

ENDORSED
FILED
SAN FRANCISCO COUNTY
SUPERIOR COURT

2012 DEC 21 PM 3:02

CLERK OF THE COURT

BY: _____
DEPUTY CLERK

1 Linda Lye (Bar No. 215584)
AMERICAN CIVIL LIBERTIES UNION
2 FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
3 San Francisco, CA 94111
Telephone: (415) 621-2493; Fax: (415) 255-8437
4 Email: llye@aclunc.org

5 Hanni M. Fakhoury (Bar No. 252629)
Nathan D. Cardozo (Bar No. 259097)
6 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
7 San Francisco, CA 94110
Telephone: (415) 436-9333; Fax: (415) 436-9993
8 Email: hanni@eff.org; nate@eff.org

9 Aden J. Fine (Bar No. 186728)
AMERICAN CIVIL LIBERTIES UNION
10 FOUNDATION
125 Broad Street, 18th Floor
11 New York, NY 10004
Telephone: (212) 549-2500
12 Email: afine@aclu.org

13 Attorneys for *Amici Curiae*

14 IN THE SUPERIOR COURT OF CALIFORNIA

15 COUNTY OF SAN FRANCISCO

16 PEOPLE OF THE STATE OF
17 CALIFORNIA,

18 Plaintiff,

19 v.

20 ROBERT DONOHOE,

21 Defendant.

Case No. 12025934

**APPLICATION FOR LEAVE TO FILE
AMICI CURIAE BRIEF AND [PROPOSED]
BRIEF OF AMICI CURIAE OF AMERICAN
CIVIL LIBERTIES UNION, AMERICAN
CIVIL LIBERTIES UNION OF NORTHERN
CALIFORNIA AND ELECTRONIC
FRONTIER FOUNDATION IN SUPPORT OF
MOTIONS TO QUASH SUBPOENA DUCES
TECUM ISSUED BY THE PEOPLE TO
TWITTER, INC.**

**LEAVE TO PARTICIPATE IN ORAL
ARGUMENT REQUESTED**

Date: January 4, 2013

Time: 1:30 p.m.

Dept: 16

1 with a protest on a single day in October. Defendants Smith and Donohoe have moved to quash
2 the subpoenas because they violate the Stored Communications Act. *See* 18 U.S.C. § 2703.
3 *Amici* concur, but seek leave to make the additional argument that the motions to quash should
4 be granted because the subpoenas violate the First and Fourth Amendments, and parallel
5 provisions under the state constitution.

6 Our Supreme Court has made clear that orders compelling the disclosure of information
7 about individuals' communications or associations must be "narrowly circumscribed" to serve a
8 "'compelling' state interest." *Britt v. Superior Court*, 20 Cal.3d 844, 848-49 (1978). "Mere
9 relevance is not sufficient." *Rancho Publications v. Superior Court*, 68 Cal.App.4th 1538, 1549
10 (1999). The California Supreme Court has held that government surveillance of what we say –
11 even when we say it in a public setting – can have a chilling effect on speech and can therefore
12 give rise to a violation of the First Amendment and the parallel state constitutional protection for
13 speech. *See White v. Davis*, 13 Cal.3d 757 (1975). The subpoenas at issue here are dramatically
14 overbroad. They seek information about the opinions and comments of defendants over a ten-
15 month period, on any and all subjects. Twitter can function like a virtual diary, reflecting a
16 user's thoughts and opinions on topics ranging from the personal to the political. Yet the
17 government seeks to capture all tweets by Defendants Smith and Donohoe, without any effort to
18 target only those communications that may have some connection to the charged crimes, or to
19 offer any basis for believing that the planning for a political protest on a single day in October
20 was likely to have commenced nine months earlier. Moreover, the subpoenas are also overbroad
21 because they seek tweets by third parties that simply mention Defendants, even if those other
22 speakers and their speech have no connection to the alleged crimes whatsoever.

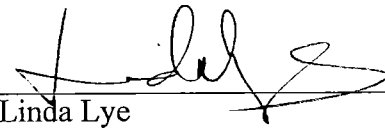
23 A district attorney's decision to prosecute is not an invitation for the government to
24 engage in intrusive fishing expeditions into a criminal defendant's opinions, beliefs, and
25 interests, let alone the opinions, beliefs, or interests of third parties unconnected to the charged
26 crime other than that they have once uttered the names of defendants or their Twitter accounts.
27 But that is precisely what the government seeks to do here. *Amici* respectfully believe that their
28 expertise on the constitutional issues will be of assistance to the Court.

1 *Amici* also request leave to participate at the oral argument at the hearing on the motions
2 to quash the subpoenas on Twitter, Inc.

3 Accordingly, the ACLU, ACLU-NC, and EFF respectfully request leave of this Court to
4 file the accompanying Brief of *Amici Curiae*.

5 Dated: December 21, 2012

Respectfully submitted,

6
7
8 By: 
Linda Lye

9
10 Linda Lye (Bar No. 215584)
11 AMERICAN CIVIL LIBERTIES UNION
12 FOUNDATION OF NORTHERN CALIFORNIA
13 39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493; Fax: (415) 255-8437
Email: llye@aclunc.org

14 *Attorneys for amicus* American Civil Liberties
Union of Northern California

15 Hanni M. Fakhoury (Bar No. 252629)
16 Nathan D. Cardozo (Bar No. 259097)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333; Fax: (415) 436-9993
Email: hanni@eff.org; nate@eff.org

17
18
19 *Attorneys for amicus* Electronic Frontier Foundation

20 Aden Fine (Bar No. 186728)
21 AMERICAN CIVIL LIBERTIES UNION
22 FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
23 afine@aclu.org

24 *Attorneys for amicus* American Civil Liberties
25 Union

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND..... 2

III. ARGUMENT 4

 A. THE SUBPOENAS VIOLATE THE FIRST AMENDMENT BECAUSE THEY
 SEEK EXPRESSIVE AND ASSOCIATIONAL INFORMATION BUT ARE
 OVERBROAD..... 4

 1. The First Amendment Provides a Qualified Privilege Against Compelled
 Disclosure of Speech and Associational Activity 5

