No. 15-60205

IN THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

GOOGLE, INC.

Plaintiff-Appellee

V.

JAMES HOOD, III,
in his official capacity as Attorney General of the State of Mississippi

Defendant-Appellant

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF MISSISSIPPI NORTHERN DIVISION

BRIEF OF *AMICI CURIAE* THE AMERICAN CIVIL LIBERTIES UNION AND THE AMERICAN CIVIL LIBERTIES UNION OF MISSISSIPPI IN SUPPORT OF APPELLEE

Charles Irvin
American Civil Liberties Union Foundation of Mississippi
233 E. Capital Street
Jackson, MS 39225
T: (601) 354-3408
F: (601) 355-6465
cirvin@aclu-ms.org

Esha Bhandari
Samia Hossain
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 284-7369
F: (212) 549-2654
ebhandari@aclu.org
shossain@aclu.org

ATTORNEYS FOR *AMICI CURIAE*

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES

Pursuant to this Court's Rule 29.2, the undersigned counsel of record for *amici curiae* certifies that the following additional persons and entities have an interest in the outcome of this case:

1. American Civil Liberties Union, *amicus curiae*;

2. Esha Bhandari; Samia Hossain, counsel for *amicus curiae* American Civil Liberties Union;

3. American Civil Liberties Union of Mississippi, *amicus curiae*;

4. Charles Irvin, counsel for *amicus curiae* American Civil Liberties Union of Mississippi;

SO CERTIFIED this 3rd day of August, 2015

s/ Esha Bhandari
Esha Bhandari

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Mississippi is a state affiliate of the National ACLU. Founded in 1920, the ACLU has vigorously defended the First Amendment for nearly a century in state and federal courts across the country. It has also been at the forefront of efforts to ensure that the Internet remains a free and open forum for the exchange of information and ideas, and to ensure that the right to privacy remains robust in the face of new technologies. The ACLU has served as direct counsel and *amicus* in cases raising these issues. *See, e.g. Reno v. ACLU*, 521 U.S. 844 (1997); *Ashcroft v. Free Speech Coal.*, 535 U.S. 234 (2002). Accordingly, the proper resolution of this case is a matter of substantial interest to the ACLU and its members.

The ACLU files this brief in support of Appellee to defend the First Amendment rights of individual Internet users whose rights to free speech, anonymity, and privacy are at stake in this case.

STATEMENT PURSUANT TO FED. R. APP. P. 29(c)(5)

No party or party's counsel has authored any portion of this brief, and no one other than *amici curiae* or their counsel have contributed money to fund the preparation or submission of this brief.

SUMMARY OF ARGUMENT

This case arises out of an extremely broad, 79-page administrative subpoena issued to Google, Inc. by the Attorney General of the State of Mississippi. The subpoena seeks information about the identities, communications, searches, and other Internet activity of an untold number of individuals whose speech the State deems "offensive," "dangerous," or otherwise "objectionable." These vast categories encompass wholly protected speech such as the promotion of sports and political protest activity. When the State uses its subpoena authority to seek information protected by the First Amendment, it must demonstrate a compelling interest in the information, and a substantial nexus between the information sought and any such interest. The State's subpoena fails on both counts.

The asserted purpose of the State's subpoena is to investigate Google for violations of state consumer protection laws. This purpose is belied by the fact that the subpoena covers a vast array of subjects that are both unrelated to consumer protection and entirely beyond the State's jurisdiction to investigate. The subpoena instead burdens the First Amendment rights of millions of individual Internet users

with absolutely no connection to Mississippi. Among its numerous demands, the subpoena calls for the disclosure of individual Internet postings on Google services, as well as related identifying information including personal email addresses and Internet Protocol ("IP") addresses. Enforcement of the subpoena would therefore infringe the First Amendment right to speak anonymously online by identifying innumerable Internet speakers.

Furthermore, the sheer breadth of the subpoena impermissibly chills constitutionally protected speech on the Internet. This chill will disproportionately affect individuals who have views the State is likely to find unpalatable, because those individuals risk having their speech subject to greater scrutiny.

For these reasons, the order of the district court granting a preliminary injunction against enforcement of the State's subpoena to Google should be affirmed.

ARGUMENT

I. THE STATE'S SUBPOENA VIOLATES THE FIRST AMENDMENT RIGHTS OF INDIVIDUAL INTERNET USERS.

The State's issuance of the instant subpoena violates the First Amendment rights of countless individuals who use the Internet. The government has the power to seek information on protected speech only where it can demonstrate that there is a substantial nexus between the information sought and a compelling government

interest. *See, e.g.*, *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963) (holding that subpoena to race relations organization from legislative committee authorized to investigate Communist activity could not be enforced because it was not narrowly tailored to a compelling state interest). In this case, the State does not, and cannot, demonstrate any compelling interest in the wholesale gathering of information about a wide and disparate array of protected speech on Google's various services. Indeed, the subpoena seeks such a vast amount of information about so many people that by its very nature it cannot be narrowly tailored to any legitimate investigative need. As such, the subpoena is presumptively invalid.

