe III*, was unsure what standard of review should apply, since NSL gag orders are "'not a typical example' of a regulation for which procedural safeguards are required."[249] But in a departure from *Doe III*, the Ninth Circuit similarly held that regardless of the applicable standard of judicial review, the 2015 version of the NSL law provides the necessary procedural safeguards to justify any prior restraint it causes.[250] This holding would potentially stymie intermediaries' challenges to SCA § 2705(b) gag orders attached to search warrants, since there are arguably more "procedural safeguards" grounded in the fact that courts—rather than senior FBI agents or other executive branch officials—determine whether nondisclosure should apply. Ultimately, *Sessions* managed to apply the broad, liberal reading set out in *Doe III* to the 2015 amended NSL law in order to find its provisions related to gag orders constitutional. And yet in the context of secret NSLs—and, in comparison, SCA-sanctioned search warrants with gag orders—concerns over privacy and speech rights still abound.

---

245 *Id.* at 1123.

246 *Id.* at 1126.

247 *Id.* at 1125. Note that the intermediaries were most critical of this aggregate reporting rule that restricted the "bands" they could disclose, perhaps because of their heightened interest in public transparency as it relates to their receipt of NSLs in particular. *See supra* subsection II.B.i.

248 *Sessions*, 863 F.3d at 1125.

249 *Id.* at 1127 (quoting John Doe Inc. v. Mukasey (*Doe III*), 549 F.3d 861, 876 (2d Cir. 2008)).

250 *Id.* at 1129.

B. *An Indirect Infringement on Other Stakeholders' First Amendment Rights*

Likely due to the standing issues they would face, Microsoft and other intermediaries challenging gag orders attached to search warrants issued under the SCA have not successfully raised First Amendment claims on behalf of other interested parties—namely, the true targets of the surveillance in question and the public at large.[251] But an interesting thought exercise considers whether these other stakeholders would have their own indirect First Amendment claims against nondisclosure orders and the surveillance that the orders hide from parties other than the recipient of a search warrant. As a general matter, Justice Brennan's concurrence in *Lamont* suggests that there is a constitutional "right to receive" information,[252] a right which appears to be violated when intermediaries are banned from disclosing the contents of a search warrant, or even its mere existence. Furthermore, other stakeholders might have a similar free speech claim to that of the intermediaries: gag orders issued under the SCA impermissibly interfere with the long-recognized right to discuss and criticize government affairs.[253] After all, SCA-sanctioned gag orders impede society from enjoying healthy debate about the appropriate balance between privacy and liberty because if the polity does not know about the surveillance being conducted via third-party intermediaries, it is impossible for the public to contemplate, question, or criticize the practice. According to First Amendment litigator Alex Abdo, the freedom to dissent, an important component of First

---

251 Note, however, that the court in *Microsoft* did expressly bar the company from raising Fourth Amendment claims on behalf of its customers—despite noting that this holding would effectively bar the affected individuals from ever vindicating their privacy rights:

> As Microsoft alleges, the indefinite nondisclosure orders allowed under Section 2705(b) mean that some customers may never know that the government has obtained information in which those customers have a reasonable expectation of privacy. . . . For this reason, some of Microsoft's customers will be practically unable to vindicate their own Fourth Amendment rights.

Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017).

252 Justice Brennan stated:

> It is true that the First Amendment contains no specific guarantee of access to publications. However, the protection of the Bill of Rights goes beyond the specific guarantees to protect from congressional abridgment those equally fundamental personal rights necessary to make the express guarantees fully meaningful. I think the right to receive publications is such a fundamental right. The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.

Lamont v. Postmaster Gen., 381 U.S. 301, 308 (1965) (Brennan, J., concurring) (internal citations omitted).

253 *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964) (holding that there is "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials").

Amendment doctrine, "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."[254] Furthermore, "[a]s the government's surveillance capabilities grow, the threat to dissent reaches earlier into its lifecycle," to the point where individual speakers, vaguely aware that the government is secretly watching via third-party intermediaries, change their behavior and ultimately self-censor.[255] It can be inferred, then, that any free speech claims by stakeholders other than the intermediaries directly challenging SCA gag orders would turn on a court's treatment of any so-called "chilling effect" caused by the § 2705(b) gag order provision.

