

1 DURIE TANGRI LLP
RAGESH K. TANGRI (SBN 159477)
2 rtangri@durietangri.com
MICHAEL H. PAGE (SBN 154913)
3 mpage@durietangri.com
217 Leidesdorff Street
4 San Francisco, CA 94111
Telephone: 415-362-6666
5 Facsimile: 415-236-6300

6 Attorneys for *Amicus Curiae*
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE
7 LAWYERS

8
9 IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
10
11 SAN FRANCISCO DIVISION

12 FIRST UNITARIAN CHURCH OF LOS
ANGELES; ACORN ACTIVE MEDIA; BILL
13 OF RIGHTS DEFENSE COMMITTEE;
CALGUNS FOUNDATION, INC.;
14 CALIFORNIA ASSOCIATION OF FEDERAL
FIREARMS LICENSEES, INC.; CHARITY
15 AND SECURITY NETWORK; COUNCIL ON
AMERICAN ISLAMIC RELATIONS-
16 CALIFORNIA; COUNCIL ON AMERICAN
ISLAMIC RELATIONS-OHIO; COUNCIL ON
17 AMERICAN ISLAMIC RELATIONS
FOUNDATION, INC.; FRANKLIN ARMORY;
18 FREE PRESS; FREE SOFTWARE
FOUNDATION; GREENPEACE, INC.;
19 HUMAN RIGHTS WATCH; MEDIA
ALLIANCE; NATIONAL LAWYERS GUILD;
20 NATIONAL ORGANIZATION FOR THE
REFORM OF MARIJUANA LAWS,
21 CALIFORNIA CHAPTER; PATIENT
PRIVACY RIGHTS; PEOPLE FOR THE
22 AMERICAN WAY; PUBLIC KNOWLEDGE;
SHALOM CENTER; STUDENTS FOR
23 SENSIBLE DRUG POLICY; TECHFREEDOM;
and UNITARIAN UNIVERSALIST SERVICE
24 COMMITTEE,

25
26 Plaintiffs,

27 v.

28 NATIONAL SECURITY AGENCY and KEITH

Case No. 3:13-cv-03287-JSW

**BRIEF *AMICUS CURIAE* OF THE
NATIONAL ASSOCIATION OF CRIMINAL
DEFENSE LAWYERS**

Ctrm: 11 - 19th Floor
Judge: Honorable Jeffrey S. White

1 B. ALEXANDER, its Director, in his official and
2 individual capacities; the UNITED STATES OF
3 AMERICA; DEPARTMENT OF JUSTICE and
4 ERIC H. HOLDER, its Attorney General, in his
5 official and individual capacities; Acting
6 Assistant Attorney General for National Security
7 JOHN P. CARLIN, in his official and individual
8 capacities; FEDERAL BUREAU OF
9 INVESTIGATION and JAMES B. COMEY, its
10 Director, in his official and individual capacities;
11 ROBERT S. MUELLER, former Director of the
12 FEDERAL BUREAU OF INVESTIGATION, in
13 his individual capacity; JAMES R. CLAPPER,
14 Director of National Intelligence, in his official
15 and individual capacities, and DOES 1-100,

16
17
18
19
20
21
22
23
24
25
26
27
28
Defendants.

TABLE OF CONTENTS

	Page
I. THE INTEREST OF <i>AMICUS CURIAE</i>	1
II. ARGUMENT.....	1
A. Wholesale Collection Deprives Clients of Their Right to Counsel by Vitiating the Confidentiality of Attorney-Client Communications and Attorney Files.....	1
1. The Strong Protections Afforded to the Confidentiality of Legal Work: Attorney-Client Privilege, Work Product, and Duty of Confidentiality.....	1
2. Bulk Seizure Violates Confidentiality Rules and Impairs the Right to a Defense.....	4
B. The Government’s Current Practices Eviscerate FISA’s Relevance and Minimization Requirements.....	6
III. CONCLUSION.....	11

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

Page(s)

