Marcia Hofmann (Cal. Bar No. 250087)
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Telephone: (415) 830-6664
marcia@zeitgeist.law

Attorney for Amici Curiae Automattic, Inc.; CloudFlare, Inc.; CREDO Mobile, Inc.; Mapbox, Inc.; A Medium Corp.; Reddit, Inc.; Wickr Foundation; and Wikimedia Foundation

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

TWITTER, INC.,

Plaintiff,

v.

LORETTA E. LYNCH, United States Attorney General, *et al.*,

Defendants.

Case No. 14-cv-4480 YGR

BRIEF OF AMICI CURIAE AUTOMATTIC, INC.; CLOUDFLARE, INC.; CREDO MOBILE, INC.; MAPBOX, INC.; A MEDIUM CORP.; REDDIT, INC.; WICKR FOUNDATION; AND WIKIMEDIA FOUNDATION IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS THE AMENDED COMPLAINT

Date: March 15, 2016
Time: 2:00 p.m.
Courtroom 1, Fourth Floor
Hon. Yvonne Gonzalez Rogers

STATEMENT OF INTEREST OF AMICI CURIAE

Amici are Internet companies, communication service providers, and not-for-profit organizations that want to be open and honest with their users and the public about the volume of national security requests they receive from the government. Like Twitter, Amici publish regular transparency reports providing statistics about government requests for user information. Amici believe the reporting rules for national security information currently sanctioned by the government do not allow them to tell a candid story.

Automattic operates WordPress.com, a web-based publishing platform. WordPress.com is powered by the open-source WordPress software, which is available for anyone to use or improve for free. WordPress.com hosts sites for some of the largest media companies in the world, including the New York Post, CNN, and Time. It also hosts more than 70 million individual blogs operated by small businesses, individuals, and citizen journalists who publish on a wide range of topics.

CloudFlare offers some of the most advanced web security, distributed denial of service attack mitigation, and content delivery solutions available. CloudFlare is a community of more than 4 million websites handling over 5 percent of global web and blocking more than 8.3 billion potentially malicious requests every day. In order to ensure the greatest possible participation in its community, CloudFlare is committed to transparency, free speech, and due process for all legal requests.

CREDO Mobile is a U.S.-based telecommunications company that donates a portion of its revenue to progressive non-profits and engages in social change activism.

Mapbox provides highly customizable maps and mapping software for web, mobile, and embedded applications. Based in Washington, D.C., Mapbox powers the maps behind some of the most visited sites on the web.

Medium, based in San Francisco, California, offers a publishing platform that allows anyone to easily read and share stories and ideas that matter to them. Tens of millions of users have spent in sum more than 2.6 millennia reading on Medium.

Reddit is an online community where users can start, read, join, and rate discussions on topics they submit and choose. Reddit is based in San Francisco, California and attracts over 230

million monthly unique visitors.

Wickr Foundation is a non-profit organization dedicated to supporting a strong free society by championing private communications and uncensored access to information. The key mission of Wickr Foundation is to provide education, digital security and privacy tools for at-risk populations underserved by commercial markets. The Foundation operates educational and public awareness programs for policy-makers, youth, journalists, and human rights organizations. Wickr Foundation was launched by Wickr Inc., a communication platform that enables anyone in the world to communicate freely, privately and securely. Wickr Inc. publishes transparency reports on a quarterly basis.

The Wikimedia Foundation is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the Internet. Wikimedia's mission is to develop and maintain "wiki"-based projects, and to provide the full contents of those projects to individuals around the world free of charge. In December 2015, all Wikimedia Projects combined had 14.95 billion page views across mobile and desktop devices, including 7.12 billion on English Wikipedia. As of December 2015, there were over 5 million articles on English Wikipedia, and 9.9 million edits were made that month.

INTRODUCTION

This case is about an Internet company's desire to be open and honest with the public about its role, or lack thereof, in national security investigations. Its outcome is key for all organizations that want to be transparent about what they do and provide meaningful information to the public about how much national security process they receive. Reporting national security requests under the rubric approved by the United States government obfuscates rather than illuminates the volume of this sensitive and controversial process. Like Twitter, Amici want to provide useful, accurate information to the public and respond to their users' concerns in a way that does no harm to national security—and believe the First Amendment permits them to do so. Amici urge the Court to deny the government's motion to dismiss and proceed to the merits.