Furthermore, where a subpoena's breadth chills the speech of countless individuals, it is also constitutionally impermissible. The subpoena to Google is substantially overbroad in seeking information about the protected speech of Internet users, as well as information that could reveal their actual identities. It impermissibly risks chilling speech by those who may worry that they will lose their anonymity or that their protected activity will get swept into the crosshairs of a government investigation. *See, e.g.*, *NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that order requiring NAACP to hand over membership lists to Alabama Attorney General entailed a likelihood of substantial restraint upon members' right to free association).

A. The Court should consider the rights of the countless individual Internet users whose speech and communications are encompassed in the subpoena's demands.

Even though the subpoena is directed at Google, it nonetheless implicates the rights of an untold number of individuals who use Google services. Courts have recognized the importance of considering third-party First Amendment interests when they are at stake, and have consistently permitted Internet users to protect their First Amendment rights through motions to quash subpoenas issued to their Internet service providers. *See, e.g.*, *Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010), *USA Tech., Inc. v. Doe*, 713 F. Supp. 2d 901, 904–05 (N.D. Cal. 2010); *Doe v. 2TheMart.com, Inc.*, 140 F. Supp. 2d 1088, 1090–91 (W.D. Wash. 2001). Nor are the First Amendment rights of individuals forfeited merely because they have willingly given their content or communications to a third party, from whom the State seeks the information. *See United States v. Miller*, 425 U.S. 435, 444 n.6 (1976) (expressly recognizing that First Amendment claims may be implicated by the summons of a third-party's records held by a bank).

In this case, the State's 79-page subpoena to Google is targeted directly at the protected speech and communications of individual users. *See* Motion to Dismiss, Ex. A, *Google, Inc. v. Hood*, No. 3:14CV981-HTW-LRA, 2015 WL 1546160 (S.D. Miss. Jan. 12, 2015) (hereinafter "Subpoena"). Over one hundred document requests and interrogatories require Google to turn over information

about individual YouTube videos, websites, search terms, customer service requests, and so on. All told, the subpoena's requests could result in millions of posts and communications being turned over to the State.

The potential scope of the subpoena cannot be overstated. Google Search is used by over one billion users around the world who send Google 3.5 billion search queries per day (40,000 queries per second). Declaration of Brian Downing at 2, *Google, Inc. v. Hood*, No. 3:14CV981-HTW-LRA, 2015 WL 1546160 (S.D. Miss. Dec. 19, 2014). The vast majority of Internet users use Google Search over other search engines, and each search sends Google various packets of information, including the IP address of the user, the individual search term, the time of the search, any log-in information, and so on. *See* comScore, *comScore Releases March 2014 U.S. Search Engine Rankings*, (Apr. 15, 2014)[1] (stating Google leads search engine market with 67.5% explicit search share). Google's other services are used by enormous numbers of people as well. YouTube has more than one billion users, and three hundred hours of video are uploaded to YouTube every minute. YouTube, *Statistics*.[2] Google's social network, Google+, reached 300 million active users in 2013, and 1.5 billion photos are uploaded to Google+ every

[1] https://www.comscore.com/Insights/Press-Releases/2014/4/comScore-Releases-March-2014-U.S.-Search-Engine-Rankings.

[2] https://www.youtube.com/yt/press/statistics.html (last visited Aug. 3, 2015).

week. Alistair Barr, *Google's Social Network Sees 58% Jump in Users*, USA Today (Oct. 29, 2013).[3] The sheer numbers of individuals whose rights are at stake in this subpoena sound a constitutional alarm.

B. The subpoena burdens speech protected by the First Amendment.

The subpoena burdens the exercise of First Amendment rights by individual Internet users who stand to have information about their protected speech and communications turned over to the State. It is well established that First Amendment protection extends to all but certain discrete and narrowly defined categories of speech. *See Miller v. California*, 413 U.S. 15, 27 (1973) (obscenity); *N.Y. Times v. Sullivan*, 376 U.S. 254, 279–80 (1964) (defamatory statements); *Virginia v. Black*, 538 U.S. 343, 359 (2003) ("true threats"); *New York v. Ferber*, 458 U.S. 747 (1982) (child pornography); *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (direct incitement to violence). These First Amendment protections are no less robust online. *Reno*, 521 U.S. at 870 (rejecting any attempt to "qualify[] the level of First Amendment scrutiny that should be applied" to the Internet).

Despite this well established law, the State's subpoena seeks the disclosure of clearly protected speech as well as identifying information for those who posted it. The subpoena targets content posted on certain Google services, or communications between Google and its users, that "promote," "disseminate,"

[3] http://www.usatoday.com/story/tech/2013/10/29/google-plus/3296017/.

