

Nos. 13-4625, 13-4626

**In the United States Court of Appeals
for the Fourth Circuit**

In re: GRAND JURY PROCEEDINGS

UNITED STATES OF AMERICA,
Plaintiff - Appellee,

v.

UNDER SEAL,
Party-in-Interest - Appellants.

On Appeal from the United States District Court
for the Eastern District of Virginia

BRIEF OF AMICUS CURIAE EMPEOPLED, LLC
in Support of the Appellants and Reversal of the Judgment Below

Richard M. Martinez
Mahesha P. Subbaraman
ROBINS, KAPLAN,
MILLER & CIRESI, L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
(612) 349-8500
*Counsel for Amicus Curiae
Empeopled, LLC*

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 13-4625 Caption: In re Grand Jury Proceedings / United States v. Under Seal

Pursuant to FRAP 26.1 and Local Rule 26.1,

Empeopled, LLC
(name of party/amicus)

who is Amicus, makes the following disclosure:
(appellant/appellee/amicus)

1. Is party/amicus a publicly held corporation or other publicly held entity? YES NO

2. Does party/amicus have any parent corporations? YES NO
If yes, identify all parent corporations, including grandparent and great-grandparent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? YES NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? YES NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) YES NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? YES NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/ Mahesha Subbaraman

Date: October 24, 2013

Counsel for: Empeopled, LLC

CERTIFICATE OF SERVICE

I certify that on October 24, 2013 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

s/ Mahesha Subbaraman
(signature)

October 24, 2013
(date)

Table of Contents

Table of Authorities	ii
Amicus Identity, Interest, & Authority to File.....	1
Summary of the Argument.....	6
Argument	7
1. Political Privacy Is Vital to Democratic Self-Governance and Thus Protected by the Constitution	7
2. Governmental Intrusions Upon Political Privacy Must Survive the Test of Strict Scrutiny.....	11
3. By Protecting Political Privacy, Online Service Providers Advance Liberty and Self-Governance Worldwide.....	15
4. The Government’s Demand for Lavabit’s Keys Has Chilled the Privacy Efforts of Online Service Providers	21
5. The Government’s Demand for Lavabit’s Keys Thus Deserves – and Cannot Survive – Strict Scrutiny	24
Conclusion.....	33
Certificate of Compliance	34
Certificate of Service	35

Table of Authorities

	<u>Page</u>
Cases	
<i>ACLU v. Reno</i> , 929 F. Supp. 824 (E.D. Pa. 1996) <i>aff'd</i> , 521 U.S 844 (1997).....	3
<i>Bland v. Roberts</i> , No. 12-1671, 2013 U.S. App. LEXIS 19268 (4th Cir. Sept. 18, 2013).....	16, 17, 18
<i>Blumenthal v. Drudge</i> , 992 F. Supp. 44 (D.D.C. 1998).....	15
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	4, 33
<i>Bridges v. City of Bossier</i> , 92 F.3d 329 (5th Cir. 1996).....	25
<i>Burse v. United States</i> , 466 F. 2d 1059, 1088 (9th Cir. 1972).....	31, 32
<i>Casey v. City of Newport</i> , 308 F.3d 106 (1st Cir. 2002)	31
<i>Citizens United v. Fed. Election Comm'n</i> , 130 S. Ct. 876 (2010)	12, 15, 26
<i>Doe v. 2TheMart.com, Inc.</i> , 140 F. Supp. 2d 1088 (W.D. Wash. 2001)	20
<i>Gibson v. Fla. Legislative Investigation Comm.</i> , 372 U.S. 539, 572 (1963)	29, 30

Table of Authorities (cont'd)

	<u>Page</u>
Cases (cont'd)	
<i>Jordan v. Hutcheson</i> , 323 F.2d 597 (4th Cir. 1963).....	7
<i>Kamen v. Kemper Fin. Servs., Inc.</i> , 500 U.S. 90 (1991)	25
<i>Lankford v. Gelston</i> , 364 F.2d 197 (4th Cir. 1966).....	14, 27, 28, 29
<i>Lawrence v. Texas</i> , 539 U.S. 558 (2003)	33
<i>McIntyre v. Ohio Elections Comm'n</i> , 514 U.S. 334 (1995)	7, 9, 10, 12, 13
<i>NAACP v. Alabama</i> , 357 U.S. 449 (1958)	8, 9, 12, 13
<i>Olmstead v. United States</i> , 277 U.S. 438, 485 (1928)	26, 27
<i>Poe v. Ullman</i> , 367 U.S. 497 (1961)	11
<i>Roman Catholic Archdiocese of N.Y. v. Sebelius</i> , 907 F. Supp. 2d 310 (E.D.N.Y. 2012).....	14
<i>Smith v. Ark. State Highway Emps.</i> , 441 U.S. 463 (1979)	7

Table of Authorities (cont'd)

	<u>Page</u>
Cases (cont'd)	
<i>Socialist Workers Party v. Hechler</i> , 890 F.2d 1303 (4th Cir. 1989).....	10, 11, 13
<i>Sweezy v. New Hampshire</i> , 354 U.S. 234, 267 (1957)	7, 11, 30
<i>United States v. Carolene Prods. Co.</i> , 304 U.S. 144 (1938)	11, 12
<i>United States v. Kyllo</i> , 37 F.3d 526 (9th Cir. 1994).....	26
<i>United States v. Stevens</i> , 130 S. Ct. 1577 (2010)	14
<i>United States v. Van Winrow</i> , 951 F.2d 1069 (9th Cir. 1991).....	25
<i>Wis. Action Coalition v. City of Kenosha</i> , 767 F.2d 1248 (7th Cir. 1985).....	31
<i>Zeran v. Am. Online, Inc.</i> , 129 F. 3d 327 (4th Cir. 1997).....	15
Other Authorities	
<i>About empeopled</i> , EMPEOPLED, http://beta.empeopled.com/about	1

Table of Authorities (cont'd)