BACKGROUND

Twitter filed this suit on October 7, 2014 after the Department of Justice denied the company permission to publish a transparency report in which Twitter wished to provide aggregate numbers of national security process in smaller bands than those permitted by the government. Compl. (ECF No. 1.) After the passage of the USA FREEDOM Act changed the laws at the heart of Twitter's claims in June 2015, the Court gave Twitter leave to amend its complaint. Order at 12. (ECF No. 85.)

Twitter now seeks to establish its First Amendment right to publish a draft transparency report disclosing the amount of legal process it received from the Foreign Intelligence Surveillance Court (FISC) between July 1, 2013 and December 31, 2013. Am. Compl. ¶ 4. (ECF No. 88.) Twitter does not wish to reveal detail about any specific order that it may have received from the FISC during that time period, but rather seeks to publish "the actual aggregate number of [Foreign Intelligence Surveillance Act (FISA)] orders received (if any), the volume of FISA orders received by comparison to government-approved reporting structures, and similar information." Am. Compl. ¶ 4. Twitter also wants the freedom to report that "it received 'zero' FISA orders, or 'zero' of a specific kind of FISA order, for that period, if either of these circumstances is true." Am. Comp. ¶ 4. Further, Twitter seeks to release more specific details about particular FISA orders it has received in the past or may receive in the future when doing so will no longer harm national security. Am. Comp. ¶ 7.

Twitter asserts that FISA's nondisclosure provisions violate the First Amendment on their face, and to the extent the government relies on those provisions to prohibit Twitter indefinitely from publishing information about FISA orders it receives, those provisions are unconstitutional as applied. Am. Compl. ¶¶ 49-57. Further, to the extent the government might prosecute Twitter under the Espionage Act for publishing such information, that law is unconstitutional as applied to Twitter. Am. Compl. ¶¶ 58-61.

The government now moves to dismiss Twitter's amended complaint, arguing 1) the FISC should hear Twitter's challenges to FISA's nondisclosure provisions, 2) Twitter has failed to show that it has standing to challenge the constitutionality of the Espionage Act, and 3) Twitter's claims fail as a matter of law because the government may lawfully prohibit disclosure of classified information

learned through participating in a national security investigation. Defs. Mot. Dismiss. (ECF No. 94.)

ARGUMENT

Amici urge this Court to reach the merits of this case and determine whether service providers have a constitutional right to report data about national security requests, including orders issued by the FISC. This question is crucial for all companies seeking to provide accurate, useful information to their users in the aftermath of momentous public disclosures about government surveillance that have undermined user trust in online services.

I. Twitter's Claims Present Critical First Amendment Issues That Also Affect Amici and Similarly Situated Service Providers

In June 2013, government contractor Edward Snowden leaked classified records from the National Security Agency to the media, exposing government surveillance activities far more extensive than previously known to the public and raising profound questions about the lawfulness of those activities. *See, e.g.*, Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013.[1]

In the wake of worldwide public debate about U.S. communications providers' role in this controversial government surveillance, several major Internet companies negotiated with the Department of Justice for the right to publicly disclose aggregate information about the legal process they receive from the government in national security investigations. When these negotiations failed to yield results, Google, Facebook, Microsoft, Yahoo!, and LinkedIn filed motions in the FISC seeking to establish that they have a First Amendment right to publish basic aggregate data about the FISA orders they receive. *In re Motions to Disclose Aggregate Information Regarding FISA Orders and Directives*, Nos. Misc. 3-03, 13-04, 13-05, 13-06 & 13-07 (F.I.S.C. filed 2013).

The litigation settled, however, when those companies reached an agreement with the Justice Department permitting them to report national security requests in broad bands of aggregate numbers. Letter From James M. Cole, Deputy Attorney General, Department of Justice, to General Counsels of

[1] Available at http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Facebook, Google, LinkedIn, Microsoft, and Yahoo, Jan. 27, 2014.[2] The Justice Department apparently took the position that these restrictions applied not only to the parties to the agreement, but more broadly to other service providers, as well, which prompted Twitter to initiate this action. Compl. ¶¶ 35-40.