Cases

Gonzalez v. United States,
553 U.S. 242 (2008).....3

Hickman v. Taylor,
329 U.S. 495 (1947).....1, 2

Marquez v. Miranda,
No. C 92-3934 FMS, 1998 WL 57000 (N.D. Cal. Jan. 28, 1998).....3

Maryland v. King,
133 S. Ct. 1 (2012).....7

Padilla v. Kentucky,
130 S. Ct. 1473 (2010).....3

Roe v. Flores-Ortega,
528 U.S. 470 (2000).....3

Rompilla v. Beard,
545 U.S. 374 (2005).....3

Swidler & Berlin v. United States,
524 U.S. 399 (1998).....1, 2

X Corp. v. Doe,
805 F. Supp. 1298, 1307-10 (E.D. Va. 1992),
aff'd mem., 17 F.3d 1435 (4th Cir. 1994)2

Statutes

50 U.S.C. § 1801(a)9

50 U.S.C. § 1801(b)9

50 U.S.C. § 1801(h)10

50 U.S.C. § 186110

Other Authorities

124 Cong. Rec. 34,845 (1978).....9

124 Cong. Rec. 35,389 (1978).....9

*5 Intelligence Activities: Hearings on S. Res. 21 Before the Select Comm. to Study
Governmental Operations with Respect to Intelligence Activities of the United States*,
94th Cong. 9 (1975)8, 9

ABA STANDARDS FOR CRIMINAL JUSTICE, DEFENSE FUNCTION 4-3.1 (3d ed. 1993).....3

1 Adam Liptak, *Justices Wrestle Over Allowing DNA Sampling at Time of Arrest*, N.Y.
2 TIMES (Feb. 26, 2013).....7
3 Barton Gellman, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden*
4 *documents say*, WASHINGTON POST, (Oct. 30, 2013)7
5 H.R. REP. NO. 95-1283 (1978).....10
6 Minimization Procedures Used By the NSA in Connection With Acquisitions of Foreign
7 Intelligence Information Pursuant to Section 702 of the Foreign Intelligence
8 Surveillance Act of 1978, as Amended (July 1, 2008)8
9 **Rules**
10 ABA MODEL RULES OF PROF’L CONDUCT R. 1.6 (1983)2
11 **Constitutional Provisions**
12 U.S. CONST. amend. VI.....6
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 **I. THE INTEREST OF *AMICUS CURIAE***

2 Amicus National Association of Criminal Defense Lawyers (“NACDL”) is a nonprofit voluntary
 3 professional bar association that works on behalf of criminal defense attorneys to ensure justice and due
 4 process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide
 5 membership of approximately 10,000 and up to 40,000 with affiliates. NACDL’s members include
 6 private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges.
 7 NACDL is the only nationwide professional bar association for public defenders and private criminal
 8 defense lawyers. The American Bar Association recognizes NACDL as an affiliated organization and
 9 awards it full representation in its House of Delegates.

10 NACDL files numerous amicus briefs each year in the United States Supreme Court and other
 11 courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal
 12 defendants, criminal defense lawyers, and the criminal justice system as a whole. Of particular relevance
 13 here, the surveillance challenged in this action poses a direct, concrete threat to the right of association
 14 and confidentiality that is critical to an effective defense in criminal cases. NACDL has therefore
 15 decided to present its views for the Court’s consideration.¹

16 **II. ARGUMENT**

17 **A. Wholesale Collection Deprives Clients of Their Right to Counsel by Vitiating the**
 18 **Confidentiality of Attorney-Client Communications and Attorney Files**

19 **1. The Strong Protections Afforded to the Confidentiality of Legal Work:**
 20 **Attorney-Client Privilege, Work Product, and Duty of Confidentiality**

21 Keeping a client’s information confidential is among a lawyer’s most fundamental duties. The
 22 principle of confidentiality manifests itself in the attorney-client privilege, “one of the oldest recognized
 23 privileges for confidential communications.” *Swidler & Berlin v. United States*, 524 U.S. 399, 403
 24 (1998). It finds expression in the work-product doctrine, recognized by the Supreme Court sixty-six
 25 years ago in *Hickman v. Taylor*, 329 U.S. 495 (1947). And the American Bar Association Model Rules
 26 of Professional Conduct, on which lawyers’ ethics codes in most states are based, prohibit attorneys from
 27 “reveal[ing] information relating to the representation of a client” absent the client’s consent, except

28 ¹ The Government has consented to the filing of this brief, while reserving the right to object on other grounds.

