

EXHIBIT A

IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION – FELONY BRANCH

In the Matter of the Search of
www.disruptj20.org that Is Stored at
Premises Owned, Maintained, Controlled,
or Operated by DreamHost

Case No. 2017 CF2 001147
Special Proceeding No. 17 CSW 3438
Chief Judge Robert E. Morin
Next court date: August 24, 2017
Event: Hearing on Motion to Compel

MEMORANDUM OF THE AVAAZ FOUNDATION AS *AMICUS CURIAE*

The Avaaz Foundation hereby respectfully submits this Memorandum as *Amicus Curiae*
as Exhibit A to its Motion for Leave to File a Memorandum as *Amicus Curiae*.

Respectfully submitted,

/s/Ashley I. Kissinger

Ashley I. Kissinger (D.C. Bar No. 463421)
LEVINE SULLIVAN KOCH & SCHULZ, LLP
1888 Sherman Street, Suite 370
Denver, Colorado 80203
Phone: 303-376-2407
Fax: 303-376-2401
akissinger@lskslaw.com

August 22, 2017

Counsel to The Avaaz Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTEREST OF THE <i>AMICUS</i>	1
INTRODUCTION	1
ARGUMENT	3
I. The Search Warrant poses a grave threat to the First Amendment rights of free speech and association.	3
II. Deprivation of these rights as held by visitors to a website risks particularly harmful consequences to citizens of foreign countries and United States citizens living or traveling abroad.	9
III. It is appropriate for American courts to consider the international consequences of their decision making.	14
CONCLUSION	17

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Abrams v. United States</i> , 250 U.S. 616, 630 (1919)	3
<i>Ashcroft v. Free Speech Coalition</i> , 535 U.S. 234 (2002)	3
<i>Barclays Bank PLC v. Franchise Tax Board of California</i> , 512 U.S. 298 (1994)	16
<i>Brown v. Board of Education</i> , 347 U.S. 483 (1954)	16
<i>Buckley v. American Constitutional Law Foundation, Inc.</i> , 525 U.S. 182 (1999)	5
<i>Buckley v. Valeo</i> , 424 U.S. 1, 15 (1976)	6
<i>Chisholm v. Georgia</i> , 2 U.S. 419 (1793)	14
<i>Consolidated Edison Co. of New York v. Public Service Commission of New York</i> , 447 U.S. 530 (1980)	3
<i>Denver Area Educational Telecommunications Consortium, Inc. v. FCC</i> , 518 U.S. 727 (1996)	7
<i>Doe v. Cahill</i> , 884 A.2d 451 (Del. 2005)	5
<i>Garrison v. State of Louisiana</i> , 379 U.S. 64 (1964)	4
<i>Greenbaum v. Google, Inc.</i> , 845 N.Y.S.2d 695 (N.Y. Sup. Ct. 2007)	5
<i>Lamont v. Postmaster General</i> , 381 U.S. 301 (1965)	7

<i>McIntyre v. Ohio Elections Commission</i> , 514 U.S. 334 (1995)	5
<i>Medellin v. Texas</i> , 552 U.S. 491 (2008)	15, 16
<i>National Association for Advancement of Colored People v. State of Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958)	6, 7
<i>National Socialist Party of America v. Village of Skokie</i> , 432 U.S. 43 (1977)	4
<i>New York Times Co. v. Sullivan</i> , 376 U.S. 254 (1964)	4
<i>Reno v. American Civil Liberties Union</i> , 521 U.S. 844 (1997)	5
<i>Respublica v. De Longchamps</i> , 1 U.S. 111 (Ct. of Oyer & Terminer 1784)	15
<i>Rosenblatt v. Baer</i> , 383 U.S. 75 (1966)	4
<i>Sosa v. Alvarez-Machain</i> , 542 U.S. 692 (2004)	16
<i>Stanley v. Georgia</i> , 394 U.S. 557 (1969)	6
<i>Talley v. California</i> , 362 U.S. 60 (1960)	5
<i>United States v. Rumely</i> , 345 U.S. 41 (1953)	6
<i>Wang Xiaoning v. Yahoo! Inc.</i> , No. 4:07-CV-02151-CW (N.D. Cal. July 30, 2007)	11
<i>Ware v. Hylton</i> , 3 U.S. 199 (1796)	15
<i>Whitney v. California</i> , 274 U.S. 357 (1927)	3