 2. The Subpoenas Must Satisfy *Britt* Because They Implicate First
 Amendment Interests. 7

 3. The Subpoenas Are Not Narrowly Drawn..... 8

 B. THE SUBPOENAS VIOLATE THE FOURTH AMENDMENT BECAUSE
 TWITTER USERS HAVE A REASONABLE EXPECTATION OF PRIVACY
 IN PRIVATE COMMUNICATIONS AND ACCOUNT INFORMATION 12

IV. CONCLUSION..... 15

TABLE OF AUTHORITIES

Cases

Amazon.com LLC v. Lay, 758 F. Supp.2d 1154 (W.D. Wash. 2010)11

Britt v. Superior Court, 20 Cal.3d 844 (1978)..... passim

Church of Hakeem, Inc. v. Superior Court, 110 Cal.App.3d 384 (1980).....10

City of Ontario v. Quon, 130 S. Ct. 2619 (2010)..... i

Community-Serv. Broadcasting of Mid-America, Inc. v. FCC,
593 F.2d 1102 (D.C. Cir. 1978).....7

Davis v. Superior Court, 7 Cal.App.4th 1008 (1992)..... ii, 1, 9

Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963)5

Hill v. National Collegiate Athletic Assn., 7 Cal.4th 1 (1994).....8

*In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n
Serv. to Disclose Records to Gov’t*, 620 F.3d 304 (3d Cir. 2010) i

Katz v. United States, 389 U.S. 347 (1967)13, 14

Krinsky v. Doe, 159 Cal.App.4th 1154 (2008)8

Lo-Ji Sales v. New York, 442 U.S. 319 (1979)6

Office Depot, Inc. v. Zuccarini, 596 F.3d 696 (9th Cir. 2010)4

People v. Blair, 25 Cal. 3d 640 (1979)15

People v. Chapman, 36 Cal. 3d 98 (1984).....15

People v. Harris, 36 Misc.3d 613 (NY 2012).....12, 13

People v. McKunes, 51 Cal. App. 3d 487 (1975)15

People v. Palmer, 24 Cal.4th 856 (2001).....15

People v. Vu, 143 Cal.App.4th 1009 (2006).....10

Rancho Publications v. Superior Court,
68 Cal.App.4th 1538 (1999) passim

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)8

Smith v. Maryland, 442 U.S. 735 (1979)14

Sony Music Ent. Inc. v. Does 1-40,
326 F. Supp.2d 556 (S.D.N.Y. 2004).....13

Tylo v. Superior Court, 55 Cal.App.4th 1379 (1997)7

1	<i>United Farm Workers of America v. Superior Court</i> , 170 Cal.App.3d 391 (1985)	7, 10
2	<i>United States v. Garcia</i> , 474 F.3d 994 (7th Cir. 2007).....	8
3	<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	14
4	<i>United States v. Jones</i> , 132 S. Ct. 945 (2012).....	i
5	<i>United States v. Jones</i> , 132 S.Ct. 945 (2012).....	14
6	<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	14
7	<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010).....	i, 13
8	<i>White v. Davis</i> , 13 Cal.3d 757 (1975).....	ii, 1, 6, 8
9	Constitutional & Statutory Provisions	
10	Cal. Const, art. I, §2	4
11	Cal. Const., art. I, §1	12
12	Cal. Const., art. I, §13	12
13	18 U.S.C. § 2703	1, 12
14	Cal. Pen. Code § 185.....	4
15	Cal. Pen. Code § 406.....	4
16	Cal. Pen. Code § 407.....	4
17	Cal. Pen. Code § 404(a)	4
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 **I. INTRODUCTION**

2 Ostensibly in the name of finding evidence of a potential conspiracy, the government served
3 Twitter, Inc., with subpoenas seeking, among other things, *all* communications over a *ten-month* period
4 *by or about* two defendants charged with rioting and other alleged crimes in connection with a political
5 protest. Defendants Smith and Donohoe have moved to quash the subpoenas because they violate the
6 Stored Communications Act. *See* 18 U.S.C. § 2703. *Amici* American Civil Liberties Union, American
7 Civil Liberties Union of Northern California, and Electronic Frontier Foundation concur, but seek leave
8 to make the additional argument that the motions to quash should be granted because the subpoenas
9 violate the First and Fourth Amendments and the parallel provisions of the California Constitution.

10 Our Supreme Court has made clear that orders compelling the disclosure of information about
11 individuals' communications or associations must be "narrowly circumscribed" to serve a "'compelling'
12 state interest." *Britt v. Superior Court*, 20 Cal.3d 844, 848-49 (1978). "Mere relevance is not
13 sufficient." *Rancho Publications v. Superior Court*, 68 Cal.App.4th 1538, 1549 (1999). The subpoenas
14 at issue here, however, are dramatically overbroad. They seek information about the opinions and
15 comments of defendants over a ten-month period, on any and all subjects. Twitter can function like a
16 virtual diary, reflecting a user's thoughts and opinions on topics ranging from the personal to the
17 political. Yet the government seeks to capture all tweets by Defendants Smith and Donohoe, without
18 any effort to target only those communications that may have some connection to the charged crimes, or
19 to offer any basis for believing that the planning for a political protest on a single day in October was
20 likely to have commenced nine months earlier. Moreover, the subpoenas are also overbroad because
21 they seek tweets by third parties that simply mention Defendants, even if those other speakers and their
22 speech have no connection to the alleged crimes whatsoever.

23 It is no answer to say that tweets are "public" statements and that they therefore lose all
24 constitutional protection. The California Supreme Court has rejected that proposition, holding that
25 government surveillance of what we say – even when we say it in a public setting – can have a chilling
26 effect on speech and can therefore give rise to a violation of the First Amendment and the parallel state
27 constitutional protection for speech. *See White v. Davis*, 13 Cal.3d 757 (1975).

28 In addition, the subpoenas are worded so broadly that on their face they encompass even

1 entirely *private* communications and other private account information, such as “Direct Messages”
2 and tweets from accounts that users have chosen to restrict from public view.