	<u>Page</u>
Other Authorities (cont'd)	
Amy Davidson, <i>Introducing Strongbox</i> , THE NEW YORKER, May 15, 2013, http://www.newyorker.com/online/blogs/cloread/2013/05/introducing-strongbox-anonymous-document-sharing-tool.html	20
Anjali Mullany, <i>Privacy for the People: Wall Street Protesters Use Social Media App Vibe to Communicate Anonymously</i> , N.Y. DAILY NEWS, Sept. 28, 2011, http://www.nydailynews.com/news/wall-street-protesters-app-communicate-anonymously-article-1.958432	20
Bill Chappell, <i>Citing Privacy Worries, Tech & Legal Site Groklaw Shuts Down</i> , NAT'L PUB. RADIO (NPR) TWO-WAY BLOG (Aug. 20, 2013, 1:16 PM) http://www.npr.org/blogs/thetwo-way/2013/08/20/213828634/citing-privacy-worries-tech-and-legal-site-groklaw-shuts-down	23, 24
Ian Paul, <i>U.S. VPN Provider Shuts Consumer Service In Response to Lavabit Case</i> , PC WORLD, Oct. 22, 2013, http://www.pcworld.com/article/2056554/u-s-vpn-provider-shuts-consumer-service-in-response-to-lavabit-case.html	23
INT'L TELECOMM. UNION, THE WORLD IN 2013: ICT FACTS & FIGURES (2013), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf	15
Jennifer O'Mahony, <i>Turkey Protests: How Activists Stay One Step Ahead with Social Media</i> , TELEGRAPH (U.K.), June 4, 2013, http://www.telegraph.co.uk/technology/internet-security/10098353/Turkey-protests-how-activists-stay-one-step-ahead-with-social-media.html	20

Table of Authorities (cont'd)

	<u>Page</u>
Other Authorities (cont'd)	
Jennifer Preston, <i>Seeking to Disrupt Protesters, Syria Cracks Down on Social Media</i> , N.Y. TIMES, May 22, 2011, http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html	18
Jennifer Preston, <i>YouTube Offers a Way to Blur Faces, Protecting Identities in Videos</i> , N.Y. TIMES MEDIA DECODER BLOG (July 18, 2012, 7:07 PM) http://mediadecoder.blogs.nytimes.com/2012/07/18/youtube-offers-a-way-to-blur-faces-protecting-identities-in-videos/	19
Jon Callas, <i>To Our Customers</i> , SILENT CIRCLE BLOG (Aug. 9, 2013), http://silentcircle.wordpress.com/2013/08/09/to-our-customers/	22
Josh Chin, <i>China Tightens Grip on Social Media</i> , WALL ST. J., Sept. 9, 2013, http://online.wsj.com/news/articles/SB10001424127887324549004579065113098846226	18
Kerry McQueeney, <i>Iran's Government Accused of Controlling Internet Access As It Prepares to Switch Citizens' Networks to 'Improve Security'</i> , U.K. DAILY MAIL ONLINE, Sept. 24, 2012, http://www.dailymail.co.uk/news/article-2207902/Iran-internet-censorship-Government-accused-restricting-citizens-online-access.html	16
Pamela Jones, <i>Forced Exposure</i> , GROKLAW (Aug. 20, 2013, 2:40 AM), http://groklaw.net/article.php?story=20130818120421175	24

Table of Authorities (cont'd)

	<u>Page</u>
Other Authorities (cont'd)	
Press Release, Empeopled, empeopled Launches Social Platform to Bring Better Conversation and Content Curation to the Internet (Oct. 17, 2013), http://prweb.com/releases/2013/10/prweb11244684.htm	1, 2, 3
Ronald D. Rotunda, <i>Original Intent, the View of the Framers, and the Role of the Ratifiers</i> , 41 VAND. L. REV. 507, 509-10 (1988).	7
Ryan Gallagher, <i>The Threat of Silence</i> , SLATE, Feb. 4, 2013, http://www.slate.com/articles/technology/future_tense/2013/02/silent_circle_s_latest_app_democratizes_encryption_governments_won_t_be.html	22
Tanja Aitamurto & Hanna Sistek, <i>How Social Media is Keeping the Egyptian Revolution Alive</i> , PUB. BROAD. SERV. (PBS) MEDIASHIFT BLOG, (Sept. 13, 2011) http://www.pbs.org/mediashift/2011/09/how-social-media-is-keeping-the-egyptian-revolution-alive256/	16
TECHWEEK, http://techweek.com (last visited Oct. 19, 2013).....	2
2013 Nominees, CHICAGO INNOVATION AWARDS, http://chicagoinnovationawards.com/nominations/nominate-now/	2

Amicus Identity, Interest, and Authority to File

1. Identity of Empeopled

Empeopled, LLC (“Amicus”) is an early-stage startup company dedicated to advancing democratic self-governance through social media. Empeopled provides a virtual conversation platform that enables people across the world to discover each other, organize democratically, and then dynamically decide their own future.¹ This platform is now open to the public and may be accessed online at beta.empeopled.com.

Empeopled was founded in 2012 by Aris Michalopoulos and William Howe. A graduate of the University of Chicago, Aris left a successful career in finance to help found Empeopled. The company’s vision is reflected its motto, “Better Conversation for a Better World,”² which ultimately speaks to what the Internet both can and does make possible.

Empeopled launched its online platform in April 2013.³ Since then, more than 1,000 users have joined Empeopled, creating and contributing to

¹ See Press Release, Empeopled, *empeopled Launches Social Platform to Bring Better Conversation and Content Curation to the Internet* (Oct. 17, 2013), <http://prweb.com/releases/2013/10/prweb11244684.htm>.

² *About empeopled*, EMPEOPLED, <http://beta.empeopled.com/about>.

³ See Press Release, *supra* note 1.

dozens of topical communities like “Tech World” and “The Human Rights Society.”⁴ These users participate in these topical communities via written posts and comments.⁵ Users then award points to each other’s written contributions to the extent they enrich the community as a whole. Finally, users employ crowd-voting to decide community rules and elect leaders to enforce these rules.⁶ “This means that the community can administer and govern itself to ensure high-quality, orderly conversation.”⁷

Empeopled thus constitutes “a long-term experiment to see what can be achieved when social media merges with self-governance.”⁸ As such, it was a nominee for a 2013 Chicago Innovation Award and recently was an exhibitor at the 2013 Techweek Chicago Launch Exposition.⁹

2. Interest of Empeopled

Empeopled is interested in this case because of what it means for the future of free expression on the Internet and the kind of democratic

⁴ *See id.*

⁵ *See id.*

⁶ *See id.*

⁷ *See id.*

⁸ *Id.* (quoting Empeopled co-founder Aris Michalopoulos).