<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978)	3
Other Authorities	
Agence France Presse, <i>Lebanon Man Sentenced for Insulting President on Twitter</i> , Yahoo! News (Feb. 12, 2014)	4
About Us, Avaaz, https://www.avaaz.org/page/en/about/	1
Anthony Bartkewicz, <i>Dutch Twitter User Gets 6-Month Suspended Sentence for Insulting Queen Beatrix on Twitter</i> , N.Y. Daily News (Aug. 28, 2012)	4
Brief of the United States as Amicus Curiae, <i>Brown v. Bd. of Educ.</i> , 347 U.S. 483, 1952 WL 82045 (1954)	17
Brief of the United States as Amicus Curiae Supporting Petitioner, <i>Medellin v. Texas</i> , 552 U.S. 491, 2007 WL 1909462 (2008)	17
Anne-Marie Burley, <i>The Alien Tort Statute and the Judiciary Act of 1789: A Badge of Honor</i> , 83 Am. J. Int'l L. 461, 487 (1989)	15
Ashley Cleek, <i>Russia: Anti-Corruption Donor Details Leaked</i> , Global Voices (May 4, 2011)	10
European Commission, <i>Questions and Answers on the EU-U.S. Data Protection 'Umbrella Agreement'</i> (Dec. 1, 2016)	14
Future Tense, <i>Netizen Report: Tech Community Mourns Open-Source Activist Executed by Syrian Regime</i> , Slate (Aug. 3, 2017)	12
Sami Ben Gharbia, <i>Moldavia: Sequestration of Personal Computers of 12 Young People for Posting Critical Comments Online</i> , Advox (June 13, 2008)	12
Joseph Kahn, <i>Yahoo Helped Chinese To Prosecute Journalist</i> , N.Y. Times (Sept. 8, 2005)	11
Maria Kravchenko, <i>Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2016</i> , Sovia Ctr. for Info. & Analysis (Apr. 21, 2017)	10, 11
Rebecca MacKinnon, <i>Consent of the Networked: The Worldwide Struggle for Internet Freedom</i> at 69-70 (Basic Books 2012)	10
Message to the Congress, Feb. 2, 1948, H. Doc. No. 516, 80th Cong., 2d sess.	17

Office of the United Nations High Commissioner for Human Rights, <i>The Right to Privacy in the Digital Age</i> ¶ 34 (June 30, 2014)	14
PEN America, <i>Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor</i> (Nov. 12, 2013)	8
Jonathon W. Penney, <i>Chilling Effects: Online Surveillance & Wikipedia Use</i> , 31 Berkeley Tech. L.J. 117, 168 (2016)	8
Andrea Peterson, <i>How a Failed Supreme Court Bid Is Still Causing Headaches for Hulu and Netflix</i> , Washington Post (Dec. 27, 2013)	8
Pingdom, <i>The U.S. Hosts 43% of the World’s Top 1 Million Websites</i> , Pingdom Blog (July 2, 2012)	9
Katia Rodriguez, <i>Surveillance Camp II: Privatized State Surveillance</i> , Advox (Feb. 6, 2013),	12
Juliana Ruhfus, <i>Syria’s Electronic Armies</i> , Al Jazeera English (June 18, 2015)	12
Mark Rumold, <i>In J20 Investigation, DOJ Overreaches Again. And Gets Taken To Court Again</i> , Electronic Frontier Foundation (Aug. 14, 2017)	13
William Saletan, <i>Springtime for Twitter: Is the Internet Driving the Revolutions of the Arab Spring?</i> , Slate (July 18, 2011)	11
Feliz Solomon, <i>Thailand Has Sentenced a Man to 35 Years in Prison for Facebook Posts that ‘Insult the Monarchy,’</i> Time (June 9, 2007)	4
Riley Walters, <i>Continued Federal Cyber Breaches in 2015</i> , Heritage Foundation (Nov. 19, 2015)	13
S. Rep. No. 100–599, at *7 (1988)	8, 9
U.S. Const. amend. XI	15
Ken White, <i>Department of Justice Uses Search Warrant To Get Data on Visitors to Anti-Trump Site</i> , Popehat (Aug. 14, 2017)	13

INTEREST OF THE *AMICUS*

The Avaaz Foundation is a non-governmental organization with nearly 45 million members from literally every country in the world. Founded in 2007, the mission of Avaaz –meaning “voice” in several European, Middle Eastern and Asian languages – is simple: “[O]rganize citizens of all nations to close the gap between the world we have and the world most people everywhere want.” *About Us*, Avaaz, <https://www.avaaz.org/page/en/about/>. To achieve this mission, Avaaz has a broad reach around the world, operating on five continents, in 17 languages, and through the work of over 100 employees and thousands of volunteers. *See, e.g., id.*