1 under narrowly circumscribed conditions. ABA MODEL RULES OF PROF'L CONDUCT ("MRPC") R. 1.6(a)
2 (1983).

3 Confidentiality serves crucial functions in the American legal system. In the context of litigation,
4 the Supreme Court has found that:

5 [I]t is essential that a lawyer work with a certain degree of privacy, free
6 from unnecessary intrusion by opposing parties and their counsel. Proper
7 preparation of a client's case demands that he assemble information, sift
8 what he considers to be the relevant from the irrelevant facts, prepare his
9 legal theories and plan his strategy without undue and needless
10 interference.

11 *Hickman*, 329 U.S. at 510-11. Similarly, the protections of the attorney-client privilege "encourage full
12 and frank communication between attorneys and their clients and thereby promote broader public
13 interests in the observance of law and the administration of justice." *Swidler & Berlin*, 524 U.S. at 403
14 (internal quotation marks omitted).

15 Confidentiality also serves important interests outside the context of litigation. The ethical
16 prohibition on "reveal[ing] information relating to the representation of a client" is broader than the
17 attorney-client privilege and the attorney work-product doctrine. *See, e.g., X Corp. v. Doe*, 805 F. Supp.
18 1298, 1307-10 (E.D. Va. 1992) (explaining difference between attorney-client privilege and duty of
19 confidentiality), *aff'd mem.*, 17 F.3d 1435 (4th Cir. 1994); MRPC R. 1.6 cmt. 3 ("The rule of client-
20 lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer
21 through compulsion of law."). The ethical duty of confidentiality:

22 [C]ontributes to the trust that is the hallmark of the client-lawyer
23 relationship. The client is thereby encouraged to seek legal assistance and
24 to communicate fully and frankly with the lawyer even as to embarrassing
25 or legally damaging subject matter. The lawyer needs this information to
26 represent the client effectively and, if necessary, to advise the client to
27 refrain from wrongful conduct. Almost without exception, clients come to
28 lawyers in order to determine their rights and what is, in the complex of
laws and regulations, deemed to be legal and correct. Based upon
experience, lawyers know that almost all clients follow the advice given,
and the law is upheld.

MRPC R. 1.6 cmt. 2.

The duty of confidentiality has particular significance for criminal defense lawyers. The
American Bar Association's Standards for Criminal Justice, to which the courts have looked often in

1 determining the professional duties of criminal defense lawyers,² emphasize the importance of protecting
2 the client's confidentiality. Standard 4-3.1(a) provides that "[d]efense counsel should seek to establish a
3 relationship of trust and confidence with the accused," and it adds: "Defense counsel should explain the
4 necessity of full disclosure of all facts known to the client for an effective defense, and defense counsel
5 should explain the extent to which counsel's obligation of confidentiality makes privileged the accused's
6 disclosures." ABA STANDARDS FOR CRIMINAL JUSTICE, DEFENSE FUNCTION 4-3.1(a) (3d ed. 1993)
7 ("ABA STANDARDS"). The Commentary explains that "[n]othing is more fundamental to the lawyer-
8 client relationship than the establishment of trust and confidence. Without it, the client may withhold
9 essential information from the lawyer. Thus, important evidence may not be obtained, valuable defenses
10 neglected, and, perhaps most significant, defense counsel may not be forewarned of evidence that may be
11 presented by the prosecution." ABA STANDARDS 4-3.1 cmt.