3 A district attorney’s decision to prosecute is not an invitation for the government to engage in
4 intrusive fishing expeditions into a criminal defendant’s opinions, beliefs, and interests, let alone the
5 opinions, beliefs, or interests of third parties unconnected to the charged crime other than that they
6 have once uttered the names of defendants or their Twitter accounts. But that is precisely what the
7 government seeks to do here. The motions to quash should be granted because they violate the First
8 Amendment. They should also be granted because they violate the Fourth Amendment insofar as they
9 seek private communications and other information that was never publicly available.

10 II. FACTUAL BACKGROUND

11 Twitter is an online social networking and micro-blogging service. Users can sign up for an
12 account which allows them to exchange messages, called “tweets,” of 140 characters or fewer.
13 Usernames begin with the symbol “@”. Messages are posted to the authoring user’s profile page, and
14 sent to the home page of any Twitter user who has chosen to “follow” that user. A user can “follow”
15 other Twitter users, *i.e.*, become a “follower,” meaning that she will receive the tweets they post.¹

16 As Twitter explains, Twitter “contains information you will find valuable” by allowing users to
17 follow users who tweet about topics of interest; “It’s like being delivered a newspaper whose
18 headlines you’ll always find interesting – you can discover news as it’s happening, learn more about
19 topics that are important to you, and get the inside scoop in real time.”² The list of users someone
20 follows thus provides at least as much information as a magazine or newspaper subscription list.

21 A list of a Twitter user’s followers provides such a rich trove of information that analytics
22 services dedicated to analyzing this information have sprung up. The website followerwonk.com, for
23 example, allows any Twitter user to “[s]lice [his or her] followers into actionable segments” and
24 “[f]ind most influential, dormant, old, and more.”³ Followerwonk can map “the approximate

25 ¹ See [https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-](https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-support/articles/13920-get-to-know-twitter-new-user-faq#)
26 [support/articles/13920-get-to-know-twitter-new-user-faq#](https://support.twitter.com/articles/13920-get-to-know-twitter-new-user-faq#) and
<https://support.twitter.com/articles/14019-faqs-about-following#>

27 ² See [https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-](https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-support/articles/215585-twitter-101-how-should-i-get-started-using-twitter#)
28 [support/articles/215585-twitter-101-how-should-i-get-started-using-twitter#](https://support.twitter.com/articles/215585-twitter-101-how-should-i-get-started-using-twitter#)

³ See <http://followerwonk.com/analyze>.

1 geographic location” and inferred gender, among other things, of a user’s followers.⁴

2 “Following” is not necessarily a mutual relationship. User A’s choice to follow User B is
3 independent of User B’s choice to follow User A. For example, as of December 20, 2012, Bill Gates
4 (“@BillGates”) follows (*i.e.*, subscribes to the tweets of) 147 other Twitter users, but has 9,123,656
5 followers (who subscribe to his tweets).⁵ Thus, following on Twitter is a one-way information stream,
6 unlike “friending” on other social networks like Facebook, where connections are mutual.

7 Twitter users can engage in conversations with each other. A user can reply to another user’s
8 tweet. A reply is known on Twitter as an “@ reply” because the body of an “@reply” begins with the
9 “@username” of the person to whom the reply is made. Similar to an “@ reply” is a “mention.” A
10 “mention” is any tweet “that contains ‘@username’ anywhere in the body of the Tweet”; “this means
11 that @ replies are also considered mentions.”⁶

12 Default account settings make tweets publicly available.⁷ But some communications through
13 Twitter are private. First, users have the ability to protect their accounts, which prevents strangers or
14 uninvited viewers from seeing their tweets. Where a user has chosen to protect her account, other
15 Twitter users can follow her only by requesting and obtaining her approval. Without that approval, the
16 users’ tweets and list of followers and followed users will remain hidden. In other words, a protected
17 account’s tweets are only visible to followers approved by the user. Protected tweets do not appear in
18 a Twitter or Google search.⁸ Second, all users, whether or not they have chosen to protect their
19 accounts, can communicate through a “Direct Message” or “DM.” A DM functions like normal email,
20 and is “private between the sender and recipient.”⁹

21 Twitter also retains information about each account that is not public, such as “Log Data”–
22 *e.g.*, the date, time, and duration of each session in which a user is logged into Twitter – and the

23 _____
24 ⁴ For a sample analysis of Nancy Pelosi’s followers, see <http://followerwonk.com/XjXU>.

25 ⁵ See <https://twitter.com/BillGates>.

26 ⁶ See <https://support.twitter.com/articles/14023-what-are-replies-and-mentions#>.

27 ⁷ A follower subscribes to the tweets of the users they follow; a non-follower can view tweets of users
she does not follow, for example, by searching for tweets containing certain key words or visiting the
twitter profile page of the user, but would not receive them automatically.

28 ⁸ See <https://support.twitter.com/articles/20169886-how-to-protect-and-unprotect-your-tweets#>.

⁹ See <https://support.twitter.com/articles/166337-the-twitter-glossary#d>.

1 Internet Protocol (“IP”) addresses for the computer or device used to access Twitter.¹⁰ An IP address
2 is a unique numerical address that can help to identify individual computers or other devices that are
3 connected to the Internet. *See Office Depot, Inc. v. Zuccarini*, 596 F.3d 696, 698 (9th Cir. 2010).

4 The subpoenas at issue here seek six broad categories of information from Twitter pertaining to
5 each of the two defendants, Lauren Smith and Robert Donohoe, who have each been charged with
6 rioting (Cal. Pen. Code § 404(a)), routing (§ 406), unlawful assembly (§ 407), and wearing a disguise
7 during the commission of a crime (§ 185).¹¹ The categories of information sought are:

- 8 1) Subscriber information for ID @laurenriot/@robbiedonohoe
- 9 2) Photos tweeted by ID @laurenriot/@robbiedonohoe (between January 1, 2012-October 31, 2012)
- 10 3) Mentions of ID @laurenriot/@robbiedonohoe (between January 1, 2012-October 31, 2012)
- 11 4) Tweets by ID @laurenriot/@robbiedonohoe (between January 1, 2012-October 31, 2012)
- 12 5) Followers of ID @laurenriot/@robbiedonohoe
- 13 6) Twitter accounts followed by ID @laurenriot/@robbiedonohoe