Avaaz works toward its objectives by promoting public awareness and taking action on key social, political and economic decisions, including those affecting personal privacy, freedom of expression, and freedom of association around the world. It provides members the opportunity to take action on issues they feel strongly about by signing petitions, funding campaigns and humanitarian efforts, and participating offline protests and events. Technology allows it to reach and involve members of the public wherever their physical location or country of residence and enables Avaaz to support causes all over the world. As a result, Avaaz enjoys a worldwide membership and is representative of civil societies around the globe. *Id.*

INTRODUCTION

The Government seeks a decision from this Court that will have a detrimental impact on associational, privacy and speech rights of individuals not only within the United States but around the globe. According to DreamHost, the Search Warrant seeks information that could be used to identify the persons connected with the 1.3 million IP addresses used to visit a political

advocacy website, www.disruptJ20.org, and reveal what, specifically, they were reading on that website.¹ Although the website is hosted on a United States company's servers, those 1.3 million website visits may have been made from anywhere in the world, including countries with repressive regimes that punish citizens and others found there for speech and political associations those regimes find unsavory.

It is no exaggeration to say that many persons who visited this website, which was specifically designed to facilitate the protest and disruption of President Donald Trump's inauguration, would feel unsettled at best, and personally vulnerable at worst, by the effective release of their names, and the details of what website content they were viewing, to this Administration's Department of Justice. But of even greater concern is the lasting damage that an order by this Court commanding the release of such personal information to our nation's highest law enforcement agency would do. It would no doubt chill people around the globe from visiting such websites in the future for fear that they, too, might be outed. And the fact that such a chill resulted from an order from a judicial system known worldwide as a stalwart guardian of civil and political rights, would only enhance the negative effect. If United States courts with jurisdiction over what information a U.S.-based website must disclose are unable or unwilling to protect the right of persons to freely access information on the internet, associate with political organizations, and exercise their speech rights without fear of government harassment and repression, who can?

¹ Avaaz understands that the Government has now filed a Reply Brief and request to amend the Search Warrant that purportedly narrows the information sought. According to DreamHost, however, that submission does not sufficiently address the constitutional and other concerns raised in this brief.

ARGUMENT

I. The Search Warrant poses a grave threat to the First Amendment rights of free speech and association.

By its Search Warrant, the Government seeks to invade the right of internet users to privately view websites and to speak anonymously. As DreamHost has pointed out, because these are core constitutional rights in the United States, the Court is obliged to scrutinize the Search Warrant with “particular exactitude” to ensure that these rights are adequately protected. *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978); see Non-Party Dreamhost, LLC’s Resp. in Opp’n to U.S.’s Mot. for DreamHost to Show Cause at 7-10, Aug. 11, 2017. Here, the application of this “particular exactitude” requirement is not onerous; the Search Warrant is plainly overbroad on its face. By seeking to unmask every person connected to 1.3 million IP addresses, as well as to learn what they were viewing on the web, the Government has vastly overstepped its legitimate law enforcement authority.

As the United States Supreme Court has repeatedly recognized, “[t]he right to think is the beginning of freedom, and speech must be protected from the government, because speech is the beginning of thought.” *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 253 (2002). The American system recognizes that free expression is indispensable to “the discovery and spread of political truth” *Whitney v. California*, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring), *overruled on other grounds by Brandenburg v. Ohio*, 395 U.S. 444 (1969); see also *Consol. Edison Co. of New York v. Pub. Serv. Comm’n of New York*, 447 U.S. 530, 534 (1980) (“‘the best test of truth is the power of the thought to get itself accepted in the competition of the market’” (quoting *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting))). For this reason, as the world observed with the recent white nationalist demonstrations in Charlottesville, there is