"offer for sale," "engage in," or "facilitate" so-called "Dangerous or Unlawful Content/Conduct." *See, e.g.*, Subpoena at 31 (Doc. Req. No. 46) (seeking "all communications with users who post, have posted, or attempted to post videos on YouTube" that fall within the category described above); *id.* at 22 (Doc. Req. No. 23) (seeking "all communications between Google and websites or posters of videos on YouTube" that fall within the category described above). The subpoena defines "Dangerous Content or Conduct" as:

> content, conduct or information that in itself is dangerous or *has indicia* that it *could*, in *any* way, either directly, *indirectly* or *tangentially*, aid, abet, assist, *facilitate*, *encourage* or *promote* activity that *could* lead to physical harm or injury and takes into account all facts and circumstances, including the age of the intended audience.

Id. at 4 (emphases added).[4]

[4] The subpoena requests that use this category of "Dangerous Content or Conduct" to single out records about individual users' content and communications include documents and information relating to:

(1) The use of Google services to "promote, offer for sale, disseminate, facilitate, or otherwise engage in Dangerous or Unlawful Content/Conduct. *See* Subpoena at 24 (Doc. Req. No. 28); 27 (Interrog. No. 16); 31 (Doc. Req. No. 45) (relating specifically to YouTube videos); 43 (Interrog. No. 33).

(2) The display of advertisements next to or in conjunction with websites or YouTube videos promoting/facilitating/selling/disseminating such content. *See id.* at 17 (Interrog. No. 10); 20 (Doc. Req. No. 16); 21 (Doc. Req. No. 17); 23 (Doc. Req. No. 26); 25 (Doc. Req. No. 33); 26 (Doc. Req. No. 35); 31 (Doc. Req. No. 47); 65 (Interrog. No. 56).

(3) Communications between Google and content posters or users of Google Advertising Services that are or appear to be disseminating such content.

This definition is so broad that it encompasses an enormous amount of speech protected by the First Amendment. While it is not outside the State's subpoena power to demand information related to protected speech, any such request must be tailored to a compelling state interest. The State may not arbitrarily define "[d]angerous" speech that "could lead to physical harm or injury" as a type of speech that categorically deserves government scrutiny.

A few examples suffice to demonstrate the absurdity and scope of the subpoena's demands. Virtually any topic could be said to "indirectly" or "tangentially" "aid," or "facilitate" activity that "could lead to physical harm or injury"—from politics to skydiving. Discussing political activism or organizing a protest, as the "#BlackLivesMatter" movement does online, could inadvertently lead to physical harm or injury, including anything from an accidental fall to excessive force by arresting officers.[5] Any forums providing advice to victims of

---

See id. at 22 (Doc. Req. No. 23); 31(Doc. Req. No. 46); 32 (Doc. Req. No. 48).

(4) Complaints or reports relating to such content. *See id.* at 23 (Doc. Req. No. 27) (including complaints about "offensive" or "objectionable" content); 24 (Doc. Req. No. 30); 36 (Doc. Req. No. 58); 37 (Doc. Req. No. 62); 38 (Doc. Req. No. 65).

[5] *See* Georgia Wells, *Ferguson to New York, Social Media is the Organizer's Biggest Megaphone*, The Wall Street Journal Digits Blog, Dec. 4, 2014, http://blogs.wsj.com/digits/2014/12/04/ferguson-to-new-york-social-media-is-the-organizers-biggest-megaphone/ (describing importance of social media as a tool for organizing movements and protests, particularly for #blacklivesmatter).

domestic violence similarly may facilitate activity on the part of victims that "could" lead to physical injury—including against those very victims.[6] Discussion of the use of firearms on Google+ would also fall within the subpoena's ambit,[7] as would YouTube videos planning or promoting Fourth of July fireworks displays,[8] or anything depicting an individual playing a sport.[9] Internet posts about these activities encompass protected expression, and furthermore, are so commonplace online that if Google were to respond to the subpoena request in full, it would undoubtedly implicate millions of instances of user content and communications.

As broad as the subpoena's definition of "Dangerous Content or Conduct" is, the subpoena is broader still. It also seeks information regarding "offensive" or objectionable" content on any of Google's services. One such request reads as follows:

---

[6] *See* Anna L. Hurley et al., *The Construction of Self in Online Support Groups for Victims of Domestic Violence*, 46 British J. Soc. Psych. 859, 859–60 (2007) (describing how online "self-presentation" of domestic violence victims "may facilitate self-disclosure, as well as the provision of support and advice").

[7] *See, e.g.*, Google+, *Guns Across Google*, https://plus.google.com/communities/117483623355487604133 (a Google+ community page including discussions, information, and YouTube videos about firearms) (last visited Aug. 3, 2015).

[8] *See, e.g.*, NY on Air, *Macy's Fireworks in NYC* (July 4, 2015), https://www.youtube.com/watch?v=ZexAuD8e4J8.

[9] *See, e.g.*, N.Y. Times, *Gnarly in Pink*, June 24, 2014, https://www.youtube.com/watch?v=LpR7Mp6sjY0 (film celebrating group of 6-year-old girls who share a passion for skateboarding).