Schauer describes this chilling effect as "the potential deterrent effect of a vague, or more commonly, an overbroad statute, [which] was [once] seen as reason enough to bend traditional rules of standing": "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."[256]

Unfortunately, the Supreme Court's approach towards this doctrine has not taken a very unified approach over the years. On the one hand, in cases such as *NAACP v. Alabama ex rel. Patterson*[257] and *Shelton v. Tucke*r,[258] the Court appeared to evaluate constitutional challenges raised by targets of government surveillance purely on the basis of the First Amendment and the related chilling effect. Even certain cases that appear on their face to grapple with the scope of government surveillance under the Fourth Amendment have been decided on, or at least heavily influenced by, the right to associate

254 Abdo, *supra* note 3, at 448.

255 *Id*.

256 Schauer, *supra* note 21, at 685, 688.

257 The *NAACP* Court reasoned:

> [C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.

357 U.S. 449, 462 (1958). Thus, the Court held that a state subpoena compelling disclosure of the organization's membership lists violated the Fourteenth Amendment (via the First Amendment). *Id.*

258 *Shelton* held that a state statute requiring teachers to list every organization to which they belonged or regularly contributed violated the First Amendment: "to 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." 364 U.S. 479, 485-86 (1960).

under the First Amendment.[259] But elsewhere, the Court has cast doubt on the efficacy of the chilling effect argument as a First Amendment claim. In *Laird v. Tatum*, the Court held that any chilling effect caused by the U.S. Army's surveillance of civilian political activity was an insufficient basis for standing.[260] Nonetheless, just years after that *Laird* was decided, Justice Marshall's dissent from the majority in *Smith*—the seminal case that articulated the third-party doctrine and eventually instigated the passage of the SCA—rearticulated the concern over a potential chilling effect caused by government surveillance.[261] Most recently, Justice Sotomayor's concurrence in *Jones* invited the Court to reconsider *Smith*'s third-party doctrine in light of the chilling effect it might have on the freedom to associate: "awareness that the government may be watching chills associational and expressive freedoms."[262] With *Carpenter* on the docket this term, the Supreme Court now has an opportunity to move away from assessing acts of government surveillance purely under Fourth Amendment doctrine, and instead may return to *NAACP*, *Shelton*, and *Keith*-like considerations of the chilling effect doctrine.[263]

As to how a First Amendment-based chilling effect argument advanced by constituents other than the intermediary-recipients of SCA-sanctioned

---

259 *See, e.g.*, United States v. U.S. Dist. Court for the E. Dist. of Mich. (*Keith*), 407 U.S. 297, 320 (1972) ("Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech.").

260 As the *Laird* Court explained:

> The decisions in [past cases recognizing a First Amendment claim based on a chilling effect] fully recognize that governmental action may be subject to constitutional challenge even though it has only an indirect effect on the exercise of First Amendment rights. At the same time, however, these decisions have in no way eroded the established principle that to entitle a private individual to invoke the judicial power[,] . . . he must show that he has sustained, or is immediately in danger of sustaining, a direct injury as the result of that action.

408 U.S. 1, 12-13 (1972) (internal quotation marks omitted).

261 "The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts." *Smith v. Maryland*, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting) (citing NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 463 (1958)).

262 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

263 Alex Abdo argues that a First Amendment analysis of *Carpenter*

> 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. . . . 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.

Abdo, *supra* note 3, at 456.

search warrants would play out, the 2012 state criminal law case, *People v. Harris*, and the criticism that came in its wake are instructive. After Twitter went against the nondisclosure order it received from prosecutors and notified the defendant that it had received a subpoena seeking more than three months' worth of his tweets and subscriber information,[264] Harris—the Occupy Wall Street protestor on trial for public disorder—attempted to challenge the order himself.[265] "This is the legal equivalent of busting a party with loud noise and demanding my phone records for 3.5 months to see if I helped plan it," he tweeted at the time.[266] But the court rejected the defendant's motion to quash the subpoena, holding that:

> New York courts have yet to specifically address whether a criminal defendant has standing to quash a subpoena issued to a third-party online social networking service seeking to obtain the defendant's user information and postings. Nonetheless, an analogy may be drawn to the bank record cases where courts have consistently held that an individual has no right to challenge a subpoena issued against the third-party bank.[267]

Note that here, the court was in part referencing *United States v. Miller*, where the Supreme Court held that a bank customer, like the defendant in *Smith*, had no reasonable expectation of privacy in cancelled checks and other transactional information held by his bank under the Fourth Amendment's third-party doctrine.[268] As Aden Fine, then a senior staff attorney with the American Civil Liberties Union's Speech, Privacy and Technology Project, told me in 2012, *Harris* is distinct from such "bank record cases" because "'this case limits First Amendment rights as well" because tweets directly deal with free speech, and "[u]sers should be able to go to court to protect their constitutional rights."[269] The *Harris* case further illustrates, then, that as privacy rights seem to erode in the age of Twitter, particularly in the face of growing government surveillance of communications, First Amendment rights should be deployed to fill the gap, thereby giving individuals like Harris the opportunity to vindicate their constitutional rights.