⁹ *See 2013 Nominees, CHICAGO INNOVATION AWARDS*, <http://chicagoinnovationawards.com/nominations/nominate-now/> (last visited Oct. 19, 2013); *TECHWEEK*, <http://techweek.com> (last visited Oct. 19, 2013).

initiative and civic participation that Empeopled hopes to foster among its users. As Empeopled co-founder Aris Michalopoulos explains: “I imagine Empeopled one day becoming a platform for charitable causes, grass-roots lobbyist groups and maybe even virtual political parties.”¹⁰

Empeopled’s chances of achieving this goal, however, depend on its ability to innovate and provide its users with new ways to empower both themselves and each other. In this regard, Empeopled believes that just as private membership lists and a secret ballot are vital to civic participation in a democratic society, so too are the privacy-protecting measures that are employed by online service providers worldwide in order to encourage free speech and association among their users on the Internet.

That is why the outcome of this appeal matters to Empeopled. At stake in this appeal are the future of the Internet, and the freedom of online service providers like Empeopled to meet both the privacy and free speech needs of their users worldwide. In this regard, “[a]s the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion.” *ACLU v. Reno*, 929 F. Supp. 824,

¹⁰ Press Release, *supra* note 1 (quoting Aris Michalopoulos).

883 (E.D. Pa. 1996) (Dalzell, J., concurring), *aff'd*, 521 U.S. 844 (1997). And yet, because of the Government's actions in this case, over 400,000 users of Lavabit's e-mail service have lost an important, secure, and fundamentally private means of speaking to each other and the rest of the world.

That loss means a great deal for people worldwide who seek to share their political beliefs and form grassroots organizations but cannot do so—or fear doing so—absent the political privacy that online service providers afford. In turn, online service providers like Empeopled have a significant interest in protecting the political privacy of their users given the kinds of conversations and collaboration that such privacy enables. For this reason, the cost of a ruling against Lavabit in this case would be immeasurable, sending a clear—and chilling—message to online service providers about how much they should value the political privacy of their users.

Empeopled thus respectfully submits this *amicus* brief to assist this Court in its duty “to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.” *Boyd v. United States*, 116 U.S. 616, 635 (1886). In doing so, Empeopled hopes this Court will give serious consideration to what this case means for online service providers and the millions of people they empower across the globe.

3. Authority of Empeopled to File

Empeopled files this *amicus* brief under Fed. R. App. P. 29(a), having received the consent of all the parties in this case. Moreover, per Fed. R. App. P. 29(c)(5), Empeopled states that no party, nor counsel for any party, in this case: (1) wrote this brief in part or in whole; or (2) contributed money meant to fund the preparation or submission of this brief. Only Empeopled, including its members and counsel, has contributed money meant to fund the preparation and submission of this brief.

Summary of the Argument

The Government's seizure of Appellant's private encryption keys is a matter of exceptional importance to online service providers. The chilling effect of this seizure has forced such providers to reexamine their ability and willingness to protect the political privacy of their users—users who depend on this privacy to speak freely, advocate their political beliefs, and organize democratically, all through the Internet.

Accordingly, this Court should apply strict scrutiny in considering whether the Government's demand for Appellant's private encryption keys was proper in this case. Such exacting judicial review is warranted given the fundamental political rights this case implicates, and the chilling effect of the Government's demand. Because of this demand, the privacy of over 400,000 users of Appellant's e-mail service was threatened in an effort by the Government to obtain evidence on just one of these users.

This should lead the Court to find as a matter of strict scrutiny that: (1) the Government's investigative interest was not a compelling basis to seize Appellant's keys; and (2) this seizure was not, in any event, narrowly tailored to meet this investigative interest. The judgments of the court below allowing this seizure should thus be reversed in their entirety.

Argument

1. Political Privacy Is Vital to Democratic Self-Governance and Thus Protected by the Constitution.

“The First Amendment protects the right of an individual to speak freely, to advocate ideas, to associate with others, and to petition his government for redress of grievances.” *Smith v. Ark. State Highway Emps.*, 441 U.S. 463, 464 (1979). But it is “the right of a citizen to political privacy, as protected by the Fourteenth Amendment” that unlocks the door to these First Amendment rights, helping to ensure that everyone gets to participate in deciding our nation’s future – minorities and dissidents included. *Sweezy v. New Hampshire*, 354 U.S. 234, 267 (1957) (Frankfurter, J., concurring); see also *Jordan v. Hutcheson*, 323 F.2d 597, 600 & n.4 (4th Cir. 1963) (quoting this language from Justice Frankfurter’s *Sweezy* concurrence).

The Framers understood this as they drafted the Constitution *in secret* over the summer of 1787,¹¹ and then *privately* collaborated with each other to publish *anonymous* editorials arguing over whether the States should adopt the Constitution. See *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334,

¹¹ See Ronald D. Rotunda, *Original Intent, the View of the Framers, and the Role of the Ratifiers*, 41 VAND. L. REV. 507, 509-10 (1988).

360–67 (1995) (Thomas, J., concurring). And in the 226 years since then, federal courts have defended political privacy from government intrusion, especially in matters of association, speech, and the right to vote.

Free Association. Consider the Supreme Court’s essential defense of political privacy during the midst of the Civil Rights Movement in *NAACP v. Alabama*, 357 U.S. 449 (1958). At issue in *NAACP* was a “judgment of contempt” against the NAACP for refusing “to comply fully with a court order requiring in part the production of membership lists.” *Id.* at 451. Alabama argued it needed the lists to prove that the NAACP’s activities in Alabama violated Alabama’s business registration laws. *See id.* at 464. Alabama further argued that any chilling effect that might result from its obtaining the lists should be disregarded since it “follow[ed] not from state action but from private community pressures.” *Id.* at 463.

A unanimous Supreme Court, however, rejected this view, finding instead that “[i]n the domain of ... indispensable liberties, whether of speech, press, or association ... abridgment of such rights, even though unintended, may inevitably follow from varied forms of governmental action.” *Id.* at 461. The Court consequently refused to let Alabama seize the NAACP’s membership lists given “the vital relationship between freedom

to associate and privacy in one's associations" and "the deterrent effect on the free enjoyment of the right to associate which disclosure of [the NAACP] membership lists is likely to have." *Id.* at 462, 466.