> Provide a searchable database of those instances where offensive, objectionable, dangerous or unlawful content has been identified by you or your users, through a user-generated "flagging" process or any other system or manner since January 1, 2012, where a decision was made not to remove the content. For each, provide a copy of the user, or "flagged" complaint and indicate if the content was monetized in any way.

Subpoena at 35 (Doc. Req. No. 57); *see also id.* at 36 (Doc. Req. No. 59) (requesting "all documents reflecting reports or complaints to Google" about any entity violating the subpoena's definition of "Dangerous Content or Conduct").

The terms "offensive" and "objectionable" are not defined in the subpoena, and, in any event, the First Amendment protects speech that is offensive or objectionable. *See United States v. Stevens*, 559 U.S. 460, 470 (2010) (holding that videos depicting animal cruelty did not fall under any of the narrowly circumscribed categories of unprotected speech—and thus were protected—even if the videos were offensive and "deemed valueless"). Similar to its collection of information about "dangerous" speech, the State appears to assume that categorically gathering information about "offensive" or "objectionable" speech can also be a compelling interest. Given that such speech is constitutionally protected, however, that assumption is contrary to the State's properly compelling interest in respecting constitutional boundaries.

The "flagging" process that the above request refers to is included in many Google services, such as YouTube and Google+. It allows a user to notify Google

about content she believes conflicts with Google's user policies or community guidelines.[10] Google then decides whether or not to remove the content. The company's user policies and community guidelines are offered as a service to users, and are not tailored to single out speech unprotected by First Amendment doctrine. *See Reno*, 521 U.S. at 880 (striking down provisions of the Communications Decency Act that "would confer broad powers of censorship, in the form of a 'heckler's veto,' upon any opponent of indecent speech who might simply log on [and stifle expression]."). [11] The fact that Google exercises editorial judgment about which content to allow on its services and which to take down does not mean the State can substitute that judgment for the requirements of the

[10] *See* Declaration of Victoria Grand, Ex. 2, *Google, Inc. v. Hood*, No. 3:14CV981-HTW-LRA, 2015 WL 1546160 (S.D. Miss. Dec. 19, 2014) (Flagging Content); *see also id.* Ex. 6 (AdSense Content Policies Prohibited Content); *id.* Ex. 1 (YouTube Community Guidelines).

[11] The subpoena thereby formalizes a heckler's veto policy by using complaints about speech as a trigger for disclosure. The government cannot restrict lawful speech because of the way listeners might perceive it or react to it. *See Forsyth County v. Nationalist Movement*, 505 U.S. 123, 134–35 (1992) ("Speech cannot be financially burdened, any more than it can be punished or banned, simply because it might offend a hostile mob."); *Hopper v. City of Pasco*, 241 F.3d 1067, 1080 (9th Cir. 2001) ("Such censorship by public opinion only adds to the risk of constitutional impropriety." (quotations omitted)); *see also Beckerman v. City of Tupelo*, 664 F.2d 502, 502, 510 (5th Cir. 1981) (invalidating a parade licensing scheme authorizing the denial of a permit if the police determined that allowing the parade would "probably . . . provoke disorderly conduct" because "the fact that some speech may stir listeners to disagree—perhaps even to disagree violently—does not by that fact alone permit regulation." (citation and quotations omitted)).

First Amendment. The State's requests regarding "flagged" or "offensive" content are exceedingly broad given how many millions of individuals use Google services that allow flagging.[12] If even a small percentage of content is flagged, the number of flagged posts could run into the millions. And even where flagging has not resulted in false positives, the content may well be constitutionally protected speech that the State has no basis to target.

The State has impermissibly focused its subpoena on individual Internet users' speech that it deems "[d]angerous," "objectionable," or "offensive," which the Supreme Court has explained cannot be a basis for burdening speech. *See Stevens*, 559 U.S. at 470. As a result, the subpoena implicates the First Amendment rights of individual Internet users who stand to have information about their protected speech and communications turned over to the State.

C. The subpoena is so broad that it cannot be tailored to any compelling investigative interest.

As described above, the subpoena's scope is exceedingly broad and cannot possibly be tailored to any compelling state interest. The First Amendment prohibits government from taking actions that burden speech except in extraordinary circumstances. *See, e.g.*, *Ashcroft*, 535 U.S. at 244. More specifically, courts have recognized that government demands for information

[12] *See supra* Section I.A (describing statistics on use of Google services).

concerning expressive activities inherently burden speech and therefore implicate the First Amendment. *See, e.g.*, *Gibson*, 372 U.S. at 558 ("It is particularly important that the exercise of the power of compulsory process be carefully circumscribed when the investigative process tends to impinge upon such highly sensitive areas as freedom of speech or press, freedom of political a[ss]ociation, and freedom of communication of ideas." (citation and quotation marks omitted)); *United States v. Rumely*, 345 U.S. 41, 46 (1953) (holding that congressional committee did not have authority, as limited by the First Amendment, to issue a subpoena to bookseller seeking names of those who had purchased political publications).