tolerance in the United States for the expression of even the most repugnant and controversial ideas. *See, e.g., Nat'l Socialist Party of Am. v. Vill. of Skokie*, 432 U.S. 43, 43-44 (1977) (First Amendment applied to review of state court injunction prohibiting Nazi Party from displaying swastika and distributing anti-Semitic literature in public parade). There is also protection for scathing criticism of government officials, including the United States President – a basic right that United States citizens often take for granted but is not uniformly recognized around the world. *See, e.g., Feliz Solomon, Thailand Has Sentenced a Man to 35 Years in Prison for Facebook Posts that 'Insult the Monarchy,'* Time (June 9, 2007), <http://time.com/4812376/thailand-lese-majeste-facebook-royal-defamation/>; Agence France Presse, *Lebanon Man Sentenced for Insulting President on Twitter*, Yahoo! News (Feb. 12, 2014), <https://uk.news.yahoo.com/lebanon-man-sentenced-insulting-president-twitter-201032957.html#SOMpgkb>; Anthony Bartkewicz, *Dutch Twitter User Gets 6-Month Suspended Sentence for Insulting Queen Beatrix on Twitter*, N.Y. Daily News (Aug. 28, 2012), <http://www.nydailynews.com/news/world/dutch-twitter-user-6-month-suspended-sentence-insulting-queen-beatrix-twitter-article-1.1146214#ixzz2vBZ5PBI4>. Indeed, where, as appears to be the case here, the speech at issue is made in connection with the inauguration of the United States President after a hotly contested campaign, the First Amendment interests of the speakers are at their pinnacle. *See, e.g., Garrison v. State of La.*, 379 U.S. 64, 75 (1964) (“The First and Fourteenth Amendments embody our ‘profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public

officials.” (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)); *Rosenblatt v. Baer*, 383 U.S. 75, 85 (1966) (“Criticism of government is at the very center of the constitutionally protected area of free discussion. Criticism of those responsible for government operations must be free, lest criticism of government itself be penalized.”).

The right to engage in expressive activities *anonymously* is critical to the adequate protection of these underlying speech rights, and that right is equally well settled. *See Buckley v. Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 200 (1999); *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 347, 357 (1995); *Talley v. California*, 362 U.S. 60, 64-66 (1960). Anonymous speech has played a crucial role in American public life, and it is particularly deserving of protection given the severe consequences that can befall the speaker if the shield of anonymity is removed:

Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society.

McIntyre, 514 U.S. at 357 (citation omitted); *see also id.* at 341-43 (discussing history and importance of anonymous expressive activity). Thus, while acknowledging that “[t]he right to remain anonymous may be abused when it shields fraudulent conduct,” the Supreme Court has emphasized that “political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.” *Id.* at 357.²

² It goes without saying that the First Amendment’s protection for anonymous speech applies to all speakers, whether they convey their message by handing out a paper pamphlet or by

There are two corollary rights protected by the Constitution that are at stake in this proceeding as well. One is the right to associate with others privately. *See Buckley v. Valeo*, 424 U.S. 1, 15 (1976) (the First Amendment “protects political association as well as political expression.”). Sixty years ago, when Alabama demanded to see the NAACP’s membership lists, the Supreme Court explained the importance of associational freedom:

Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the ‘liberty’ assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech. Of course, it is immaterial whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters, and state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny.

Nat’l Ass’n for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449, 460-61 (1958) (citations omitted). The Court refused to compel production of the membership lists, holding that to do so would infringe the constitutional “right of the members to pursue their lawful private interests privately and to associate freely with others in so doing” *Id.* at 466.

The other is the right to read information free from the surveillance of government. “If the First Amendment means anything, it means that a state has no business telling a man . . . what books he may read or what films he may watch.” *Stanley v. Georgia*, 394 U.S. 557, 565

communicating via the internet. *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997) (there is “no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet].”); *Greenbaum v. Google, Inc.*, 845 N.Y.S.2d 695, 698 (N.Y. Sup. Ct. 2007) (“Courts . . . have repeatedly recognized that the First Amendment protects the right to participate in online forums anonymously or under a pseudonym, and that anonymous speech can foster the free and diverse exchange of ideas.”); *Doe v. Cahill*, 884 A.2d 451, 456 (Del. 2005) (confirming that First Amendment protection “extends to anonymous internet speech” and recognizing that such speech “in some instances can become the modern equivalent of political pamphleteering.”).

(1969). As Justice Douglas poignantly explained, “[i]f the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land.” *United States v. Rumely*, 345 U.S. 41, 58 (1953) (Douglas, J., concurring).