14 The declaration in support of each subpoena states that the Twitter “account may contain
15 communications between [Lauren Smith/Robert Donohoe] and the above-named co-defendants that
16 would tend to show that there was a conspiracy or agreement to” commit the charged crimes; “thus,
17 the records or lack thereof are material to the crimes charged.” (Original in all capital letters.)¹²

18 III. ARGUMENT

19 A. THE SUBPOENAS VIOLATE THE FIRST AMENDMENT BECAUSE THEY 20 SEEK EXPRESSIVE AND ASSOCIATIONAL INFORMATION BUT ARE 21 OVERBROAD

22 The subpoenas violate the First Amendment and parallel state constitutional protections¹³
23 because they compel the disclosure of protected expressive and associational information, but are not
24 “narrowly circumscribed” to serve a “‘compelling’ state interest.” *Britt*, 20 Cal.3d at 848-49. These

25 ¹⁰ *See* <https://twitter.com/privacy>.

26 ¹¹ *Amici* do not take a position on whether the Twitter usernames @laurenriot and @robbiedonohoe
27 belong to Defendants Smith and Donohoe, but simply assume for the purposes of this motion that they
28 do, such that tweets by these IDs are speech by Ms. Smith and Mr. Donohoe and tweets about these IDs
are speech about Ms. Smith and Mr. Donohoe.

¹² The subpoenas on Twitter for records pertaining to Ms. Smith and Mr. Donohoe are attached as an
Appendix to this brief, and also attached to the declaration filed by each defendant in support of the
parallel motions to quash. *See* Declaration of Counsel ISO Motion to Quash Prosecution Subpoena
Duces Tecum, filed Dec. 3, 2012, in *People v. Donohoe*, Case No. 12025934 & Declaration of Counsel
ISO Motion to Quash The Subpoena Duces Tecum Issued By the People, filed Nov. 30, 2012, in *People*
v. Smith, Case No. 12025925.

¹³ *See* Cal. Const, art. I, §2 (liberty of speech), §3 (assembly).

1 dragnet subpoenas seek ten months’ of communications by Defendants Smith and Donohoe and by
2 unrelated third parties, potentially including private direct messages and protected tweets. The
3 overbroad subpoenas must be quashed to prevent an unconstitutional chill of First Amendment and
4 state constitutional freedoms.

5 **1. The First Amendment Provides a Qualified Privilege Against Compelled**
6 **Disclosure of Speech and Associational Activity**

7 The First Amendment protects the right of free speech and of association. *See, e.g., NAACP v.*
8 *Alabama*, 357 U.S. 449 (1958). Our Supreme Court has found a qualified First Amendment privilege
9 against inquiry into constitutionally protected activities. In *Britt*, the Court issued a writ of mandate
10 directing the trial court to vacate discovery orders compelling plaintiffs to disclose, *inter alia*,
11 membership lists of political organizations to which they belonged and all “communications [with]
12 any member of your family” or members of the political organizations. *Britt*, 20 Cal.3d at 851. The
13 Court recognized that “compelled disclosure will often deter ... constitutionally protected activities as
14 potently as direct prohibition.” *Id.* at 857. Where an order compels disclosure of information
15 implicating First Amendment freedoms, the “disclosure [must] serve a ‘compelling’ state purpose”
16 and the order “must be drawn with narrow specificity.” *Id.* at 855, 856 (internal quotation marks,
17 citations omitted); *see also Gibson v. Florida Legislative Investigation Comm.*, 372 U.S. 539, 546
18 (1963) (state legislative subpoena could not be enforced: “essential prerequisite to the validity of an
19 investigation which intrudes into the area of constitutionally protected rights of speech [and]
20 association” is “substantial relation between the information sought and a subject of overriding and
21 compelling state interest”). As one court has subsequently explained, “[m]ere relevance is not
22 sufficient”; instead, “the party seeking discovery must make a higher showing of relevance and
23 materiality than otherwise would be required for less sensitive material.” *Rancho Publications*, 68
24 Cal.App.4th at 1549.

25 The trial court discovery orders in *Britt* failed to satisfy this standard for two reasons. First,
26 they compelled disclosure of information pertaining not only to the plaintiffs in the case but also
27 “directly impinge[d] on the constitutional rights of numerous individuals” unrelated “to the underlying
28 lawsuit.” *Britt*, 20 Cal.3d at 858. Second, “even as to the named plaintiffs, the challenged order is

1 likewise impermissibly overbroad.” *Id.* The suit was against an airport for diminution in plaintiffs’
2 property values and other damages caused by operation of the airport. *Id.* at 849. Yet “plaintiffs’
3 constitutionally protected associational activities, even those concerned with protesting airport
4 operations, appear quite unrelated to the matters placed at issue by plaintiffs’ complaints.” *Id.* at 859-
5 60. The Court therefore concluded that the discovery orders “go[] far beyond any limited disclosure
6 that defendant’s legitimate litigation interests may justify.” *Id.* at 852.

7 Disclosure orders must satisfy *Britt* whenever they implicate First Amendment freedoms, and
8 are not triggered solely by speech or associational activities that occur in private. The purpose of
9 *Britt*’s heightened scrutiny is to “safeguard” “constitutionally protected activity ... from governmental
10 interference.” *Id.* “First Amendment freedoms, such as the right of association,” the Court observed,
11 “are protected from attack not only against heavy-handed frontal attack, but also from being stifled by
12 more subtle governmental interference.” *Id.* (citation omitted).