Where, as here, the government seeks information about protected speech and communications, it must show both an "overriding and compelling" interest in obtaining that information and a substantial nexus between the information and that interest in order to overcome constitutional scrutiny. *See Gibson*, 372 U.S. at 546 (holding that a state legislative committee subpoena could not be enforced because "it is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech . . . that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest"). In other words, the government "must use a scalpel, not an ax" when First Amendment interests are at

stake. *Ealy v. Littlejohn*, 569 F.2d 219, 228 (5th Cir. 1978); *see also Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n*, 667 F.2d 267, 273 (2d Cir. 1981) (holding that a third-party subpoena is invalid "when the end can be more narrowly achieved" (quoting *Shelton v. Tucker*, 364 U.S. 479, 488 (1960) (quotation marks omitted))); *Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972) (holding that "[w]hen governmental activity collides with First Amendment rights, the Government has the burden of establishing that its interests are legitimate and compelling and that the incidental infringement upon First Amendment rights is no greater than is essential to vindicate its subordinating interests"); *In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1302 (4th Cir. 1987) (quashing a subpoena requiring videotape distributers to produce copies of videos, and holding that the government must act "in the least intrusive manner possible").

The State cannot make the required showing here. While it claims to be investigating Google's potential violations of Mississippi consumer protection laws, *see* Subpoena at 1–2, this claim is contradicted by the extraordinary breadth of the subpoena. As an initial matter, the subpoena seeks information about alleged conduct that violates the laws of *other* states or jurisdictions,[13] and is in no way

[13] Indeed, the subpoena explicitly includes *other* states' laws, as well as federal laws, in its definition of "Unlawful Content" or "Illegal Content" that is then subject to scrutiny by the State. *See* Subpoena at 7–8 (defining such content as that

tailored to information about Mississippi residents, or entities that do business in Mississippi.[14]

More importantly, however, the request seeks vast amounts of information about speech that is constitutionally protected. Mississippi cannot possibly demonstrate that the majority of the information responsive to the subpoena bears any nexus—let alone a substantial one—to a legitimate investigation of illegal conduct. *See Gibson*, 372 U.S. at 546; *Familias Unidas v. Briscoe*, 619 F.2d 391, 400–01 (5th Cir. 1980) (invalidating a Texas statute compelling public school-related disclosures on First Amendment grounds because, while the disclosure requirements were generally related to a permissible state purpose, they "swe[pt] too broadly"); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1058 (Colo.

---

which is itself in violation of, or has indicia that it could directly or indirectly facilitate, any violation of "any criminal or civil law of the United States or that of any state or territory.").

[14] Most of the subpoena requests that seek information about individual users' content and communications are not, on their face, limited to individuals in Mississippi. The subpoena thus implicates the rights of all Google users without regard to geographic limitation. In fact, the subpoena notes that where it specifically asks about Mississippi consumers, and Google "only has responsive information for all consumers without regard to location, then 'Mississippi consumer' shall mean consumer without regard to state of residence." Furthermore, the subpoena states that whenever it "seeks information on Mississippi consumers or activities and [Google does] not possess and produce such information, [Google] should produce the information requested for all consumers or all [its] activities without regard to geographic limitation." *See* Subpoena at 8–9, 11.

2002) (holding that "because the law enforcement officials' need to investigate crime will almost invariably be a compelling one . . . the court must engage in a more specific inquiry as to whether law enforcement officials have a compelling need *for the precise and specific information sought*." (emphasis original)); *see also supra* Section I.B. (discussing examples of information that would fall within the subpoena's scope).

The State is required to do more than simply claim a general interest in enforcing the law when serving a subpoena with such serious First Amendment implications. *See Bates v. City of Little Rock*, 361 U.S. 516, 525 (1960) ("[G]overnmental action does not automatically become reasonably related to the achievement of a legitimate and substantial government purpose by mere assertion."). Because there is no legitimate investigative reason for the State to so burden the protected speech of individual Internet users, and because it could have issued a much narrower request to obtain any information it might legitimately need, the subpoena is unconstitutional under the First Amendment.

D. The subpoena impermissibly seeks information that could identify anonymous Internet speakers.

The State's subpoena also demands information from Google that has the potential to reveal the identities of thousands, if not millions, of Internet users who have exercised their constitutional right to speak anonymously online. As explained below, the subpoena seeks the identifying information of individuals

who: a) post protected speech on Google's web platforms; and b) access information through Google. The State has not demonstrated a compelling justification for seeking such information wholesale, nor has it narrowly tailored its subpoena to any such interest. As a result, the subpoena violates Internet users' First Amendment right to speak anonymously by both directly unmasking speakers and creating a chilling effect over anonymous speech across the Internet.