12 The Standards (and relevant case authority from this District) address a circumstance analogous
13 to the surveillance at issue here. Standard 4-3.1(b) provides that "[t]o ensure the privacy essential for
14 confidential communication between defense counsel and client, adequate facilities should be available
15 for private discussions between counsel and accused in jails, prisons, courthouses and other places where
16 accused persons must confer with counsel." ABA STANDARDS 4-3.1(b). The Commentary declares: "It
17 is fundamental that the communication between client and lawyer be untrammelled. The reading by
18 prison officials of correspondence between prisoners and their lawyers inhibits communication and
19 impairs the attorney-client relationship, may compel time-consuming and expensive travel by the lawyer
20 to assure confidentiality, or even prevent legitimate grievances from being brought to light." *Id.* cmt.
21 *See also* *Marquez v. Miranda*, No. C 92-3934 FMS, 1998 WL 57000, at *2-3 (N.D. Cal. Jan. 28, 1998)
22 (holding that prison guards' practice of conducting brief "scans" of prisoner's legal mail violated
23 prisoner's rights under First and Sixth Amendments because of "potential chilling effect" of such review
24 which "renders[] the prisoner less willing or able to raise substantial legal issues.").

25
26
27
28 ² *See, e.g., Padilla v. Kentucky*, 130 S. Ct. 1473, 1482 (2010); *Gonzalez v. United States*, 553 U.S. 242,
249 (2008); *Rompilla v. Beard*, 545 U.S. 374, 387 (2005); *Roe v. Flores-Ortega*, 528 U.S. 470, 479
(2000).

1 Defense counsel and other attorneys, in short, have a unique obligation to ensure the
2 confidentiality of their communications with, and on behalf of, their clients, and to avoid—sometimes at
3 considerable cost and effort—employing means of communication that may compromise that
4 confidentiality. But today, for the first time, we are confronted with a legal regime in which there are no
5 longer *any* secure alternatives: A regime in which details of virtually every attorney-client
6 communication are not merely at *risk* of being intercepted, retained, and reviewed, but in which details of
7 all of those communications are *in fact* being seized and retained.

8 **2. Bulk Seizure Violates Confidentiality Rules and Impairs the Right to a** 9 **Defense**

10 As the Complaint and briefing by the parties make clear, and as the Government has conceded,
11 the NSA’s indiscriminate collection of telephony records is almost *literally* comprehensive: for years, it
12 has collected and stored records of nearly every single telephone call made via every major service
13 provider in America. Those records are not limited to merely a list of phone numbers called, but a wealth
14 of data including the time and duration of each call, the IMSI and/or IMEI identifiers of the devices, the
15 trunk identifier, telephone calling card numbers, and locations of mobile devices. Those records have
16 been seized without any particularized showing that any of the participants are implicated in or suspected
17 of any wrongdoing whatsoever, on the basis that—somewhere within that haystack of billions of
18 innocent transactions—there may be a needle of data related to possible terrorist activity. As a result, the
19 Government contends, the phone records of *every* American citizen are subject to seizure as “relevant” to
20 terrorist activity. As discussed below, the Government’s “relevance” theory is unbounded, as it could
21 just as easily justify the seizure of *any* universe of information (such as, for example, mass quantities of
22 documents stored in Google or Yahoo’s “clouds”) on the theory that searching that universe might yield
23 data that could have been (but was not) legitimately sought. That theory was expressly rejected by
24 Congress in enacting the Foreign Intelligence Surveillance Act (“FISA”) provisions challenged herein,
25 which were enacted specifically to rein in prior wholesale surveillance.

26 The wholesale seizure and retention of telephony data by law enforcement agencies, without any
27 showing of particularized cause, is of particular concern to defense counsel. Consider, for example, a
28 few hypotheticals. The first is familiar to all law students from Crim 101: your client comes to you,

1 admits to a shooting, hands you the weapon, and asks you what to do with it. Your obligations are well
2 established: the communication from your client is sacrosanct, but your obligation as an officer of the
3 court is to deliver the weapon to the police as evidence without disclosing attorney-client
4 communications in the process.