In June, Congress passed the USA FREEDOM Act, which largely incorporated the Justice Department's approved reporting framework into the FISA. Pub. L. No. 114-23, 129 Stat. 268, codified at 50 U.S.C. § 1874. Specifically, the USA FREEDOM Act gives recipients of national security process four reporting options, allowing them to issue:

- A semiannual report on the number of national security letters (NSLs), customer accounts affected by NSLs, FISA orders for content, FISA orders for non-content, and customer selectors targeted by each type of FISA order as separate categories in bands of 1000, beginning with 0 (*i.e.*, 0-999), with some breakdown by FISA authority for non-content figures;

- A semiannual report on the number of NSLs, customer accounts affected by NSLs, FISA orders for content, FISA orders for non-content, and customer selectors targeted by each type of FISA order as separate categories in bands of 500, beginning with 0 (*i.e.*, 0-499);[3]

- A semiannual report on the total number of all national security requests received, and the total number of customer selectors targeted by all national security process, in bands of 250, beginning with 0 (*i.e.*, 0-249); or

- An annual report on the total number of all national security requests received, and the total number of customer selectors targeted by all national security process, in bands of 100, beginning with 0 (*i.e.*, 0-99).

50 U.S.C. § 1874(a)(1)-(4). The USA FREEDOM Act did not amend FISA's pre-existing nondisclosure provisions, however. While this framework provides guidance, it fails to clarify the legal limits of reporting aggregate information about national security process.

As a result, this case poses a fundamental lingering question: to what extent do companies have a *constitutional right* to report truthful aggregate data about national security requests? Amici believe

[2] Available at http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.

[3] The law also limits the time period a report may cover, ranging from 180 days to one year. 50 U.S.C. § 1874(b)(1)-(3). When publishing a report that discloses categories in bands of 500 and 1000, providers are required to wait 18 months before reporting any FISA order or directive concerning a platform, product, or service for which the provider has not previously received a FISA order or directive. *Id.* § 1874(b)(B).

that there is no basis in law or policy for the government to prohibit recipients from disclosing the mere fact that they have or have not received a national security request, and from publishing an accurate, meaningful account of that statistic. And while the government has taken the position that it believes "[n]othing prevents a company from reporting that it has received no national security legal process at all," Reply in Further Support of Defs. Partial Mot. Dismiss at 2 (ECF No. 57), it remains unclear whether the First Amendment guarantees that disclosure, or whether a company that has received a national security request in the past could report zero for subsequent periods of time.

The Court should resolve this question because the reporting framework approved by the government is a particularly poor fit for service providers that receive little, if any, process in national security investigations. The bands are simply too large to give the public a meaningful sense of the volume of national security requests such a company may receive.

Compare the permitted ranges to the number of regular law enforcement requests that companies can report with specificity. For example, between July 1 and December 31, 2013 (the same period covered by the transparency report Twitter seeks through this litigation to publish), Automattic received 36 non-national security requests for user information from all law enforcement authorities worldwide (including all federal and state authorities).[4] CloudFlare received 50 non-national security requests from law enforcement throughout the United States during 2013.[5] Similarly, LinkedIn received 70 non-national security requests from United States law enforcement seeking user data between July 1 and December 31, 2013.[6] Each of these companies detailed the number and type of these requests in their transparency reports—but reported that they received 0-249 national security requests for the same period, even though the high end of the permitted range is several times the number of *all* law enforcement requests each company received.

[4] Automattic, *Information Requests*, http://transparency.automattic.com/information-requests-2013-h2 (last visited Feb. 5, 2016).

[5] CloudFlare, *2013 Transparency Report: 1/1/2013-12/31/2013,* https://www.cloudflare.com/transparency2013 (last visited Feb. 5, 2016).

[6] LinkedIn, *Our Transparency Report*, https://www.linkedin.com/legal/transparency (last visited Feb. 5, 2016).

Did these companies receive zero national security requests during the reporting period? Or a handful? Or hundreds of FISA orders? Under the government's framework, recipients cannot say. It forces them to tell a misleading story that leaves users with more questions than answers about these highly sensitive and controversial requests.