When the Government interferes with these rights by seeking the names of persons who were previously anonymous, the chilling effects can be severe. In *Patterson*, the Supreme Court noted that the disclosure of NAACP members’ identities “is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.” 357 U.S. at 462-63; *see id.* at 462 (“Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.”). The Court has reached the same conclusion in other circumstances. For example, in *Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965), the Supreme Court struck down a requirement that mail recipients file a written request with the post office to receive communist literature because such a requirement “is almost certain” to deter “uninhibited, robust, and wide-open debate and discussion.” *Id.* at 307 (people “might think they would invite disaster if they read what the Federal Government says contains the seeds of treason.”). Similarly, in *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996), the Court concluded that a requirement that viewers affirmatively request certain “sex-related” cable programming would “further restrict viewing by subscribers who fear for their reputations

should the [cable] operator, advertently or inadvertently, disclose the list of those who wish to watch the ‘patently offensive’ channel.” *Id.* at 754. This same chilling effect carries over to the internet. In a 2013 survey, PEN America found that 16% of writers surveyed “have refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious” due to fears of surveillance by the Government and “another 12% have seriously considered it.” PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013),

https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; see also Jonathon W. Penney, *Chilling Effects: Online Surveillance & Wikipedia Use*, 31 Berkeley Tech. L.J. 117, 168 (2016) (finding that revelations about government surveillance in 2013 “had a salient and observable chilling effect on Wikipedia users accessing certain Wikipedia articles”).

It is worth noting that the courts are not the only American institution that has recognized and protected the right to read, speak, and affiliate with others anonymously. For example, in the late 1980s Congress enacted the Video Privacy Protection Act in response to a “gleefully irreverent” article that a reporter penned upon obtaining the video rental history of then-United States Supreme Court nominee Judge Robert Bork. See, e.g., Andrea Peterson, *How a Failed Supreme Court Bid Is Still Causing Headaches for Hulu and Netflix*, Washington Post (Dec. 27, 2013),

<https://www.washingtonpost.com/news/the-switch/wp/2013/12/27/how-a-failed-supreme-court-bid-is-still-causing-headaches-for-hulu-and-netflix>. In supporting the passage of the Act, which generally prohibits the disclosure of personally identifiable video rental records, Senator Patrick

Leahy warned of “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems” which he described as “a new, more subtle and pervasive form of surveillance.” S. Rep. No. 100–599, at *7 (1988) (Sen. Leahy). He presciently observed that “[t]hese ‘information pools’ create privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard.” *Id.*³

In the nearly twenty years since Senator Leahy spoke, the “information pools” he referred to have grown almost unfathomably in width, encompassing data on more and more people, and depth, combining information from an ever-growing collection of sources. And with that growth has come a corresponding threat of chilling effects on speech and freedom of association. Given the number and strength of the First Amendment interests at stake here, the Court should require the Government to hurdle an extraordinarily high bar to demonstrate that the Search Warrant is a legitimate exercise of law enforcement authority. The fact that the Government is apparently unwilling to even discuss the scope of the Search Warrant with DreamHost, or to explain in its briefing why it needs a vast trove of personal information about people connected to 1.3 million website visits in connection with a law enforcement investigation stemming from the arrest of 200 people accused of relatively minor crimes, should give this Court great pause.

II. Deprivation of these rights as held by visitors to a website risks particularly harmful consequences to citizens of foreign countries and United States citizens living or traveling abroad.

³ See also *id.* at 5–6 (“In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.”).

As of five years ago, fully forty-three percent (43%) of the world's top 1 million websites are, like www.disruptJ20.org, hosted in the United States. *See* Pingdom, *The U.S. Hosts 43% of the World's Top 1 Million Websites*, Pingdom Blog (July 2, 2012), <http://royal.pingdom.com/2012/07/02/united-states-hosts-43-percent-worlds-top-1-million-websites/>. A large number of legal requests for personally identifying information about website visitors are therefore made, and challenged, in the United States. Yet the visitors to those websites live in every country of the world. Many of those persons are, as a practical and financial matter, unable to challenge those requests. How American courts adjudicate such requests therefore has a direct global impact on whether the fundamental privacy, speech and associational rights they implicate are enjoyed by others around the world.

Allowing the Government to obtain the information it seeks in this case would have potentially serious consequences on the freedoms of American expatriates and citizens of foreign countries. Repressive regimes have frequently used IP addresses and other personally identifiable information to crack down on dissent within their countries. For example, in May 2010, donors to an anticorruption whistle-blowing website in Russia, Rospil.info, began receiving harassing phone calls. *See* Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* at 69-70 (Basic Books 2012); *accord* Ashley Cleek, *Russia: Anti-Corruption Donor Details Leaked*, Global Voices (May 4, 2011), <https://globalvoices.org/2011/05/04/russia-anti-corruption-donor-details-leaked/>. The donors had all made their contributions through Yanex.money, a payment system run by a Russian internet services company, and the company had been forced to turn over its “financial and personal records” about those donors to the Federal Security Service of the Russian Federation