13 Our Supreme Court has made clear that the government can violate free speech protections by
14 surveilling speech that occurs in public settings. In *White*, the plaintiff, a professor at UCLA,
15 challenged the Los Angeles Police Department’s practice of attending classes and preparing reports
16 about classroom discussions. *See White*, 13 Cal.3d at 762. The Court held that “police surveillance of
17 university classrooms and organizations meetings” can impermissibly chill speech, in violation of the
18 free speech protections in the state and federal constitutions, and reversed the trial court’s grant of a
19 demurrer. *Id.* at 767 & n.3. Notably, the Court rejected the defendant’s argument that the
20 “‘semipublic’ nature of a university classroom negates any claim of ‘First Amendment privacy.’” *Id.*
21 at 768 n.4. Although a teacher or student exposes her views to other class members whenever she
22 speaks in class, the Court explained that “such a risk is qualitatively different than that posed by a
23 governmental surveillance system involving the filing of reports in permanent police records.” *Id.*; *cf.*
24 *also Lo-Ji Sales v. New York*, 442 U.S. 319, 329 (1979) (“there is no basis for the notion that because a
25 retail store invites the public to enter, it consents to wholesale searches and seizures [by the
26 government] that do not conform to Fourth Amendment guarantees.”). Federal courts, similarly, have
27 recognized the infringement on First Amendment rights when the government records otherwise
28 public speech. *See, e.g., Community-Serv. Broadcasting of Mid-America, Inc. v. FCC* 593 F.2d 1102,

1 1122 (D.C. Cir. 1978) (requirement that government-funded non-commercial radio stations tape-
2 record public affairs programs for review by FCC unconstitutional because burdened more speech
3 than necessary to serve government’s interests).

4 Courts have thus applied *Britt*’s qualified privilege even when the protected activity occurred
5 in public. For example, in *United Farm Workers of America v. Superior Court*, 170 Cal.App.3d 391
6 (1985), farmers filed suit against a union for damages stemming from a strike, and sought lists of
7 strikers and picketers. Strikers and picketers strike and picket in public, yet the court applied *Britt*,
8 and held that the information should not be released to the plaintiff farmers, absent a more
9 particularized showing of relevance. *Id.* at 395; *cf. also Tylo v. Superior Court*, 55 Cal.App.4th 1379,
10 1387-89 (1997) (applying *Britt*; rejecting claim that celebrity plaintiff waived her right to privacy).

11 **2. The Subpoenas Must Satisfy *Britt* Because They Implicate First**
12 **Amendment Interests.**

13 *Britt* governs the analysis because the subpoenas seek information that squarely implicates the
14 constitutional speech and associational rights of defendants and innumerable third parties.

15 The subpoenas seek information about the speech and associational activities of Defendants
16 Donohoe and Smith, and indeed even that of third parties unrelated to this criminal prosecution. In
17 particular, the subpoenas seek disclosure of all tweets by Defendants Smith and Donohoe (categories 2
18 and 4: photos and tweets by Smith and Donohoe) and all tweets about Defendants by *third parties*
19 (category 3: “mentions of” Smith and Donohoe). In this regard, they resemble the request in *Britt* for
20 all communications between plaintiffs and their family members or other members of the political
21 organizations. *See Britt*, 20 Cal.3d at 850. The subpoenas also seek disclosure of associational
22 information, *viz.*, the people with whom Defendants associate, that is, who they follow, or who follow
23 them (categories 5 and 6: followers of and Twitter accounts followed by). Similarly, category 1 (for
24 subscriber information) implicates associational information, as discussed further below. As such,
25 these requests are similar to the requests for associational information in *Britt* and *UFW*.

26 *Britt* applies even to the extent the information sought was at one time publicly viewable on
27 Twitter. This is so because exposing one’s views and associations to other private citizens is
28 “qualitatively different [from] a governmental surveillance system involving the filing of reports in

1 permanent police records.” *White*, 13 Cal.3d at 768 n. 4. The constitutional interest in preserving the
2 free flow of ideas is at least as important in this context – the internet – as in *White* – the university.
3 *See, e.g., Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997) (recognizing importance
4 of internet as forum for speech); *Krinsky v. Doe*, 159 Cal.App.4th 1154, 1164 (2008) (same). But the
5 danger of chilling expressive activity through use of new technology is far greater than in *White*. By
6 stockpiling ten months’ worth of communications, the government can compile far more
7 comprehensive information about the views, associations, and habits of defendants and third parties
8 through the subpoenas here, than it could possibly have gleaned about the professors and students in
9 *White* by sending police officers into classrooms and meetings. *See also United States v. Garcia*, 474
10 F.3d 994, 998 (7th Cir. 2007) (“Technological progress poses a threat to privacy by enabling an extent
11 of surveillance that in earlier times would have been prohibitively expensive”). Indeed, it was
12 precisely to guard against the danger of “information-amassing practices” that the people of California
13 enacted the Privacy Initiative, now enshrined in Article I, Section 1 of the California Constitution. *See*
14 *Hill v. National Collegiate Athletic Assn.*, 7 Cal.4th 1, 16 (1994) (quoting official ballot pamphlet).

15 Moreover, the subpoena sweeps within its scope private communications. As discussed above,
16 Twitter users can communicate privately, either through protected tweets (which can be viewed only
17 through specifically approved followers) or Direct Messages (akin to private email between two
18 users). Category 3 seeks all “mentions” of Defendants, and thus encompasses communications about
19 Defendants by third parties, including not only public tweets, but also private Direct Messages and
20 protected tweets. Categories 2 and 4 similarly seek photos and tweets by Defendants Smith and
21 Donohoe, and thus could encompass tweets during periods they may have chosen to protect their
22 accounts, as well as private Direct Messages they sent.

23 **3. The Subpoenas Are Not Narrowly Drawn**

24 The subpoenas must be quashed because they are not narrowly tailored.

25 First, Categories 2 and 4 seek photos and tweets by Defendants over a ten-month period,
26 without limitation as to subject matter. Users tweet information on topics ranging from political
27 commentary to social updates. For some heavy Twitter users, their accumulated tweets amount to a
28 virtual diary. While “[m]ere relevance is not sufficient,” *Rancho Publications*, 68 Cal.App.4th at

1 1549, the government has failed to satisfy even the relevance standard. The declaration by the District
2 Attorney in support of the subpoena states only that the Twitter Accounts “*may contain*
3 communications” with co-defendants that would tend to show a conspiracy to commit the charged
4 crimes. (Emphasis added). “Mere speculation as to the possibility that some portion of the records
5 might be relevant to some substantive issue does not suffice.” *Davis v. Superior Court*, 7 Cal.App.4th
6 1008, 1017 (1992) (issuing writ directing trial court to quash subpoena). Defendants are charged with
7 committing various crimes on Columbus Day, October 8, 2012. Yet the subpoenas seek every single
8 tweet, regardless of topic, commencing January 1, 2012, despite the absence in the supporting
9 declaration of any basis for believing that the planning of the alleged crimes in connection with a
10 political protest on a single day commenced nine months earlier. And they also seek every single
11 tweet, regardless of topic, through October 31, 2012, several weeks *after* the alleged crimes had been
12 completed. Like the overbroad subpoenas in *Britt*, the subpoenas here seek information “quite
13 unrelated to the matters placed at issue” in the underlying proceeding. *Britt*, 20 Cal.3d at 859-60.

