Marcia Hofmann (Cal. Bar No. 250087)
25 Taylor Street
San Francisco, CA 94102
Telephone: (415) 830-6664
marcia@marciahofmann.com

Attorney for *Amici Curiae*
Automattic Inc.; CloudFlare, Inc.;
CREDO Mobile, Inc.; A Medium Corp.; Sonic.net, Inc.;
Wickr, Inc.; and the Wikimedia Foundation

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

TWITTER, INC.,

Plaintiff,

v.

ERIC H. HOLDER, United States Attorney General, *et al.*,

Defendants.

Case No. 14-cv-4480 YGR

BRIEF OF *AMICI CURIAE* AUTOMATTIC INC.; CLOUDFLARE, INC.; A MEDIUM CORP.; SONIC.NET, INC.; WICKR, INC.; AND THE WIKIMEDIA FOUNDATION IN OPPOSITION TO DEFENDANTS' PARTIAL MOTION TO DISMISS

Date: March 31, 2015
Time: 2:00 p.m.
Courtroom 1, Fourth Floor
Hon. Yvonne Gonzalez Rogers

STATEMENT OF INTEREST OF *AMICI CURIAE*

We are small Internet companies and communication service providers that want to be open and honest with our users and the public about the number of national security requests we receive from the government. We publish regular transparency reports that include statistics about government requests for user information, and we believe the reporting rules currently approved by the Justice Department do not allow us to tell a candid story.

Automattic Inc. is the company behind WordPress. WordPress web publishing software powers more than 23% of the Internet—from small blogs to the websites of some of the biggest media companies in the world. Automattic has 300 employees worldwide.

CloudFlare, Inc. offers some of the most advanced web security, distributed denial of service attack mitigation, and content delivery solutions available. CloudFlare is a community of over 2 million websites handling as much as 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, Inc. is a U.S.-based telecommunications company that donates a portion of its revenue to progressive non-profits and engages in social change activism.

A Medium Corporation offers a publishing platform that allows anyone to easily read and share stories and ideas that matter to them. Medium has 80 employees and is based in San Francisco, California.

Sonic.net, Inc. is a regional Internet access and telecommunications provider offering competitive services in 125 California cities. Sonic provides telephone service, DSL and Gigabit fiber-to-the-home Internet access, as well as custom services for businesses. Sonic has 210 employees and is based in Santa Rosa, California.

Wickr, Inc. provides a communication platform that enables anyone in the world to communicate freely, privately and securely. Wickr's technology was built by world-renowned encryption experts and human rights activists to protect the right to private communication and free expression around the globe. Wickr's messaging platform processes over 4 million messages a day

including text, photo, video, audio and other types of files. Users of Wickr's mobile messaging product include law enforcement agents, journalists and human rights activists, families including young children and teens, professionals and celebrities worldwide. Transparency is critical to Wickr's mission to build and protect the human right to privacy and free expression.

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. The most well known of Wikimedia's projects is Wikipedia—a free Internet encyclopedia that is the sixth-most visited website in the world and largest collection of shared knowledge in human history. Wikimedia has fewer than 250 employees.

INTRODUCTION

This case is about an Internet company's desire to be transparent about its role—or lack thereof—in national security investigations. Twitter, Inc. seeks a declaratory judgment that it has a right under the First Amendment to publish aggregate statistics about national security requests it has received from the government, and the laws and government orders restricting its ability to do so are unconstitutional and unlawful.

The outcome of this case is important for small Internet companies and communication service providers working to be transparent about their practices and provide meaningful information to the public. Reporting national security requests in the manner approved by the Justice Department obfuscates rather than illuminates the volume of national security requests a small company receives. We simply want to offer useful, accurate information and respond to the concerns of our users. *Amici* urge the Court to deny the government's partial motion to dismiss and proceed to the merits.

BACKGROUND AND FACTS

In this case, Twitter is suing the United States to establish its right to publish information about the aggregate number of national security requests the company receives from the government. Twitter filed suit after the Department of Justice denied Twitter permission to publish a transparency report in which Twitter wishes to provide aggregate numbers of national security process in smaller

bands than those currently approved by the government. Twitter also wants the freedom to report that it received zero national security requests if appropriate. Twitter seeks a declaration that the government's restrictions violate Twitter's First Amendment rights and the Administrative Procedure Act. Compl. ¶¶ 43-44.

Twitter also challenges the constitutionality of 18 U.S.C. §§ 2709 and 3511, two statutes that authorize the Federal Bureau of Investigation to issue national security letters (NSLs) in counterintelligence investigations demanding non-content information from telecommunications and Internet service providers. These letters are issued unilaterally by the Bureau without any prior judicial review, and are almost always accompanied by a non-disclosure order barring the recipient from revealing anything about the demand. Compl. ¶¶ 46-48. In fact, nondisclosure orders accompany about 97 percent of all NSLs issued by the FBI. *Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies* 92 (Dec. 12, 2013).

Finally, Twitter asserts that to the extent the government relies on the nondisclosure provisions of the Foreign Intelligence Surveillance Act to prevent Twitter from publishing the aggregate number of FISA orders it receives, those provisions are unconstitutional on their face and as applied to Twitter. Compl. ¶¶ 49-50.