(the “FSB”). MacKinnon, *supra*, at 69-70. The activists “concluded that the FSB had shared the Yandex.money account information with [members of a pro-Kremlin youth movement], although the group officially denied the allegations. The message to potential supporters of opposition groups is nonetheless clear: Watch out, or you never know who might gain access to your financial transaction records; and who knows what those angry young patriots might do if they decide to take matters into their own hands.” *Id.* at 71; *see also* Maria Kravchenko, *Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2016*, Sova Ctr. for Info. & Analysis (Apr. 21, 2017), <http://www.sova-center.ru/en/misuse/reports-analyses/2017/04/d36857/> (providing additional examples of Russian government unmasking and prosecution of online users).

Indeed, the revelation of the kind of information sought here can have serious physical consequences to the persons unmasked. In 2007, several Chinese activists sued Yahoo alleging that it had “willingly provided Chinese officials with access to private e-mail records, copies of email messages, e-mail addresses, user ID numbers, and other identifying information about the [p]laintiffs and the nature and content of their . . . electronic communications,” which, the plaintiffs claimed, aided and abetted the commission of torture and other abuses against them in China. Am. Compl. ¶ 2, *Wang Xiaoning v. Yahoo! Inc.*, No. 4:07-CV-02151-CW (N.D. Cal. July 30, 2007), Dkt. No. 51;⁴ *see also* Joseph Kahn, *Yahoo Helped Chinese To Prosecute Journalist*, N.Y. Times (Sept. 8, 2005), <http://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html?mcubz=0> (describing incident where Yahoo! provided information to Chinese

⁴ Yahoo ultimately settled the case for an undisclosed amount.

government about anonymous posting concerning “communication from Communist Party authorities to media outlets around the country”).

More broadly, countries with aggressive police states have discovered that “[i]t’s often easier to track people online, where their channels of communication are limited and inherently recordable.” William Saletan, *Springtime for Twitter: Is the Internet Driving the Revolutions of the Arab Spring?*, Slate (July 18, 2011),

http://www.slate.com/articles/technology/future_tense/2011/07/springtime_for_twitter.html. For example, in Syria, the government used IP addresses to discover “the secret offices where opposition groups gathered,” leading to raids and arrests. See Juliana Ruhfus, *Syria’s Electronic Armies*, Al Jazeera English (June 18, 2015), <http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html>. Similarly, in Chile, police attempted to obtain “data related to pseudonymous user accounts, such as IP addresses, records of previous connections, real names, and physical addresses” from a website that coordinates union activities, in order to investigate users who had commented about an ongoing strike. See Katitza Rodriguez, *Surveillance Camp II: Privatized State Surveillance*, Advox (Feb. 6, 2013), <https://advox.globalvoices.org/2013/02/06/surveillance-camp-ii-privatized-state-surveillance/>. The website in that instance was able to resist the request, but that is often not the case, whether for practical or legal reasons. For example, in the Republic of Moldova, twelve activists who had “expressed critical opinions against the ruling communist party” had their computers seized, after, it was believed, a Moldovan IT company gave the police their IP addresses. See Sami Ben Gharbia, *Moldavia:*

Sequestration of Personal Computers of 12 Young People for Posting Critical Comments Online, Advox (June 13, 2008),

<https://advox.globalvoices.org/2008/06/13/moldavia-destruction-of-personal-computers/>. These foreign efforts to monitor speech online continue today. See Future Tense, *Netizen Report: Tech Community Mourns Open-Source Activist Executed by Syrian Regime*, Slate (Aug. 3, 2017),

http://www.slate.com/blogs/future_tense/2017/08/03/

[netizen_report_tech_community_mourns_open_source_activist_executed_by_syrian.html](http://www.slate.com/blogs/future_tense/2017/08/03/netizen_report_tech_community_mourns_open_source_activist_executed_by_syrian.html)

(discussing amendments to Tajikistan’s criminal law that grant security services the right to monitor “anyone who visits websites deemed ‘undesirable’”).

The fact that any information provided in response to the Search Warrant will be revealed to the United States government, and not one of the repressive regimes discussed above, provides no guarantee it will not end up in foreign hands. The federal government experienced at least fifteen cyber security breaches in 2015, including the Department of State’s email system and the personnel records of millions of government employees. See Riley Walters, *Continued Federal Cyber Breaches in 2015*, Heritage Foundation (Nov. 19, 2015), <http://www.heritage.org/cybersecurity/report/continued-federal-cyber-breaches-2015>. It is also conceivable that the Government might share some of the information voluntarily with other law enforcement agencies abroad. In either case, the public, including those persons whose information would be disclosed, may never find out about this release.