Free Expression. Another key defense of political privacy is present in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). After Margaret McIntyre distributed political leaflets opposing a school levy near a public meeting—leaflets that were not "false, misleading, or libelous"—she was convicted of violating Ohio election law. *See id.* at 337-38. Her crime? Deciding to publish many of the leaflets without putting her name on them. *See id.* at 338. Subsequently, on appeal, Ohio argued that the election law at issue was "a reasonable regulation of the electoral process" that was needed to "prevent[] fraudulent and libelous statements" and "provid[e] the electorate with relevant information." *Id.* at 341, 348.

The Supreme Court took a different view: "Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent." *Id.* at 357. The Court thereby affirmed how political privacy and self-governance work hand in hand: "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights ... to protect unpopular

individuals from retaliation....” *Id.* In turn, the Court observed that while such anonymity may be abused, still, “our society accords greater weight to the value of free speech than to the dangers of its misuse.” *Id.*

Right to Vote. The Supreme Court has described the “secret ballot” as “the hard-won right to vote one’s conscience without fear of retaliation.” *McIntyre*, 514 U.S. at 344. Accordingly, this Court’s decision in *Socialist Workers Party v. Hechler*, 890 F.2d 1303 (4th Cir. 1989) defended both this right and the essential way in which this right connects political privacy with self-governance. At issue in *Hechler* was a constitutional challenge to various West Virginia election laws, including a law that required persons signing minor-party-candidate nomination petitions to also declare their “desire to vote” for the candidate named in the petition. *See id.* at 1304. West Virginia argued this law “protect[ed] the voter ... from inadvertently signing his primary nomination vote away.” *Id.* at 1310.

This Court noted, however, the real effect of this law: to “discourage people from joining unpopular or controversial parties or causes.” *Id.* at 1309. For this reason, this Court emphasized that “the important thing is what the *voter* thinks” – and, from this perspective, the need of every voter to keep his or her vote private was clear. *Id.* at 1310. The law at issue thus

could not pass muster, as it “discourage[d] citizens from participation in the electoral process simply because they do not wish people to know how they will vote.” *Id.* at 1309 (quotation and citation omitted).

Private membership lists. Anonymous political speech. Secret ballots. These are “not a series of isolated points pricked out” by the Constitution. *Poe v. Ullman*, 367 U.S. 497, 543 (1961) (Harlan, J., dissenting). Rather, they are part of “the full scope of ... liberty guaranteed by the Due Process Clause.” *Id.* And for good reason, as “[h]istory has amply proved the virtue of political activity by minority, dissident groups, who innumerable times have been in the vanguard of democratic thought.” *Sweezy*, 354 U.S. at 251. Thus, when government conduct serves to curtail the privacy that makes such “political activity” possible, this conduct demands the toughest form of judicial review available under the Constitution: strict scrutiny.

2. Governmental Intrusions Upon Political Privacy Must Survive the Test of Strict Scrutiny .

Seventy-five years ago, the Supreme Court acknowledged the general need for “more exacting judicial scrutiny” when laws impose “restrictions upon the right to vote ... [or] restraints upon the dissemination of information ... [or] interferences with political organization.” *United States*

v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938). Since then, when state action has intruded in a significant manner on political speech, association, or the right to vote, the legal test for whether such an action can survive constitutional review has almost always been “strict scrutiny.” *See, e.g., Citizens United v. Fed. Election Comm’n*, 130 S. Ct. 876, 898 (2010) (“Laws that burden political speech are ‘subject to strict scrutiny’”).

Under the test of “strict scrutiny,” the Government must prove to the Court that its intrusion “furthers a compelling interest and is narrowly tailored to achieve that interest.” *Id.* Hence, the Supreme Court has applied strict scrutiny not only where state action has directly restricted a core right like free speech (e.g., a total ban on leafleting), but also where state action has invaded a realm of political privacy that is vital to the exercise of a core right (e.g., a ban on publishing anonymous leaflets).

For example, in *NAACP v. Alabama*, the Court relied on the following premise in proceeding to find that Alabama could not demand disclosure of the NAACP’s private membership lists: “[S]tate action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny.” 357 U.S. at 461. Likewise, in *McIntyre v. Ohio*, the Court held that while Margaret McIntyre may not have put her name on some of her

political leaflets, “[w]hen a law burdens core political speech, we apply ‘exacting scrutiny.’” 514 U.S. at 348. Finally, in *Hechler v. Socialist Workers Party*, this Court applied a standard tantamount to strict scrutiny in finding that West Virginia’s stated “interest in making voters disclose their voting preferences is neither legitimate nor strong.” 890 F.3d at 1310.

It did not matter in these cases what form the government intrusion upon political privacy took—be it statute (*McIntyre*, *Hechler*) or court order (*NAACP*). Nor did it matter in *NAACP* that the intrusion was justified on non-political grounds (i.e., to enforce a state business registration law). In each case, strict scrutiny was applied, in large part because of the chilling effect of such intrusions on the future exercise of either political speech, free association, or the right to vote. *See NAACP*, 357 U.S. at 463 (noting the “deterrent effect” of the disclosures at issue); *McIntyre*, 514 U.S. at 357 (emphasizing that the First Amendment exists “to protect unpopular individuals from retaliation”); *Hechler*, 890 F.3d at 1310 (rejecting “desire to vote” disclosure rule for its “chilling effect on the voter”).

Besides concern for a “chilling effect,” two other important reasons counsel application of “strict scrutiny” where government intrusions upon political privacy are at issue. First, intrusions upon a law-abiding citizen’s

privacy generally carry a significant risk of irreparable harm. As this Court noted in regard to a warrantless police raid of multiple private homes during an manhunt that lasted 19 days: “The parties seeking redress have committed no acts warranting violation of the privacy of their homes.... There can be little doubt that actions for money damages would not suffice to repair the injury suffered by the victims of the police searches. [T]he wrongs inflicted are not readily measurable in terms of dollars and cents.” *Lankford v. Gelston*, 364 F.2d 197, 201-02 (4th Cir. 1966).