The government has moved to dismiss Twitter's complaint in part, claiming 1) the Court lacks subject matter jurisdiction to review a letter from Deputy Attorney General James M. Cole to certain Internet companies explaining what national security statistics they are permitted to publish, 2) the Foreign Intelligence Surveillance Court should hear the challenge to FISA's nondisclosure provisions, and 3) Twitter's challenge to the NSL standard of review fails as a matter of law.

ARGUMENT

Amici urge this Court to reach the merits of this case and determine whether companies have a right to report data about national security requests. This question is crucial for all companies like *amici* seeking to provide accurate, useful information to their users in the aftermath of momentous public disclosures about government surveillance.

In June 2013, a National Security Agency contractor named Edward Snowden leaked a trove of agency records 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. Among other revelations, the records disclosed a surveillance program known as PRISM in which the NSA taps directly into the servers of Google, Apple, Microsoft, Facebook, and several other prominent Internet companies to collect users' emails, photos, audio and video communications, searches, connection logs, and other information. 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] Glenn Greenwald and Ewan MacAskill, *NSA PRISM Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN, June 6, 2013.[2] While PRISM is intended to gather intelligence about designated foreigners abroad, the program also sweeps up the data of Americans who are communicating with those targets. The Internet companies disputed that they gave the government direct access to their servers, as the press had reported. Joshua Brustein, *The Companies' Lines on PRISM*, BLOOMBERG, June 7, 2013.[3]

In the wake of the Snowden leak, several major Internet companies negotiated with the Department of Justice for the right to publicly disclose aggregate information about the national security requests they receive from the government. When these negotiations failed to yield results, Google, Facebook, Microsoft, Yahoo!, and LinkedIn filed suit in the Foreign Intelligence Surveillance Court seeking to establish that they have a First Amendment right to publish basic aggregate data about the FISA orders they receive. *See* Ryan Gallagher, *Tech Giants United in Court to Fight Against Government Surveillance Secrecy*, SLATE, Sept. 10, 2013.[4]

---

[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.

[2] Available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[3] Available at http://www.bloomberg.com/bw/articles/2013-06-07/the-companies-lines-on-prism.

[4] Available at http://www.slate.com/blogs/future_tense/2013/09/10/yahoo_google_facebook_microsoft_fight_for_permission_to_release_data_about.html.

The case settled when those companies reached an agreement with the Justice Department permitting them to report national security requests in two different ways. Letter From James M. Cole, Deputy Attorney General, Department of Justice, to General Counsels of Facebook, Google, LinkedIn, Microsoft, and Yahoo, Jan. 27, 2014.[5] The first option is to report numbers 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 1000, beginning with 0 (*i.e.*, 0-999). *Id.* at 2-3. Alternatively, the companies could choose to report 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). *Id.* at 3. The government apparently takes the position that these restrictions apply not only to the parties to the agreement, but more broadly to other companies, as well. Compl. ¶¶ 35-40.

The current Justice Department framework makes it impossible for small companies like *amici* to paint a truthful picture of what we see. The negotiated solution may work well for large companies that receive a high number of national security requests. But the bands are simply too wide for us to give our users any useful sense of the volume of national security requests we may receive. Under the Justice Department's rules, it does not matter if the number is zero, one, or 100, because the figures will always be the same: 0-249 or 0-999.

Compare these permitted ranges to the number of regular law enforcement requests that *amici* can report with specificity. For example, between July 1 and December 31, 2013, Automattic received 36 non-national security requests for user information from all law enforcement authorities worldwide (including all federal and state authorities).[6] CloudFlare received 50 non-national security requests from law enforcement throughout the United States during 2013.[7] Both companies detailed

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

[6] Automattic, *Information Requests*, http://transparency.automattic.com/information-requests-2013-h2 (last visited Feb. 17, 2015).

[7] CloudFlare, ***2013** Transparency Report: 1/1/2013-12/31/2013,* https://www.cloudflare.com/transparency2013 (last visited Feb. 17, 2015).

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. Did these companies receive no national security requests? A handful? A couple hundred? According to the Justice Department, they are not allowed to say—which leaves their users with more questions than answers when it comes to this highly sensitive and controversial category of request. Reporting this way creates speculation about the level of government interest in a service, which invariably leads to suspicion and lack of trust from users and the public.

This reporting framework is a poor fit for companies like ours, and the erosion of trust it causes has a very real, negative impact on our businesses. 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 our users' data (or lack thereof). This is especially true for our many users outside the United States, who may decide to use competing services based abroad if we lose their confidence. *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).[8]

We just want to speak truthfully, address the legitimate concerns of our users, and provide useful information to the public. We urge the Court to deny the government's partial motion to dismiss and proceed to the merits. This case raises a basic question that is not resolved by the Justice Department's framework: to what extent do companies have a right to report data about national security requests? *Amici* believe 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 account of that statistic. We hope the Court will address this question

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

to provide legal certainty for all service providers, large and small, seeking to be upfront with their users.

CONCLUSION

A*mici* respectfully request that this Court deny the government's partial motion to dismiss and reach the merits of the case.

DATED: February 17, 2015

Respectfully submitted,

/s/ Marcia Hofmann

Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
marcia@marciahofmann.com
Telephone: (415) 830-6664

Attorney for *Amici Curiae*
Automattic Inc.; CloudFlare, Inc.; CREDO Mobile, Inc.; A Medium Corp.; Sonic.net, Inc.; Wickr, Inc.; and the Wikimedia Foundation