---

264 Note that it was later determined that because one day's worth of the tweets sought by the prosecution were less than 180 days old, that information would have to be compelled by a *search warrant*, rather than a *subpoena*, pursuant to 18 U.S.C. § 2703. People v. Harris (*Harris II*), 949 N.Y.S.2d 590, 596 (Crim. Ct. 2012).

265 People v. Harris (*Harris I*), 945 N.Y.S.2d 505, 506 (Crim. Ct. 2012).

266 Simmons, *supra* note 167.

267 *Harris I*, 945 N.Y.S.2d at 507-08 (footnote omitted) (citing United States v. Miller, 425 U.S. 435, 442 (1976), where the Court held that a bank customer, like the defendant in *Smith*, had no reasonable expectation of privacy in cancelled checks and other transactional information held by his bank).

268 425 U.S. 435, 442 (1976).

269 Simmons, *supra* note 167.

CONCLUSION

In October 2017, the DOJ issued new guidelines limiting the circumstances under which prosecutors should seek gag orders in connection to domestic criminal investigations under the SCA,[270] likely with the merits of intermediaries' and potentially others' First Amendment challenges to such orders in mind. The DOJ's goal was likely to obviate the need for Microsoft, or any other Internet intermediary or interested stakeholder, to bring suit in raising a facial challenge to § 2705(b)—and it seems to have succeeded, given that Microsoft volunteered to drop its suit as soon as the new policy was released.[271] Therefore, should the guidelines be viewed as an end to the saga of SCA-sanctioned gag orders and their effect on the privacy and speech rights of intermediaries, individuals, and the public at large? And what does the new gag order policy mean for the rest of the SCA's government surveillance regime in the digital age? Ultimately, the DOJ's guidelines are not a complete solution, but they are a step in the right direction toward finding an appropriate balance between security and liberty.[272]

Deputy Attorney General Rod Rosenstein's memorandum to prosecutors generally calls for each application for a notice-of-preclusion order to "have an appropriate factual basis" and to "extend only as long as necessary to satisfy the government's interest."[273] Specifically, in terms of scope, the new policy calls on prosecutors seeking gag orders to "*tailor* the[ir] application to include the available facts of the specific case and/or concerns attendant to the particular type of investigation."[274] This requirement, of course, goes well beyond the mere "reason to believe" standard stated in § 2705(b), as the statute does not require the government to show any facts supporting such a belief.[275] From the list of factors the SCA's gag order provision uses to assess the validity of a government request to preclude notice, the guidelines also require prosecutors to state which particular element its available facts in support.[276] This change is clearly designed to curtail the number of gag order requests made by the government, while retaining the permissive catchall reason to pursue a gag order: "or otherwise seriously jeopardizing an investigation or unduly delaying a trial."[277] Lastly, in terms of time

---

270 *See generally* Rosenstein Memo, *supra* note 15.

271 *Farivar*, supra note 11.

272 The guidelines are also similar in style to broad interpretation of the NSL gag order statutes used in *Doe III* and *Sessions*.

273 Rosenstein Memo, *supra* note 15, at 1.

274 *Id.* at 2 (emphasis added).

275 18 U.S.C. § 2705(b) (2012).

276 Rosenstein Memo, *supra* note 15, at 2.

277 18 U.S.C. § 2705(b).

restrictions, "barring exceptional circumstances, prosecutors filing § 2705(b) applications may only seek to delay notice for one year or less," and any requests for an extension of the original expiration date must be supported with additional facts that have come to light during the course of the criminal investigation.[278] This new initiative is sweeping, seeming to aim at ending the practice of issuing indefinite, arguably permanent gag orders on Internet intermediaries.