Reporting national security requests in this manner encourages public speculation about the U.S. government's level of interest in a service, which can lead to suspicion and distrust among users and have a very real, negative impact on business. Users of online platforms and communications services are more sensitive than ever to disclosures of their data to governments, and there is a strong desire for truthful, accurate information about government interest in users' data (or lack thereof). This is especially true for users outside the United States, who may choose non-U.S. competitors once their confidence in U.S. Internet companies' candor is shaken. *See generally* Danielle Kehl, New America's Open Technology Institute, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity* 7-19 (July 2014) (discussing the negative economic impact of the surveillance revelations on American businesses, both domestically and internationally).[7] For any U.S. Internet company with non-U.S. users, the international community's trust is essential to basic business operations. And its absence is a competitive disadvantage. One example: the European Court of Justice recently invalidated the U.S.-EU Safe Harbor arrangement—which had enabled transfers of Europeans' data to the United States—due in significant part to revelations about the U.S. government's surveillance activities. *Schrems v. Data Protection Commissioner*, Case C-362/14 (EJC Oct. 6, 2015). This decision creates for Amici substantial and costly obstacles to operating in the European Union.

Twitter's claims are important for all service providers seeking to re-establish trust in the wake of the Snowden disclosures. Amici hope the Court will reach these issues to provide greater legal certainty for all service providers seeking to be honest and upfront with their users.

[7] Available at http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf.

II. This Court Should Hear This First Amendment Case and Not Defer to the Foreign Intelligence Surveillance Court

The government argues that this Court should decline to exercise jurisdiction over Counts I and II because they "concern legal process issued by the FISC and provisions of FISA administered under FISC supervision." Defs. Mot. Dismiss at 10. To the contrary, this Court is the correct forum.

First, this case is a First Amendment challenge to the underlying statute, not a challenge to an order of the FISC. Twitter contends that FISA's nondisclosure provisions are unconstitutional facially and as applied, to the extent these provisions might prohibit Twitter from publishing information about the number of FISA orders it receives that would not harm national security. Am. Compl. ¶¶ 49-57. And these are not Twitter's only constitutional claims. Twitter also argues that the Espionage Act is unconstitutional as applied to Twitter—a claim the FISC has no jurisdiction to review. Am. Compl. ¶¶ 58-61. There is no jurisdictional impediment to this Court's review of *all* Twitter's First Amendment claims, and it should do so for the sake of judicial efficiency.

Second, this Court should hear the case because its proceedings are open and public by default, which allows greater public awareness of how this litigation proceeds. The FISC is fundamentally different from any other United States district court because its docket, hearings, and records are generally classified. While this Court "operate[s] primarily in public, with secrecy the exception," the FISC "operates primarily in secret, with public access the exception." *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 488 (F.I.S.C. 2007).

Congress has recognized the problematic nature of the FISC's secret proceedings. It has tried to make the court more transparent by, among other things, providing a process for limited amicus curiae participation in FISC matters. USA FREEDOM Act, Pub. L. 114-23, 129 Stat. 279 § 401, codified at 50 U.S.C. § 1803. While this change is a step toward greater public participation in FISC proceedings, the court still conducts its judicial proceedings primarily out of public view and does not allow for the level of amici participation that other district courts permit. Potential FISC amici face profound and basic constraints on their ability to contribute effectively. For example, amici must have a security clearance to obtain access to classified case materials and proceedings. 50 U.S.C. §

1803(i)(3)(B); (6)(C). Furthermore, amici may only review legal precedents, applications, certifications, petitions, motions, or other materials that the FISC believes in its sole discretion "are relevant to the duties of the amicus curiae." *Id.* § 1803(i)(6)(A)(i). These restrictions mean that amici will likely have very limited (if any) access to the materials and proceedings in a FISC matter, which undermines their ability to meaningfully participate. By contrast, the filings in this Court are public by default and available to all unless sealed, which allows for more informed, robust amicus involvement.

Given the important constitutional issues raised by Twitter's complaint and the precedential value this decision will have for Amici and the rest of the technology industry, this case should be heard by a court that makes its proceedings and records public by default. This Court, not the FISC, is the right forum for this case.

CONCLUSION

Amici just want to speak truthfully, address their users' legitimate concerns, and provide useful data to the public. Amici respectfully request that this Court deny the government's motion to dismiss and reach the merits of the case.

DATED: February 5, 2016

Respectfully submitted,

/s/ Marcia Hofmann

Marcia Hofmann
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
marcia@zeitgeist.law
Telephone: (415) 830-6664

Attorney for Amici Curiae Automattic, Inc.; CloudFlare, Inc.; CREDO Mobile, Inc.; Mapbox, Inc.; A Medium Corp.; Reddit, Inc.; Wickr Foundation; and Wikimedia Foundation