Second, government intrusions upon political privacy affect liberties that are meant to “protect[] against the Government” – not “leave us at the mercy of *noblesse oblige*.” *United States v. Stevens*, 130 S. Ct. 1577, 1591 (2010). The First Amendment thus “does not require citizens to accept assurances from the government that, if the government later determines it has made a misstep, it will take ameliorative action. To the contrary, the Bill of Rights itself, and the First Amendment in particular, reflect a degree of skepticism towards governmental self-restraint and self-correction.” *Roman Catholic Archdiocese of N.Y. v. Sebelius*, 907 F. Supp. 2d 310, 331 (E.D.N.Y. 2012). And such skepticism is critical when state action intrudes upon the

political privacy—and resulting capacity for self-governance—that online service providers afford to their users across the world.

3. By Protecting Political Privacy, Online Service Providers Advance Liberty and Self-Governance Worldwide.

In 1997, “approximately 40 million people worldwide” were using the Internet. *Zeran v. Am. Online, Inc.*, 129 F. 3d 327, 328 (4th Cir. 1997). Now, in 2013, an estimated 2.7 billion people—or almost 40% of the world’s population—use the Internet.¹² Much of this explosive growth is due to the “new forms, and new forums, for the expression of ideas” that the Internet makes available. *Citizens United*, 130 S. Ct. at 917. Indeed, “users of Internet information are also its producers. ... [E]very person who taps into the Internet is his [or her] own journalist.” *Blumenthal v. Drudge*, 992 F. Supp. 44, 48 n.7 (D.D.C. 1998) (citation and quotation omitted).

This makes the Internet a vital means for enabling political speech, association, and discourse—in short, democratic self-governance. Recent events in Iran help make this clear: “For dissidents opposing the Islamic Republic’s leadership, the [I]nternet has become one of the most powerful

¹² INT’L TELECOMM. UNION, THE WORLD IN 2013: ICT FACTS & FIGURES 1 (2013), <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>.

communication tools at their disposal. Demonstrations have been orchestrated using blogs and social networks to gather support and increase numbers.”¹³ Moreover, “[a]s Iran played down events to outsiders, dissidents used Twitter, Facebook and YouTube to tell the world what was really happening,” including the killing of Iranian student Neda Soltan, “whose murder at the hands of a government militiaman was captured on a camera phone and uploaded to YouTube in [June] 2009.”¹⁴ Recent events in both Syria and Egypt bear out a similar pattern of events.¹⁵

This Court recently encountered this political reality on a smaller scale in *Bland v. Roberts* with respect to campaign speech on Facebook, “an online social network where members develop personalized web profiles

¹³ Kerry McQueeney, *Iran’s Government Accused of Controlling Internet Access As It Prepares to Switch Citizens’ Networks to ‘Improve Security’*, U.K. DAILY MAIL ONLINE, Sept. 24, 2012, <http://www.dailymail.co.uk/news/article-2207902/Iran-internet-censorship-Government-accused-restricting-citizens-online-access.html>.

¹⁴ *Id.*

¹⁵ See *infra* note 18 and accompanying text (describing the political use of social media in Syria); see also Tanja Aitamurto & Hanna Sistek, *How Social Media is Keeping the Egyptian Revolution Alive*, PUB. BROAD. SERV. (PBS) MEDIASHIFT BLOG, (Sept. 13, 2011) <http://www.pbs.org/mediashift/2011/09/how-social-media-is-keeping-the-egyptian-revolution-alive256/> (“As the military has closed Tahrir Square ... smaller protests are happening elsewhere in Cairo. Facebook pages ... with more than 1.6 million followers, are used for spreading the message about protests.....”).

to interact and share information with other members.” No. 12-1671, 2013 U.S. App. LEXIS 19268, at *42 (4th Cir. Sept. 18, 2013). *Bland* concerned claims by six sheriff’s office employees that they were fired in violation of the First Amendment for supporting the sitting sheriff’s electoral opponent. *Id.* at *2. These retaliation claims, in turn, rested on a variety of online speech by these employees that the sheriff allegedly monitored, including the “liking” of a Facebook page—something the district court held was “insufficient speech to merit constitutional protection.” *Id.* at *41.

This Court disagreed: “In sum, liking a political candidate’s campaign [Facebook] page communicates the user’s approval of the candidate and supports the campaign by associating the user with it. In this way, it is the Internet equivalent of displaying a political sign in one’s front yard” *Id.* at *46. The Court thereby recognized the substantive nature of the kind of political speech that takes place on the Internet—particularly as facilitated by online service providers like Facebook. *Id.* at *45 (“In the context of a political campaign’s Facebook page, the meaning that the user approves of the candidacy whose page is being liked is unmistakable.”). The Court further acknowledged the capacity of such speech to support a retaliation claim: in short, such speech generated “a genuine factual issue

concerning whether [the employee's] Facebook support" for the sheriff's opponent was what cost the employee his job. *Id.* at *50-51.

The facts of *Bland* thus reveal not only the vital political speech that takes place on the Internet, but also the frequent need for political privacy when engaging in such speech. And in this regard, the sheriff's alleged conduct in *Bland* is but the tip of the iceberg in terms of the risks that many users face in speaking online. For example, the *New York Times* reports that in Syria—a nation with 580,000 Facebook users—government agents have ordered dissidents to “turn over their Facebook passwords” and have even beaten dissidents for “regime criticisms on their Facebook pages.”¹⁶ In turn, the *Wall Street Journal* reports that Chinese leaders have recently declared that “social-media users who post comments considered to be slanderous could face prison if the posts attract wide attention.”¹⁷

¹⁶ Jennifer Preston, *Seeking to Disrupt Protesters, Syria Cracks Down on Social Media*, N.Y. TIMES, May 22, 2011, <http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html> (further explaining how one Syrian dissident was only able to avoid detention “because he had created multiple Facebook accounts with fake identities”).

¹⁷ Josh Chin, *China Tightens Grip on Social Media*, WALL ST. J., Sept. 9, 2013, <http://online.wsj.com/news/articles/SB10001424127887324549004579065113098846226> (“In recent months, the [Chinese] government has ... detain[ed] dozens for spreading rumors and warn[ed] influential micro-bloggers with large numbers of followers to watch what they say.”).

Given these risks, online service providers are stepping up to find new and better ways to protect their users' political privacy. For instance, as the *New York Times* reported in 2012: "To help protect dissidents using video to tell their stories in countries with repressive government regimes, YouTube [has] made available a new tool ... [that] allow[s] people to obscure faces within videos uploaded onto its platform."¹⁸

The ultimate result of these efforts has been the civic empowerment of millions of people worldwide. The *Telegraph* thus offers the following account of a Turkish citizen under the pseudonym Damla:

[A]n activist in Ankara, [Damla] is constantly refreshing private Facebook groups for updates, posting pictures onto Twitter, and using a popular app for group private messaging to talk to her friends.