14 Second, Category 3 seeks all “mentions” of @laurenriot or @robbiedonohoe, also over a ten-
15 month period, and also without limitation to the subject matter of the tweet. This category of
16 information is not narrowly drawn for the same reasons as Categories 2 and 4, but also for an
17 additional reason. It seeks communications by third parties who are not charged with any crime in this
18 matter, potentially including even protected tweets and Direct Messages that were never publicly
19 viewable on Twitter. The declaration in support of the subpoena states that the information sought
20 “may contain communications” between Defendants Smith or Donohoe and their 17 co-defendants.
21 But the subpoenas are not limited to seeking “mentions” of Smith or Donohoe *by the 17 named co-*
22 *defendants*. Instead, they seek “mentions” *by any Twitter user*. This plainly sweeps in far more
23 communication than would serve the government’s stated interest in obtaining evidence of a
24 conspiracy between the co-defendants. By compelling disclosure of these communications by
25 unrelated third parties, the subpoenas are hopelessly overbroad. *See Britt*, 20 Cal.3d at 858 (order
26 “unquestionably overbroad” because compelled disclosure of information pertaining to “numerous
27 individuals who have taken no action whatsoever with respect to the underlying lawsuit”).

28 Third, Category 5 seeks the followers of the Twitter accounts of Ms. Smith and Mr. Donohoe.

1 This category is overbroad for two reasons. First, followers are Twitter users who have chosen to
2 subscribe to another user’s tweets. As a result, a list of followers sheds more light on the choices,
3 preferences, and interests of the followers than the user followed. But the subpoenas are not limited to
4 determining whether the co-defendants were followers of Ms. Smith or Mr. Donohoe; instead, they
5 seek *all* followers, even those who have nothing to do with this criminal prosecution. The
6 government’s interest in obtaining evidence of a conspiracy between the 19 co-defendants does not
7 justify obtaining information about the reading preferences of unrelated third parties. *See Church of*
8 *Hakeem, Inc. v. Superior Court*, 110 Cal.App.3d 384, 390 (1980) (issuing writ directing trial court to
9 nullify order compelling disclosure of membership list “because innocent, non-litigant members are
10 entitled to First Amendment protection no matter what legitimate activities may have been engaged in
11 by the church, its founder, or some few of its member-ministers”). Second, and relatedly, following is
12 a one-way relationship. User A’s choice to follow User B is totally independent of User B’s choice to
13 follow, or not follow, User A. Thus, the “following” relationship lacks the inherent mutuality that is a
14 necessary component of a conspiracy. *See, e.g., People v. Vu*, 143 Cal.App.4th 1009, 1025 (2006) (“a
15 criminal conspiracy may be shown by direct or circumstantial evidence that the parties positively or
16 tacitly came to a *mutual* understanding to accomplish the act and unlawful design”) (emphasis added,
17 citation omitted). As a result, this request cannot satisfy the “higher showing of relevance and
18 materiality” that is necessary here. *Rancho Publications*, 68 Cal.App.4th at 1549.

19 Fourth, Category 6 seeks “Twitter accounts followed by” Defendants Smith and Donohoe. As
20 a threshold matter, it is unclear whether this request seeks only the list of Twitter users followed by
21 Defendants Smith and Donohoe, or *all account information*, including the tweets, of every Twitter
22 user they followed. The latter would plainly be overbroad by sweeping in vast amounts of information
23 belonging to unrelated third parties. *See Britt*, 20 Cal.3d at 858; *Church of Hakeem*, 110 Cal.App.3d
24 at 390. But even if construed only to seek the list of Twitter users followed by Defendants Smith and
25 Donohoe, it would still be unconstitutional.¹⁴ The list of users that someone follows paints a highly
26 textured picture of that person’s likes, interests, and political or religious leanings, among other

27
28 ¹⁴ The fact that a list of users followed may have been publicly viewable does not obviate the need to
satisfy *Britt*. In *United Farm Workers*, the court of appeal applied *Britt* to a discovery request to a union
for lists of strikers and picketers, *see id.* at 395, even though striking and picketing occurs in public.

1 personal information. The Twitter users someone follows may be personal acquaintances, celebrities
2 (@ladygaga), newscasters (@andersoncooper), politicians (@senfeinstein), or political campaigns
3 (@YesOnProp30). Publications of all sorts, ranging from political blogs (@HuffingtonPost) to
4 newspapers (@latimes) and celebrity gossip magazines (@peplemag), have Twitter accounts, as do a
5 slew of organizations ranging the political and issue spectrum (@NRA, @AFLCIO, @Scientology,
6 @TeaPartyExpress, @Sierra_Club). As Twitter itself boasts, it allows users to “learn more about
7 topics that are important to you.”¹⁵ As a result, obtaining the list of Twitters users a person follows
8 allows the government to learn about the topics that are important to that person. But “the First
9 Amendment protects the disclosure of an individual’s “reading, listening, and viewing habits.”
10 *Amazon.com LLC v. Lay*, 758 F. Supp.2d 1154, 1168 (W.D. Wash. 2010) (North Carolina Department
11 of Revenue’s demand that Amazon.com disclose information about customers’ purchases violated
12 First Amendment). First Amendment protections against compelled disclosure are particularly
13 important “where a group espouses dissident beliefs.” *NAACP*, 357 U.S. at 462. The subpoenas do
14 not simply seek to ascertain whether Defendants Smith and Donohoe were “followers” of their co-
15 defendants. Instead, they seek detailed information about their reading preferences which far exceeds
16 any legitimate government interest in obtaining evidence of a conspiracy between the 19 co-
17 defendants. The government cannot make the particularized showing of relevance necessary to obtain
18 this constitutionally sensitive information.