Moreover, regardless of the Government’s actual motives in this case, it appears to the world at large that it is using an incredibly broad dragnet to obtain IP addresses of its potential

political opponents. See Mark Rumold, *In J20 Investigation, DOJ Overreaches Again. And Gets Taken To Court Again*, Electronic Frontier Foundation (Aug. 14, 2017),

[https://www.eff.org/deeplinks/](https://www.eff.org/deeplinks/2017/08/j20-investigation-doj-overreaches-again-and-gets-taken-court-again)

[2017/08/j20-investigation-doj-overreaches-again-and-gets-taken-court-again](https://www.eff.org/deeplinks/2017/08/j20-investigation-doj-overreaches-again-and-gets-taken-court-again); Ken White,

Department of Justice Uses Search Warrant To Get Data on Visitors to Anti-Trump Site, Popehat (Aug. 14, 2017),

<https://www.popehat.com/2017/08/14/department-of-justice-uses-search-warrant-to-get-data-on-visitors-to-anti-trump-site/>. Given the protections for privacy, speech and associational rights

enshrined in American law, and the fact that the United States prides itself on *not* being a repressive government, a court order enforcing this Search Warrant will have a palpable chilling effect around the world. The United States weakens its moral authority to speak out on these fundamental human rights issues when it does not stand up for those rights within its own borders. While the executive branch is apparently oblivious to this fact in this case, as set forth in Part III below, this Court need not be.

III. It is appropriate for American courts to consider the international consequences of their decision making.

This Court can and should consider the international consequences of its decision in this proceeding. The growing consensus in international human rights law is that the right to privacy applies extraterritorially. “If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country,” as the Department of Justice is seeking to do here, “then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond.” See Office

of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* ¶ 34 (June 30, 2014),

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (describing obligations under the International Covenant on Civil and Political Rights, which has 169 parties including the United States). This is also consistent with the principles of the recent EU-U.S. Data Protection “Umbrella Agreement” made last year, which provides protection to EU citizens’ data that is transferred to United States law enforcement authorities. See European Commission, *Questions and Answers on the EU-U.S. Data Protection ‘Umbrella Agreement’* (Dec. 1, 2016), http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm.

The Supreme Court has, in fact, repeatedly considered the consequences to foreign citizens, American citizens abroad, and the United States’ place in the world in its decisionmaking. The justices have been mindful of these concerns since the Court’s earliest days. See, e.g., *Chisholm v. Georgia*, 2 U.S. 419, 474 (1793) (opinion of Jay, C.J.) (“the United States had, by taking a place among the nations of the earth, become amenable to the laws of nations; and it was their interest as well as their duty to provide, that those laws should be respected and obeyed . . .”), *rev’d on other grounds*, U.S. Const. amend. XI; see also *Ware v. Hylton*, 3 U.S. 199, 281 (1796) (opinion of Wilson, J.) (“When the United States declared their independence, they were bound to receive the law of nations, in its modern state of purity and refinement. By every nation, whatever is its form of government, the confiscation of debts has long been considered disreputable: and, we know, that not a single confiscation of that kind stained the code of any of the European powers, who were engaged in the war, which our

revolution produced.”); *see also Respublica v. De Longchamps*, 1 U.S. 111, 117 (Ct. of Oyer & Terminer 1784) (opinion of M’Kean, C.J.) (noting, in determining punishment for striking a foreign ambassador, that “it is now the interest as well as duty of the government, to animadvert upon your conduct with a becoming severity, such a severity as may tend to reform yourself, to deter others from the commission of the like crime, preserve the honor of the State, and maintain peace with our great and good Ally, and the whole world.”). As one scholar has noted, the Founders’ belief in the importance of “compliance with the law of nations had a strong positive component. Collective compliance by all nations would assure a world safe for trade and travel, rich in the exchange of goods and ideas, conducive to both national and human progress.” Anne-Marie Burley, *The Alien Tort Statute and the Judiciary Act of 1789: A Badge of Honor*, 83 Am. J. Int’l L. 461, 487 (1989).