She will receive links to maps only visible to fellow activists that show the location of makeshift clinics in houses and even in restaurants' basements, and can watch live streams of protests on the Ustream service if she is at home.

She told the *Telegraph*: "It has had a massive impact, and if it wasn't for social media we wouldn't have the right information on anything. It's been our

¹⁸ Jennifer Preston, *YouTube Offers a Way to Blur Faces, Protecting Identities in Videos*, N.Y. TIMES MEDIA DECODER BLOG (July 18, 2012, 7:07 PM) <http://mediadecoder.blogs.nytimes.com/2012/07/18/youtube-offers-a-way-to-blur-faces-protecting-identities-in-videos/>.

saviour.” Damla said the use of private group messaging meant activists could “react quickly to check whether we’re all safe”¹⁹

This reality also obtains here at home. Indeed, Wall Street protestors are relying on the political privacy afforded by online service providers to organize their protests.²⁰ A major American magazine is now offering “an online place where people can send documents and messages to the magazine, and we ... can offer them a reasonable amount of anonymity.”²¹ And Americans in general are relying on the anonymity afforded to them by their online service providers to speak in a variety of ways.²² The

¹⁹ Jennifer O’Mahony, *Turkey Protests: How Activists Stay One Step Ahead with Social Media*, TELEGRAPH (U.K.), June 4, 2013, <http://www.telegraph.co.uk/technology/internet-security/10098353/Turkey-protests-how-activists-stay-one-step-ahead-with-social-media.html>.

²⁰ See Anjali Mullany, *Privacy for the People: Wall Street Protesters Use Social Media App Vibe to Communicate Anonymously*, N.Y. DAILY NEWS, Sept. 28, 2011, <http://www.nydailynews.com/news/wall-street-protesters-app-communicate-anonymously-article-1.958432>.

²¹ Amy Davidson, *Introducing Strongbox*, THE NEW YORKER, May 15, 2013, <http://www.newyorker.com/online/blogs/cloread/2013/05/introducing-strongbox-anonymous-document-sharing-tool.html>.

²² Based on this reality, one federal court has concluded: “The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights.” *Doe v. 2TheMart.com, Inc.*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

privacy efforts of online service providers are thus enabling more people than ever before to exercise basic political rights without fear. And that progress is precisely what has been endangered by the Government's demand for Lavabit's private encryption keys in this case.

4. The Government's Demand for Lavabit's Keys Has Chilled the Privacy Efforts of Online Service Providers.

On the surface, the facts of the present case appear straightforward: "Lavabit is an e-mail service provider, and this case arises out of a criminal investigation into one of its customers. In the course of that investigation, Lavabit was ordered to disclose the company's private encryption keys, which it refused to do." Appellant's Br. 1. Lavabit's refusal then subjected Lavabit to a contempt order that finally led Lavabit to "provide[] its private keys to the government—but also shut down its service entirely." *Id.* at 10. Over 400,000 Lavabit users thus lost access to a service that gave them "an unparalleled degree of security and privacy," and Lavabit's founder, Ladar Levison, lost "nearly ten years of hard work." *Id.* at 2, 10.

But the effects of the Government's demand for Lavabit's encryption keys were not limited to Lavabit, Mr. Levison, and Lavabit's over 400,000 users. *Id.* at 4. Silent Circle, for example, was also affected. The operator of

a secure, encrypted e-mail service called “Silent Mail,” Silent Circle decided to end this service shortly after Lavabit shut itself down. Silent Circle made this decision for the following reason: “We see the writing the wall, and we have decided that it is best for us to shut down Silent Mail now. We have not received subpoenas, warrants, security letters, or anything else by any government, and this is why we are acting now.”²³

That Silent Circle deemed it necessary to take this action is telling given the important role that Silent Circle has played in to helping to advance the protection of political privacy and free speech worldwide. As *Slate* reports, Silent Circle is responsible for developing privacy tools that enable “human rights reporters in Afghanistan, Jordan, and South Sudan ... to send photos, voice recordings, videos, and PDFs securely. ... [A Silent Circle tool] was [recently] used in South Sudan to transmit a video of brutality that took place at a vehicle checkpoint.”²⁴ In this regard, Silent

²³ Jon Callas, *To Our Customers*, SILENT CIRCLE BLOG (Aug. 9, 2013), <http://silentcircle.wordpress.com/2013/08/09/to-our-customers/>. Also, as Amicus’s filing of this brief indicates, this case has left many online service providers in doubt about what future government restrictions they may eventually face in protecting the privacy of their users.

²⁴ Ryan Gallagher, *The Threat of Silence*, SLATE, Feb. 4, 2013, http://www.slate.com/articles/technology/future_tense/2013/02/silent_circle_s_latest_app_democratizes_encryption_governments_won_t_be.html.

Circle's credo is simply stated by its CEO and ex-Navy SEAL, Mike Janke:

"We feel that every citizen has a right to communicate."²⁵

And on this score, the Government's demand for all of Lavabit's private keys did not just affect online service providers like Silent Circle: it also affected citizens as well, and in much the same way that Silent Circle was affected. As *National Public Radio* reports: "The website Groklaw, which for 10 years demystified complex issues involving technology and the law, is shutting down. Editor Pamela Jones writes that she can't run the site without email, and that since emails' privacy can't be guaranteed, she can no longer do the site's work."²⁶ What drove Jones to these conclusions? Jones herself explains in her final web posting on Groklaw:

The owner of Lavabit tells us that he's stopped using email and if we knew what he knew, we'd

²⁵ *Id.*; see also Ian Paul, *U.S. VPN Provider Shuts Consumer Service In Response to Lavabit Case*, PC WORLD, Oct. 22, 2013, <http://www.pcworld.com/article/2056554/u-s-vpn-provider-shuts-consumer-service-in-response-to-lavabit-case.html> (reporting that the Lavabit case has also led online service provider CryptoSeal to shut down insofar as CryptoSeal afforded its U.S. users with "secure tunnels to the Internet that allow[ed] [these] users to ... maintain at least a modicum of privacy online").