But whether the DOJ's guidelines will have the effect of ending the routine use of these indefinite gag orders is questionable at best. As Rosenstein's memo notes, the SCA's gag order provision is written to ultimately leave the scope of notice-of-preclusion orders out of the hands of the government (or any other interested party) and instead up to the discretion of the courts: "the Department recognizes that judges may direct shorter or longer periods for orders, consistent with the language of § 2705(b)."[279] Courts considering issuing gag orders on Internet intermediaries "for *such period* as [they] deem[] appropriate" are, of course, not bound by DOJ's new policy.[280] Furthermore, it is unclear how binding these guidelines are even on the prosecutors to whom they are directed. For this reason, the EFF responded that it is "naturally skeptical of this change coming in the form of an administrative policy that can be revoked whenever the DOJ sees fit."[281]

On the other end of the spectrum of possible reforms, however, a complete and total overhaul of the SCA or even the ECPA as a whole seems unlikely in light of the current political climate. This assumption will be tested in part by the Email Privacy Act, which would codify *Warshak* and require the government to obtain a search warrant with probable cause in order to access any digital communications, no matter their age in electronic storage.[282] The bill first passed in the House of Representatives unanimously in 2016, but has been in a standstill in the Senate since early 2017.[283] In the meantime, then, the DOJ's guidelines are a step in the right direction, as the EFF and other privacy advocates concede.[284]

However, a better solution to the problem of SCA-sanctioned gag orders—and the broader issue of government surveillance via third-party

---

278 Rosenstein Memo, *supra* note 15, at 2.

279 *Id.* at 3.

280 18 U.S.C. § 2705(b) (emphasis added).

281 Andrew Crocker, *New DOJ Policy on Gag Orders Is Good, but the Courts Could Have Done Better*, ELECTRONIC FRONTIER FOUND. (Oct. 25, 2017), https://www.eff.org/deeplinks/2017/10/new-doj-policy-gag-orders-good-courts-could-have-done-better [https://perma.cc/H2MJ-ZRTE].

282 *See* Dustin Voltz, *U.S. House Passes Bill Requiring Warrants to Search Old Emails*, REUTERS (Feb. 6, 2017, 6:2 5PM), https://www.reuters.com/article/us-usa-congress-emails-idUSKBN15L2N3 [https://perma.cc/TYE7-SV5D].

283 *Id.*

284 *See* Crocker, *supra* note 281.

intermediaries—might be found in the judiciary, rather than through prosecutorial discretion or statutory amendment. Abdo advocates for a far-reaching reconfiguration of the standards that courts use to assess the constitutionality of government surveillance and the gag orders that often hide its reach.[285] Under the current Fourth Amendment-centric analysis of government surveillance, "[t]he result is that the First Amendment freedoms of speech and of the press are often at the mercy of Fourth Amendment doctrine."[286] Abdo argues that these issues should instead be judged according to First Amendment doctrine for several reasons: 1) the Fourth Amendment's third-party doctrine has significant, overlooked implications for free expression; 2) the Fourth Amendment "is often blind" to the mosaic theory of big data aggregation; 3) the Fourth Amendment focuses on individual, rather than societal, harms, thereby ignoring any chilling effect surveillance might have on other constituents; 4) the Fourth Amendment does not use the protective strict scrutiny standard of review and does not require narrow tailoring; and 5) the Fourth Amendment has developed in the context of criminal cases, where there is "judicial antipathy" towards claimants and their relief sought.[287]

This shift towards the First Amendment—which is less a novel approach and more a return to the standard used in cases such as *Lamont*, *NAACP*, and *Shelton*—would not have the effect of completely undoing the ability of investigators to reach Internet intermediaries in the digital age, but it would at least allow more opportunity for those third parties to have their First Amendment rights vindicated, giving them the freedom to tell individuals and the public when their respective rights and interests are being implicated. Moreover, with more information about the practice and effect of government surveillance in the marketplace of ideas, true targets would be able to assert their own constitutional rights and the public would be able to debate about the often competing values of security, privacy, and free speech—and that development, in turn, might lead to real, lasting change. The Supreme Court will soon have the opportunity to consider reinjecting the First Amendment into constitutional issues surrounding government surveillance in *Carpenter*. Here, a reinforcement of free speech rights in the face of constitutionally suspect government surveillance via Internet intermediaries and gag orders silencing said intermediaries could work as an antidote to the problem of shrinking privacy rights in the digital age, thereby fulfilling the initial

285 Abdo, *supra* note 3, at 445.
286 *Id.* at 451.
287 *Id.* at 445.

promise of the SCA and ensuring that in the twenty-first century, the First Amendment is much more than a local ordinance.[288]

Preferred Citation: Amanda R. Simmons, Comment, *Surveilling and Then Shooting the Messenger: Intermediaries, Gag Orders, and the First Amendment*, 167 U. PA. L. REV. ONLINE 191 (2018), http://www.pennlawreview.com/online/167-U-Pa-L-Rev-Online-191.pdf.

288 *Contra* BARLOW, *supra* note 1 ("[I]n Cyberspace, the First Amendment is a local ordinance.").