19 Finally, Category 1 seeks “Subscriber information” for Defendants Smith and Donohoe. The
20 subpoenas do not delineate a time period for which the information is sought (other requests seek the
21 information for a ten month period), suggesting that the government seeks subscriber information
22 spanning the entire history of the Twitter accounts. Nor do they define the term “subscriber
23 information,” but the term likely includes the “Log Data” retained by Twitter that reveals information
24 about the date, time, and duration of each session in which a user is logged into Twitter, and the IP
25 address(es) for the computers or devices used to access Twitter.¹⁶ This information could be used to

26 ¹⁵ [https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-](https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-support/articles/215585-twitter-101-how-should-i-get-started-using-twitter#)
27 [support/articles/215585-twitter-101-how-should-i-get-started-using-twitter#](https://support.twitter.com/groups/31-twitter-basics/topics/104-welcome-to-twitter-support/articles/215585-twitter-101-how-should-i-get-started-using-twitter#).

28 ¹⁶ The federal Stored Communications Act defines subscriber information to include, among other things, “local and long distance telephone connection records, or records of session times and durations,” “length of service (including start date) and types of service utilized,” “telephone or

1 map a person’s behavior and associations. For instance, if a Twitter user logs in from her workplace
2 in the morning, a union hall in the afternoon, and the gay and lesbian community center in the
3 evening, she might present three different IP addresses over the course of a single day. The
4 accumulation of such data over time could give the government a surprisingly detailed window into
5 the associations and private habits of a frequent Twitter user. Accordingly, because the information
6 that the District Attorney seeks with Category 1 would tend to reveal Defendants’ “private association
7 affiliations” over the entire time period that subject Twitter accounts were open, such data “are
8 presumptively immune from inquisition.” *See Britt*, 20 Cal.3d at 855. Because the government
9 cannot show a compelling state interest in such a request, especially without temporal limitation, this
10 category, too, fails *Britt*.¹⁷

11
12 **B. THE SUBPOENAS VIOLATE THE FOURTH AMENDMENT BECAUSE**
13 **TWITTER USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN**
14 **PRIVATE COMMUNICATIONS AND ACCOUNT INFORMATION**

15 The subpoenas also violate the Fourth Amendment and state constitutional privacy
16 protections¹⁸ insofar as they seek private Twitter communications and other private account
17 information. The government cannot obtain this information without a warrant.

18 Categories 2, 3, and 4 seek all photos and tweets by or about Defendants Smith and Donohoe
19 over a ten-month period, without limitation as to topic. This broad request covers private forms of
20 communication on Twitter, such as protected tweets or Direct Messages, by defendants and third

21 _____
22 instrument number or other subscriber number or identity, including any temporarily assigned network
23 address,” and “means and source of payment for such service (including any credit card or bank account
24 numbers.” 18 U.S.C. § 2703 (c)(2).

25 ¹⁷ The government is likely to point to the New York County District Attorney’s Office subpoena on
26 Twitter for records pertaining to Malcolm Harris, a criminal defendant. In *People v. Harris*, 36 Misc.3d
27 613 (NY 2012), the court denied Harris’ motion to quash the subpoena on Twitter on standing grounds,
28 analogizing the case to “bank records cases” in which “New York law precludes an individual’s motion
to quash a subpoena seeking the production of the individual’s bank records directly from the third-party
bank.” *Id.* at 616-17. The rule is directly to the contrary in California, in which our Supreme Court has
rejected the so-called “third party doctrine” and held that individuals retain a privacy interest in their
bank records. *See Valley Bank of Nevada v. Superior Court*, 15 Cal.3d 652 (1975) (bank records);
Burrows v. Superior Court, 13 Cal. 3d 238 (1975) (bank records). After the New York court denied Mr.
Harris’ motion to quash on standing grounds, Twitter moved to quash and the court denied the motion
on the merits. *See People v. Harris*, 36 Misc.3d 868 (NY 2012). The court did not address the First
Amendment arguments presented here, and an appeal of that decision is pending.

¹⁸ *See* Cal. Const., art. I, §1 (privacy), §13 (search and seizure).

1 parties. But Twitter users have a legitimate expectation of privacy in protected tweets or Direct
2 Messages because the right to engage in private communications is “one that society is prepared to
3 recognize as ‘reasonable.’” *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J.,
4 concurring). In *Katz*, the Supreme Court held that government eavesdropping on a defendant’s
5 conversation conducted in a public telephone booth constituted a search within the meaning of the
6 Fourth Amendment. *Id.* at 353. As the Court explained:

7 No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person
8 in a telephone booth may rely upon the protection of the Fourth Amendment. One who
9 occupies it, shuts the door behind him, and pays the toll that permits him to place a call is
10 surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to
11 the world. To read the Constitution more narrowly is to ignore the vital role that the public
12 telephone has come to play in private communication.

13 *Id.* at 352 (footnotes omitted). Twitter users who take the affirmative step of protecting their tweets
14 (default account settings render tweets public) or who specifically choose to communicate with other
15 Twitter users through the Direct Messaging function are entitled to assume that their words “will not
16 be broadcast to the world.” *Id.* Protected tweets and Direct Messages are no different from private
17 emails, which, like telephone calls and letters, are clearly entitled to Fourth Amendment protection.
18 *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (“email requires strong protection
19 under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian
20 of private communication, an essential purpose it has long been recognized to serve”). “As some
21 forms of communication begin to diminish, the Fourth Amendment must recognize and protect
22 nascent ones that arise.” *Id.* “To construe the Constitution otherwise “is to ignore the vital role that”
23 Internet communications have come to play in this day and age. *Katz*, 389 U.S. at 352.¹⁹

24 In addition, Category 1 seeks “Subscriber information” which as noted above likely includes
25 “Log Data” retained by Twitter, such as date, time, and duration of each session when a user logs into
26 Twitter and the IP addresses for the computer or device used to access Twitter.²⁰ None of this account

27 ¹⁹ The New York court’s denial of Twitter’s motion to suppress in *Harris* is distinguishable because the
28 court there rejected the Fourth Amendment’s applicability to *public* tweets. *See Harris*, 36 Misc. 3d at
874 (distinguishing public tweet from “a private direct message”).