As this Court has recognized, "anonymous speech is protected by the First Amendment . . . [and] extends beyond traditional publishing." *Justice for All v. Faulkner*, 410 F.3d 760, 764 (5th Cir. 2005). The Supreme Court has held that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication is an aspect of the freedom of speech." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). This recognition has guarded the role that anonymity has played over the course of our nation's history—starting with the Federalist Papers—as a "shield from the tyranny of the majority." *Id.* at 357. The courts have been emphatic: anonymous speech "is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent." *Id. See also* Jonathan Turley, *Registering Publius: The Supreme Court and the Right to Anonymity*, 2002 Cato Sup. Ct. Rev. 57, 58 (2002) ("For the Framers and their contemporaries, anonymity was the deciding factor between whether their writings would produce a social exchange or a personal beating.");

2theMart.com, Inc., 140 F. Supp. 2d at 1097 ("[T]he constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.").

Because the First Amendment protects the right to speak anonymously, the State must demonstrate a substantial nexus between the information sought and a compelling government interest. *See supra* Section I.C; *see also NLRB v. Midland Daily News*, 151 F.3d 472, 475 (6th Cir. 1998) (affirming denial of NLRB's motion to compel identification of anonymous advertisers because its subpoena "facially failed to demonstrate a substantial state interest" and was not "the least extensive means" by which to proceed). The State cannot possibly satisfy this standard when it seeks identifying information about a wide swathe of Google users engaged in anonymous speech.

It would be difficult to lay out all the ways in which the State's subpoena demands information that could identify speakers in violation of their First Amendment right to remain anonymous. For the purposes of both brevity and clarity, this discussion will divide the subpoena's demands into two non-exclusive and overlapping categories of anonymous speakers who use Google services: content providers and users accessing information.

First, the subpoena seeks to identify content providers who host websites displayed on Google's search results, submit video content to YouTube, or

otherwise contribute material to Google's web services. The subpoena seeks personally identifying information about those people through communications and transactional data requests like the following:

> Provide all communications with users who post, have posted, or attempted to post videos on YouTube that promote, disseminate, offer for sale, engage in or facilitate Dangerous or Unlawful Content/Conduct, including but not limited to, the sale of illicit drugs and pharmaceuticals.

Subpoena at 31 (Doc. Req. No. 46).[15] This request, and others like it, demand "all communications," which would include all "e-mail messages, text messages,

[15] The subpoena contains a host of requests that would similarly identify content providers who are engaging in protected speech. *See, e.g.*, Subpoena at 15 (Doc. Req. No. 6) (seeking documents—including communications—related to the provision of customer assistance to any website suspected of promoting "Dangerous or Illegal Content/Conduct"); 16 (Doc. Req. No. 8) (requesting "all records that identify or address online pharmacy sales"); 21 (Doc. Req. No. 17) (requesting documents related to contracts or agreements to provide Google advertising services to content providers who appear to be promoting "Dangerous or Illegal Content/Conduct"); 22 (Doc. Req. No. 23) (seeking all communications between Google and content providers who appear to be promoting "Dangerous or Illegal Content/Conduct"); 23 (Doc. Req. No. 25) (seeking communications from Google to content providers about whether their content is lawful or unlawful); 24 (Doc. Req. No. 28) (requesting documents—including communications—between Google and content providers concerning the use of Google services to promote "Dangerous or Illegal Content/Conduct"); 29–30 (Doc. Req. No. 42) (seeking all documents—including communications—that relate to investigations of content providers promoting "Dangerous or Illegal Content/Conduct"); 31 (Doc. Req. No. 46) (seeking all communications with users who have posted or attempted to post YouTube videos that promote "Dangerous or Unlawful Content/Conduct); 32 (Doc. Req. No. 48) (seeking all communications with entities using Google advertising services that appear to be promoting "Dangerous or Unlawful Content/Conduct).

instant messaging," "telephone records," "letters or other correspondence," and other communications data from anyone whose speech falls into the category of interest to the State. *See id.* at 5. For example, if an individual posting "Dangerous" content has emailed Google for assistance at any point, that email would be turned over to the State, along with any identifying information in it, such as the content provider's name and personal email address. Google's communications data could also include transactional information from the content provider, such as the IP address from which she posted her content. This information alone, coupled with the time of the post, could be enough to identify the speaker, because IP addresses are generally assigned to individual users by their Internet service providers. *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir. 2004).[16] If a content provider has created a YouTube or other Google account in order to post content

[16] The demand for "communications" related to speech posted on Google's services is particularly pernicious from a First Amendment perspective, because details that are not publicly available may often provide context and meaning to speech made publicly. By determining the geographic location from which a post was made—through the IP address—the government can derive meaning that might not otherwise be apparent to the public. For example, a comment that "I dislike the police" can have very different implications if the speaker's location is known. For that reason, location information can have First Amendment implications. *See City of Ladue v. Gilleo*, 512 U.S. 43, 56 (1994) ("Displaying a sign from one's own residence often carries a message quite distinct from placing the same sign someplace else, or conveying the same text or picture by other means."); *Santa Monica Food Not Bombs v. City of Santa Monica*, 450 F.3d 1022, 1048 (9th Cir. 2006) ("[A] location itself may be significant to the content of the message.").

without using her real name, Google's transactional data could also include information about the account log-in activity associated with content, which could also serve to identify the individual.