The Supreme Court has reaffirmed this commitment in modern times. In *Medellin v. Texas*, 552 U.S. 491 (2008), the Court considered whether a decision of the International Court of Justice about consular rights under the Vienna Convention was enforceable in a state court in the United States. While it ultimately ruled that the ICJ ruling was not directly enforceable federal law, the Court noted the “compelling interests” of “ensuring the reciprocal observance of the Vienna Convention, protecting relations with foreign governments, and demonstrating commitment to the role of international law.” *Id.* at 524. Justice Stevens noted in his concurrence that the “entire Court” had considered the “costs of refusing to respect the ICJ’s judgment” in the justices’ various opinions. *Id.* at 537 (Stevens, J., concurring); *see also id.* at 566 (Breyer, J., dissenting) (observing that majority’s holding increases the likelihood “of precipitating actions by other nations putting at risk American citizens who have the misfortune

to be arrested while traveling abroad, or of diminishing our Nation's reputation abroad as a result of our failure to follow the 'rule of law' principles that we preach.”).

Similarly, in *Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004), involving claims under the Alien Tort Statute (“ATS”), Justice Breyer noted that “since enforcement of an international norm by one nation’s courts implies that other nations’ courts may do the same, [he] would ask whether the exercise of jurisdiction under the ATS is consistent with those notions of comity that lead each nation to respect the sovereign rights of other nations by limiting the reach of its laws and their enforcement.” *Id.* at 761 (Breyer, J., concurring in part and concurring in the judgment); *see also Barclays Bank PLC v. Franchise Tax Bd. of Cal.*, 512 U.S. 298, 337 (1994) (O’Connor, J., concurring in judgment and dissenting in part) (noting objections by “[m]ost of the United States’ trading partners” to California tax and expressing concern about “[t]hese adverse consequences, which affect the Nation as a whole . . .”).

Indeed, the United States government itself has urged courts to consider these consequences. In *Brown v. Board of Education*, 347 U.S. 483 (1954), the government argued in an amicus brief that “[i]f we wish to inspire the people of the world whose freedom is in jeopardy, if we wish to restore hope to those who have already lost their civil liberties, if we wish to fulfill the promise that is ours, we must correct the remaining imperfections in our practice of democracy.” *See Br. of the United States as Amicus Curiae, Brown v. Bd. of Educ.*, 347 U.S. 483 (1954) (Nos. 1, 2, 4, 10), 1952 WL 82045, at *32 (quoting Message to the Congress, Feb. 2, 1948, H. Doc. No. 516, 80th Cong., 2d sess., p. 7); *see id.* at *7 (“[T]he undeniable existence of racial discrimination gives unfriendly governments the most effective kind of ammunition for their propaganda warfare. The hostile reaction among normally friendly peoples, many of whom

are particularly sensitive in regard to the status of non-European races, is growing in alarming proportions.”). More recently, in *Medellin*, the Justice Department argued that the Supreme Court should rule that the lower court must enforce the President’s determination to have state courts give effect to a decision of the International Court of Justice, noting “(1) the importance of securing reciprocal protection of Americans detained abroad; (2) the need to avoid harming relations with foreign governments, including Mexico; and (3) the interest in reinforcing the United States’ commitment to the rule of law.” Br. of the United States as Amicus Curiae Supporting Pet’r, *Medellin v. Texas*, 552 U.S. 491 (2008) (No. 06-984), 2007 WL 1909462, at *11.

The reasons given by the Supreme Court for considering the impact of decisions on foreign parties – the promotion of safe trade and travel, the exchange of goods and ideas, and human progress – are especially salient in the interconnected, rapidly evolving world in which we live. Private information about an individual, once released, can spread throughout the world in a blink of an eye. Therefore, in deciding the Government’s motion, this Court should consider the impact its decision will have on not just Americans living in the United States, but on people around the world.

CONCLUSION

The Court’s adjudication of the Government’s motion to compel DreamHost’s compliance with its Search Warrant will have far reaching effects across the globe. A decision granting the motion will potentially impact those foreign citizens and expatriate Americans who actually visited the website in question. But more importantly, it will make others think twice before speaking out or even simply seeking out more information in the future. This Court

should deny the motion, or at least significantly limit the scope of the compelled disclosure, to protect against the infringement of such fundamental rights worldwide.

Respectfully submitted,

/s/Ashley I. Kissinger

Ashley I. Kissinger (D.C. Bar No. 463421)
LEVINE SULLIVAN KOCH & SCHULZ, LLP
1888 Sherman Street, Suite 370
Denver, CO 80203
Tel. 303-376-2407
Fax 303-376-2401
akissinger@lskslaw.com

August 22, 2017