²⁰ IP addresses can be matched with publicly available databases that “indicate the ‘likely’ locations of
the residences or other venues where defendants used their Internet-connected computers.” *See Sony
Music Ent. Inc. v. Does 1-40*, 326 F. Supp.2d 556, 567 (S.D.N.Y. 2004).

1 information would have been broadcast by a user to the general public. But the user has every right to
2 expect that the details surrounding her internet reading habits, particularly those revealing intimate
3 associations, *see supra* at pages 11-12, should remain private.

4 The fact that the information sought is in the possession of Twitter, a third party, does not
5 mean that Twitter users lack a reasonable privacy expectation. *Cf. Smith v. Maryland*, 442 U.S. 735
6 (1979) (installation of pen register to collect telephone numbers dialed does not violate Fourth
7 Amendment rights of telephone customers); *United States v. Miller*, 425 U.S. 435 (1976) (account
8 holder lacked Fourth Amendment interest in bank records created and maintained by bank in course of
9 financial transactions). The federal “third-party” doctrine does not apply in these circumstances is
10 and, in any event, is not the law in California.

11 The doctrine does not apply to the portions of the subpoena that seek private communications
12 such as Direct Messages and protected tweets. This is so because the third-party doctrine has never
13 applied when the government seeks the content of communications. In *Katz*, the government attached
14 a listening device to a phone booth to intercept and record phone conversations; the Supreme Court
15 found a search, 389 U.S. at 353, even though callers used the telephone company to transmit their
16 conversations. “Letters and other sealed packages are in the general class of effects in which the
17 public at large has a legitimate expectation of privacy,” *United States v. Jacobsen*, 466 U.S. 109, 114
18 (1984), even though senders use the post office or a delivery service to transmit them.

19 Nor does the third-party doctrine apply to private account information (such as “Log Data”),
20 which is transmitted passively and involuntarily by the user. *See United States v. Jones*, 132 S.Ct.
21 945, 957 (2012) (Sotomayor, J., concurring) (doctrine is “ill suited to the digital age, in which people
22 reveal a great deal of information about themselves to third parties in the course of carrying out
23 mundane tasks”). Twitter’s Privacy Policy expressly contemplates that its users retain a privacy
24 interest in their account information and is not intended to interfere with users’ ability to object to
25 government requests for information. *See* Twitter Privacy Policy (“nothing in this Privacy Policy is
26 intended to limit any legal defenses or objections that you may have to a third party’s, including a
27 government’s, request to disclose your information”).²¹

28 ²¹ <https://twitter.com/privacy> (last visited December 19, 2012).

1 The federal “third-party” doctrine cases are inapposite for a separate and independent reason:
2 It is not the law under the California Constitution. The California Supreme Court has repeatedly held
3 that people do not relinquish the privacy of personal information by revealing their affairs to
4 institutions like banks, telephone companies, and credit card companies. *See Valley Bank of Nevada v.*
5 *Superior Court* (1975) 15 Cal.3d 652 (bank records); *Burrows v. Superior Court* (1975) 13 Cal. 3d
6 238 (bank records); *People v. Blair* (1979) 25 Cal. 3d 640 (credit card records and motel telephone
7 calls); *People v. Chapman* (1984) 36 Cal. 3d 98 (unlisted telephone directory information);²² *see also*
8 *People v. McKunes* (1975) 51 Cal. App. 3d 487 (telephone records). The Court held that because bank
9 accounts, hotels, telephones and credit cards are a necessity of participating in modern life, opening
10 accounts with the institutions that control those commodities is not truly volitional. Thus, customers
11 reasonably expect that the personal information compiled will be used solely for account
12 administration, and that the companies which hold records will not release information to law
13 enforcement authorities unless they have obtained valid, judicially-supervised, legal process.
14 Similarly, communicating through the Internet, including through platforms like Twitter, is a
15 ubiquitous feature of modern life. Users reasonably expect that the personal information compiled by
16 platforms like Twitter, to facilitate use of the Internet, will be used solely for that purpose and not
17 disclosed wholesale to the police absent a warrant.

18 IV. CONCLUSION

19 For the foregoing reasons, the court should grant the motions to quash the subpoenas issued by
20 the government to Twitter, Inc.²³

21 ///

22 ///

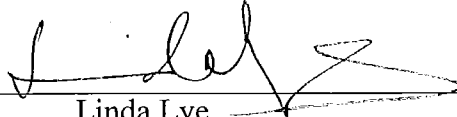
23 ///

24
25
26
27 ²² *Disapproved on other grounds, People v. Palmer*, 24 Cal.4th 856, 861, 864 (2001).

28 ²³ *Amici* respectfully request leave to participate at the hearing on the motions to quash to address the constitutional issues set forth in this brief.

1
2 Dated: December 21, 2012

Respectfully submitted,

3
4 By: 
Linda Lye

5 Linda Lye (Bar No. 215584)
6 AMERICAN CIVIL LIBERTIES UNION
7 FOUNDATION OF NORTHERN CALIFORNIA
8 39 Drumm Street
9 San Francisco, CA 94111
10 Telephone: (415) 621-2493; Fax: (415) 255-8437
11 Email: llye@aclunc.org

Attorneys for amicus American Civil Liberties Union of
Northern California

12 Hanni M. Fakhoury (Bar No. 252629)
13 Nathan D. Cardozo (Bar No. 259097)
14 ELECTRONIC FRONTIER FOUNDATION
15 454 Shotwell Street
16 San Francisco, CA 94110
17 Telephone: (415) 436-9333; Fax: (415) 436-9993
18 Email: hanni@eff.org; nate@eff.org

Attorneys for amicus Electronic Frontier Foundation

19 Aden Fine (Bar No. 186728)
20 AMERICAN CIVIL LIBERTIES UNION
21 FOUNDATION
22 125 Broad Street, 18th Floor
23 New York, NY 10004
24 Telephone: (212) 549-2500
25 Email: afine@aclu.org

Attorneys for amicus American Civil Liberties Union