The State's subpoena seeks access to all of the above-described information for individuals engaged in protected speech, with no showing that such access is in any way necessary or narrowly tailored to a legitimate investigation. As is apparent from the very broad definition of so-called "Dangerous Content or Conduct," an enormous number of content providers are implicated by this type of request. The subpoena seeks information that would risk disclosing the identities of all those who "promote" "[d]angerous" activity, including such things as engaging in political activity or discussing medical treatments. *See supra* Section I.B. Again, this would disclose an array of private information for an enormous number of anonymous speakers online with no apparent justification.

Similarly, several of the State's demands implicate the identities of those who anonymously access information through Google, including through Google Search. Such users would include those who anonymously contact Google to complain about websites they may not want their names associated with. For example, consider the following request:

> Provide all documents, including communications, concerning the existence of spyware, malware, viruses, or other malicious code on piracy sites including the Specified Domains.

Subpoena at 74 (Doc. Req. No. 127); *see also id.* at 25 (Doc. Req. No. 33) (requesting "all communications with advertisers regarding the content of sites or YouTube videos in connection with which ads actually appear, including complaints that advertisements were placed on sites or in connection with YouTube videos that . . . appear to be promoting . . . Dangerous or Illegal Content/Conduct.").[17]

It does not take a stretch of the imagination to understand why some Google users would use anonymous email addresses or anonymizing services such as Tor[18] when complaining about malware or advertisements on websites that include controversial content—content that may still be within the First Amendment's

[17] *See also* Subpoena at 15 (Doc. Req. No. 6) (requesting documents—including communications—related to Google customer support for anyone suspected of promoting "Dangerous or Illegal Content/Conduct"); 23 (Doc. Req. No. 27) (seeking all documents relating to complaints about content); 26 (Doc. Req. No. 36) (same); 29–30 (Doc. Req. No. 42) (seeking documents related to investigations of anyone promoting "Dangerous or Illegal Content/Conduct" in connection with Google Search and other services); 36 (Doc. Req. No. 59) (requesting documents created by Google about the use of Google services by an entity that appears to be promoting "Dangerous or Illegal Content/Conduct"); 37 (Doc. Req. No. 62) (seeking all documents—including communications—in which websites are flagged by reviewers for "Dangerous or Unlawful Content/Conduct"); 38 (Doc. Req. No. 65) (same); 45 (Doc. Req. No. 82) (requesting records related to advertiser complaints); 72 (Doc. Req. No. 119) (seeking all documents, including communications, concerning the use of Google services to "locate, obtain, or view material that infringes copyright," which would include individualized search terms).

[18] Tor Project, https://www.torproject.org/ (last visited Aug. 3, 2015).

protection. The document requests above would unmask someone rightfully concerned about a virus infecting her computer because "all documents" would include her complaints (that might facially reveal her identity), and may also include her name, IP address, email address, and/or other information. The State's subpoena thus not only targets content it deems "objectionable" or "offensive," but scrutinizes content *others* personally find worthy of removal, *as well as* unmasking those very individuals who are flagging content and ostensibly helping the State achieve its goal.

The State has provided no justification for eviscerating the First Amendment protection to speak anonymously for countless individuals online. By directly unmasking content providers and those who use Google services to access information, the subpoena will also significantly deter others who use the Internet anonymously. The subpoena should therefore not be enforced.

E. The subpoena impermissibly chills protected speech online, including anonymous speech.

The subpoena impermissibly chills the free flow of protected online speech because it subjects individuals exercising their First Amendment rights to having information about their speech turned over to the State. The knowledge that the government is, in effect, keeping a copy of all speech that it deems of interest can impose a significant chilling effect. *See United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be

watching chills associational and expressive freedoms."); *see also NAACP*, 357 U.S. at 449. The forced disclosure of content is no less problematic, even if the content was at one time posted publicly. *Comty.-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102, 1122 (D.C. Cir. 1978) (holding that an F.C.C. requirement that government-funded, non-commercial radio stations tape-record all broadcast public affairs programs for the F.C.C. Commissioners' use was unconstitutional because it was likely to chill speech and served no legitimate government interest).

The threat of chill is uniquely powerful on the Internet. Although the progress of the Internet allows individuals unprecedented access to create and disseminate information through websites like YouTube and social networks including Google+, the resulting storage of vast amounts of personal information—which the government may then seek to obtain—poses a significant threat to free speech and privacy. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). The ease with which information is shared over the Internet therefore exacerbates the chilling effect that would likely be felt—rationally or otherwise—from government surveillance of speech. Courts are particularly concerned with a chilling effect over online speech regarding controversial political and social issues, as well as issues implicating personal safety and privacy. The court in *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007), noted the following in

evaluating a grand jury subpoena to Amazon.com seeking information about individual buyers:

> [I]f word were to spread over the Net—and it would—that [the government] had demanded and received Amazon's list of customers and their personal purchases, the chilling effect on expressive e-commerce would frost keyboards across America. Fiery rhetoric quickly would follow and the nuances of the subpoena (as actually written and served) would be lost as the cyberdebate roiled itself to a furious boil. One might ask whether this court should concern itself with blogger outrage disproportionate to the government's actual demand of Amazon. The logical answer is yes, it should: well-founded or not, rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers into canceling planned online book purchases, now and perhaps forever.