²⁶ Bill Chappell, *Citing Privacy Worries, Tech & Legal Site Groklaw Shuts Down*, NAT'L PUB. RADIO (NPR) TWO-WAY BLOG (Aug. 20, 2013, 1:16 PM) <http://www.npr.org/blogs/thetwo-way/2013/08/20/213828634/citing-privacy-worries-tech-and-legal-site-groklaw-shuts-down>.

stop too. There is no way to do Groklaw without email. Therein lies the conundrum.

* * *

[T]he conclusion I've reached is that there is no way to continue doing Groklaw ... which is incredibly sad. But it's good to be realistic. And the simple truth is, no matter how good the motives might be for collecting and screening everything we say to one another, and no matter how "clean" we all are ourselves from the standpoint of the screeners, I don't know how to function in such an atmosphere. I don't know how to do Groklaw like this.²⁷

Pamela Jones's departure from the online legal world is no small loss: "Last year, the American Bar Association named Groklaw one of the top 100 legal blogs. Its articles and interviews were selected by the Library of Congress to be preserved in its Web Archiving project."²⁸ It also serves to establish—just as Silent Circle's shutdown decision does—the need for "strict scrutiny" of the Government's conduct in this case.

5. The Government's Demand for Lavabit's Keys Thus Deserves – and Cannot Survive – Strict Scrutiny.

At the outset, Amicus acknowledges that the following argument for "strict scrutiny" review of the Government's conduct in this case is not one

²⁷ Pamela Jones, *Forced Exposure*, GROKLAW (Aug. 20, 2013, 2:40 AM), <http://groklaw.net/article.php?story=20130818120421175>.

²⁸ Chappell, *supra* note 25.

that Appellant raises in its opening brief. Instead, Appellant's brief focuses on dismantling the various bases on which the Government has thus far justified its demand for Lavabit's private encryption keys.²⁹

This Court should still consider Amicus's argument for two reasons. **First**, neither the political privacy nor the First Amendment dimensions of this case can be disputed given the effects of the Government's conduct so far on Lavabit's over 400,000 users and the broader online community. *See supra* Part IV. Thus, as the Supreme Court has held, "[w]hen an issue or claim is properly before the court, the court is not limited to the particular legal theories advanced by the parties, but rather retains the independent power to identify and apply the proper law." *Kamen v. Kemper Fin. Servs., Inc.*, 500 U.S. 90, 99 (1991). **Second**, it is always within the Court's power to reach a purely legal argument raised by an amicus in its brief. *See, e.g., Bridges v. City of Bossier*, 92 F.3d 329, 335 n.8 (5th Cir. 1996).³⁰

²⁹ Appellant may still adopt Amicus's argument in its reply brief, which would give this Court further reason to reach Amicus's argument. *See, e.g., United States v. Van Winrow*, 951 F.2d 1069, 1073 (9th Cir. 1991) ("[A]micus ... raises several additional challenges.... Because [Appellant] states in his brief that he wishes to adopt these arguments as his own, and because they present pure issues of law, we will consider them here.").

³⁰ In the event this Court should find that either the factual record or the parties' briefing in this case is not sufficient to address the political

With this in mind, “strict scrutiny” analysis in this case requires one to first consider whether the Government’s demand for Lavabit’s keys was supported by a “compelling interest.” *Citizens United*, 130 S. Ct. at 898. In this regard, it appears the principal reason why the Government wanted Lavabit’s private keys was because it wanted to gather evidence relevant to a criminal investigation. *See* Appellant’s Br. 5. But this interest was limited in scope given that the government’s investigation was confined to just one Lavabit user. *See id.* Indeed, Lavabit was not “a target or a subject of the government’s investigation [and] neither Lavabit nor its owner ... [was] charged with or suspected of any crime.” Appellant’s Br. 1 n.1.

The government’s interest in gathering evidence needed to conduct a full criminal investigation is an important one. It is not, however, an all-purpose justification for every method the government may want to use to get the evidence it needs. As Justice Brandeis has explained: “To declare that in the administration of the criminal law the end justifies the means—

privacy and First Amendment arguments that Amicus raises, then Amicus respectfully suggests the Court should remand to the district court for an evidentiary hearing on this argument and/or seek supplemental briefing from the parties on this argument. *Cf. United States v. Kyllo*, 37 F.3d 526, 530-31 (9th Cir. 1994) (remanding to the district court for an evidentiary hearing on the intrusiveness of a thermal imaging device in order to obtain facts needed to decide the Fourth Amendment status of the device).

to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this Court should resolutely set its face.” *Olmstead v. United States*, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

In *Lankford v. Gelston*, this Court was confronted with the stark need to apply this principle in the face of the Baltimore Police Department’s severe efforts “to capture Samuel and Earl Veney, two brothers who [had] shot and killed one policeman and seriously wounded another.” 364 F. 2d 197, 198 (4th Cir. 1966). In particular, “[d]uring a nineteen-day period in December, 1964, and January, 1965, the police conducted searches of more than 300 houses, most of them private dwellings. The searches were based in almost every instance on unverified anonymous tips. In none did the police have a search warrant.” *Id.* This Court subsequently concluded that “[t]his case reveal[ed] a series of the most flagrant invasions of privacy ever to come under the scrutiny of a federal court.” *Id.* at 201.

In reaching this conclusion, this Court acknowledged the difficult circumstances at hand: “[W]here one policeman is killed and another wounded, the police, and the public, too, are understandably outraged and impatient with any obstacle in the search for the murderer.” *Id.* at 204. At

the same time, this Court recognized that its respect for the “exceedingly difficult task of the policeman” could not be allowed to deter the Court “from protecting rights secured to all by the Constitution.” *Id.* It was thus the Court’s responsibility to vindicate those homeowners whose privacy was invaded by the Baltimore police –homeowners who “committed no acts warranting violation of the privacy of their homes.” *Id.* at 201.

The facts of the present case bear a similarity to the facts of *Lankford*, despite the shift from a real-world location to a virtual one. Indeed, this case concerns the Government’s seizure of “master keys” from Lavabit that would enable the Government to invade and monitor the private e-mail accounts of Lavabit’s over 400,000 customers, and continue to do so in the future had Lavabit not shut down its service. Appellant’s Br. at 4. The Government did not try to get a warrant for each of these accounts—nor does it appear to have established by probable cause that a search reaching all these users’ private communications was justified. *See id.*

Instead, much like the Baltimore Police Department in *Lankford*, the Government decided to pursue a criminal investigation by means of a “wholesale raid[]” –and it thus demanded Lavabit’s private keys to make this raid possible. 364 F.2d at 204. The Government then went one step

further, forbidding “Lavabit from telling anyone that it had compromised [Lavabit’s] security ... not its customers, not its business partners, and not the relevant cryptographic authorities.” Appellant’s Br. 7.

By contrast, the police raids at issue in *Lankford* at least occurred with the knowledge of the people whose homes were searched (*see* 364 F.2d at 199-200), thus enabling these people to seek later redress in this Court. Here, absent Lavabit’s decision to shut down its e-mail service after turning over its keys to the Government, the Government stood poised to execute a virtual raid affecting 400,000 private e-mail accounts, without any of the owners ever knowing this had happened or getting the chance to object in court—users who, as far as the record indicates, have “committed no acts warranting violation of the privacy of their [e-mail].” *Id.* at 201.

Accordingly, the Government’s interest in conducting this raid in the hopes of seizing communications made by a single criminal suspect is not sufficiently compelling to pass strict scrutiny. Nor can it be, when one considers the long-term effect of such government conduct on both the political privacy and First Amendment rights of every American. As Justice Douglas notes: “If the files of the N.A.A.C.P. can be ransacked because some Communists may have joined it, then all walls of privacy are broken

down. By that reasoning the records of the confessional can be ransacked because a ... criminal was implicated." *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 572 (1963) (Douglas, J., concurring).

Yet, even if this Court were to assume as a matter of argument that the Government's investigative interest in this case was compelling enough to support a demand for Lavabit's keys, this demand still cannot pass "strict scrutiny" given its lack of "narrow tailoring." In this regard, the Supreme Court cautions: "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 association, and freedom of communication of ideas...." *Sweezy*, 354 U.S. at 245.

But the Government's demand for Lavabit's keys in this case was anything but "carefully circumscribed." *Id.* To the contrary, this demand ultimately entailed the Government getting the power to "monitor the ... *content* of all communications between Lavabit and all of its customers, or even masquerade as [Lavabit] if it chose to do so." Appellant's Br. 7 (emphasis in original). Put another way, with Lavabit's keys in hand, the

Government became able to monitor every Lavabit user's e-mail without ever again seeking a court order directed at a specific user.

This demand thus lacks the kind of narrow tailoring that strict scrutiny calls for. *See Casey v. City of Newport*, 308 F.3d 106, 114 (1st Cir. 2002) (“[T]he narrow-tailoring test requires ... consider[ation] [of] whether the regulation ... sweeps more broadly than necessary to promote the government's interest.”) This is especially clear when one considers the “compromise” that Lavabit proposed and the Government rejected in this case—a compromise that would have enabled the Government to obtain the information it wanted while also protecting the privacy of every other Lavabit user. *See Appellant's Br. 8-9; see also Wis. Action Coalition v. City of Kenosha*, 767 F.2d 1248, 1255 (7th Cir. 1985) (“Obviously, if there exists a less restrictive method of furthering the legitimate governmental interest, the regulation in question is not as precise as it could be.”).

Of course, the Government may argue that without Lavabit's keys, it potentially stood to lose “some evidence substantially connected to the compelling objects of [its] investigation.” *Burse v. United States*, 466 F. 2d 1059, 1088 (9th Cir. 1972), *modified*, 863 F.2d 667 (9th Cir. 1988). But this cannot overcome the reality that with these keys, the Government almost

certainly gained “a quantity of information that was none of ... [its] business.” *Id.* Nor can this overcome the chilling effect that this intrusion has exerted on online service providers and users alike. *See supra* Part IV. This case thus underscores why “[w]hen First Amendment interests are at stake, the Government must use a scalpel, not an ax.” *Id.*

Conclusion

History teaches us that “unconstitutional practices get their first footing ... by silent approaches and slight deviations from legal modes of procedure.” *Boyd*, 116 U.S. at 635. But so long “[a]s the Constitution endures, persons in every generation can invoke its principles in their own search for greater freedom.” *Lawrence v. Texas*, 539 U.S. 558, 579 (2003). Appellant stands before this Court seeking such freedom. Amicus now joins that cause. This Court should reverse the judgments below, and thus vindicate the efforts of online service providers to protect the political privacy and the First Amendment rights of their users.

Respectfully submitted,

Dated: October 24, 2013

s/ Mahesha P. Subbaraman

Richard M. Martinez
Mahesha P. Subbaraman
ROBINS, KAPLAN, MILLER &
CIRESI, L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
(612) 349-8500

Counsel for *Amicus Curiae*
Empeopled, LLC

Certificate of Compliance

Pursuant to Fed. R. App. P. 32(a)(7)(C), the undersigned certifies that this *amicus curiae* brief complies with all of the applicable type-volume limitations of Fed. R. App. P. 32(a)(7)(B) and the applicable typeface and type-style requirements of Fed. R. App. P. 32(a)(5) and (6). This brief was prepared using a proportionally spaced font (Book Antiqua). Exclusive of portions exempted by Fed. R. App. P. 32(a)(7)(B)(III), this brief contains 6,793 words, according to the word-count function of the word processor (Microsoft Word 2010) that was used to prepare this brief.

Dated: October 24, 2013

s/ Mahesha P. Subbaraman

Richard M. Martinez
Mahesha P. Subbaraman
ROBINS, KAPLAN, MILLER &
CIRESI, L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
(612) 349-8500

Counsel for *Amicus Curiae*
Empeopled, LLC

Certificate of Service

I hereby certify that on October 24, 2013, I electronically filed the foregoing document with the United States Court of Appeals for the Fourth Circuit by using the CM/ECF system. I certify that the following parties or their counsel of record are registered as ECF Filers and that they will be served by the CM/ECF system:

Jesse Ryan Binnall
Marcia C. Hofmann
Laurin Howard Mills
Ian James Samuel
David Alan Warrington

James L. Trump
Michael Phillip Ben'Ary

Dated: October 24, 2013

s/ Mahesha P. Subbaraman

Richard M. Martinez
Mahesha Subbaraman
ROBINS, KAPLAN, MILLER &
CIRESI, L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402-2015
(612) 349-8500

Counsel for *Amicus Curiae*
Empeopled, LLC