Id. at 573.

Furthermore, the fear of chill is not merely speculative. In 2006, the government subpoenaed information from the four major Internet search engines (AOL, Microsoft, Yahoo, and Google) regarding what their customers were searching for on the Internet. As one might expect, the public reacted with fear and individuals modified their online search habits. *See, e.g.,* Katie Hafner, *After Subpoenas, Internet Searches Give Some Pause*, N.Y. Times, Jan. 25, 2006 at Al. The chilling effect was great enough that the district court considering a challenge to one of the subpoenas *sua sponte* raised privacy concerns with the request. *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 687–88 (N.D. Cal. 2006).

In this case, the State has similarly asked for all documents and communications—which could include search logs and IP addresses—relating to "objectionable" content. This includes demands for information on individual searches for copyright infringing material, which could cover a wide range of search requests on Google's search engines. *See* Subpoena at 72 (Doc. Req. No. 119). And yet this request is only *one* piece of the subpoena which, taken as a whole, would require turning over massive amounts of documents and data about individual online activity. The subpoena might thus result in individuals significantly curtailing their search habits and speech across the Internet. The extent of the chill is compounded by the fact that the State's subpoena imposes an ongoing obligation on Google to turn over content posted now and in the future. *See* Subpoena at 11.

Additionally, by seeking identifying information about Google's content providers and users, the subpoena significantly chills anonymous online speech. Countless people and organizations anonymously post content online in order to more freely engage in speech and expression, including for political and artistic purposes.[19] Many people create online content anonymously in order to protect

[19] *See* David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. HCR, 29th Sess., Agenda Item 3 at 19, U.N. Doc. A/HRC/29/32 (May 22, 2015) ("Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and

their safety, families, employment prospects, and for a whole host of other reasons. In fact, it is exceedingly common for people to express themselves on the Internet using pseudonyms rather than their real names.[20] By directly unmasking numerous online speakers, the subpoena not only chills those Google users' speech, but also deters unknown numbers of people from actively posting and searching for content on the Internet.

Even small infringements on individuals' rights require a compelling justification in the First Amendment context because "[f]reedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." *Healy v. James*, 408 U.S. 169, 183 (1972); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) ("It is characteristic of the freedoms of expression in general that they are vulnerable to gravely damaging yet barely visible encroachments."). The State has provided no such compelling justification for collecting massive amounts of information about

---

expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.").

[20] *See* Klint Finley, *Web Commenters Claim They Use Pseudonyms for Privacy, Not Trolling*, Wired (Dec. 15, 2014, 6:55 PM), http://www.wired.com/2014/12/disqus/ (stating survey by web commenting company noted that 63% of people on its service use pseudonyms).

online speech and identifying data related to that speech. The State's subpoena thus impermissibly chills constitutionally protected expression on the Internet.

CONCLUSION

This Court should hold that the district court correctly issued a preliminary injunction against enforcement of the Mississippi Attorney General's subpoena to Google because it will violate the First Amendment rights of individual Internet users, and impermissibly chills speech on the Internet. The preliminary injunction remains in the public interest. *See ACLU v. Reno*, 929 F. Supp. 824, 851 (E.D. Pa. 1996) ("No long string of citations is necessary to find that the public interest weighs in favor of having access to a free flow of constitutionally protected speech."). For these reasons, the district court order should be affirmed.

Respectfully submitted,

s/ Esha Bhandari

Charles Irvin
American Civil Liberties Union
Foundation of Mississippi
233 E. Capital Street
Jackson, MS 39225
T: (601) 354-3408
F: (601) 355-6465
cirvin@aclu-ms.org

Esha Bhandari
Samia Hossain
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 284-7369
F: (212) 549-2654
ebhandari@aclu.org
shossain@aclu.org

Dated: August 3, 2015

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

    - This brief contains 6,992 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) and L.R. 32.1 because:

    - This brief has been prepared in a proportionally-spaced typeface using Microsoft Word, font size 14 Times New Roman for body text, and font size 14 for footnotes.

SO CERTIFIED, this the 3rd day of August, 2015.

*s/ Esha Bhandari*_____
Esha Bhandari

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that this brief of *Amici Curiae* in support of Appellee has been served on all counsel of record by transmission of copies thereof through the Court's CM/ECF system on this 3rd day of August, 2015.

*s/ Esha Bhandari*_____
Esha Bhandari

Counsel for Amici Curiae