5 But now imagine that the authorities to whom you must deliver that weapon have access to a
6 database containing a record of every phone call to and from your office in the 24 hours before your
7 client's visit: records that include the number and device identification of caller, the time and length of
8 the call, the location from which the call was placed, and the like. Assuming your client called in
9 advance of his visit, it should be short work for a competent detective, armed with that data, to deduce
10 his identity. The attorney-client privilege on which he relied in coming to you is now of no value.

11 Similarly, imagine a client who retains you to defend him shortly after his arrest for any crime, no
12 matter how far afield from terrorist activity: insider trading, for example. The bare details of your phone
13 calls after your initial meeting, even without knowing the content of those calls, will reveal a wealth of
14 data that is—or should be—covered by both the attorney-client privilege and the work product doctrine.
15 Who are the co-conspirators? The fact witnesses? The alibi witnesses? The nontestifying experts you
16 retained? The testifying experts you do not yet have to disclose? Without any cause, and in derogation
17 of centuries-old, basic principles of justice and due process, the government already has that list.

18 The Government's position—that it somehow hasn't actually seized a citizen's information until
19 and unless it queries or reads it—would be absurd in any other context. Imagine an indiscriminate police
20 seizure of all of the paper files in an attorney's office. No court in the land would deny a motion to
21 return those papers by accepting the prosecution's argument that "it's okay, we haven't read them yet,
22 but we might need them in a later investigation." There is no reason why the bounds of Constitutional
23 protections are different when the data is electronic.

24 Finally, consider the NSA's wholesale collection from the potential client's point of view. As set
25 forth in Plaintiffs' motion, each Plaintiff's First Amendment right to free association is chilled and
26 constrained by the NSA's actions. But for citizens seeking legal advice, either in defense of past actions
27 (charged or uncharged) or as to the legality of contemplated actions, the United States Constitution
28 embodies and protects as sacrosanct a much more specific right of association: "to have the Assistance

1 of Counsel for his defence.” U.S. CONST. amend. VI. Now consider the chilling effect on that
2 fundamental right in the case of a citizen who has allegedly committed a crime, or is simply considering
3 a course of action, the legality of which he is unsure. He should call a lawyer, and seek counsel. But if
4 the cost of doing so is to inform the Government that he is seeking the counsel of an attorney known to
5 specialize in his particular problem, how less likely is he to do so? And how much worse off are both he
6 and society as a result of that reluctance? In a world where every reasonable modern method of
7 communication is apparently subject to routine mass seizure by the Government, the right to consult with
8 counsel, under the protection of the attorney-client privilege, simply disappears.

9 Plaintiffs’ motion is replete with examples of the chilling effect the NSA’s telephony program has
10 on people who are thereby reluctant to seek suicide counseling, or telephone fellow Muslims, or join in
11 advocating political causes. Those effects are at least matched by the chilling effect on both First and
12 Sixth Amendment rights to associate with one’s counsel of choice, knowing that the very exercise of
13 those rights may inform the Government of one’s identity and one’s need for an attorney.

14 **B. The Government’s Current Practices Eviscerate FISA’s Relevance and**
15 **Minimization Requirements**

16 The Government claims authority for its unlimited seizure of billions of telephony records of
17 ordinary citizens, with no showing of cause, under Section 215 of the Patriot Act, notwithstanding that
18 Section’s express limitation to seizure of tangible items “relevant to an authorized investigation.” That
19 limitation, according to the Government, is wholly illusory: “the relevance standard provides the
20 Government with broad authority to collect data that is necessary to conduct authorized investigations.”
21 Administration White Paper at 15, ECF No. 25-11. This purported “broad authority,” the Government
22 claims, represents “the balanced scheme that Congress adopted when it joined the broad relevance
23 standard with the requirement for judicial approval set forth in Section 215.” *Id.*

24 There are four fundamental problems with this argument. *First*, it knows no bounds: it defines as
25 “relevant” *any* universe of data, even data that does not yet exist, so long as there is a possibility that
26 possession of that universe might someday make it easier for the Government to locate actually relevant
27 data within it. The exception swallows the rule. It would be much easier to catch criminals if the police
28 could simply record every phone call, and then search through them for the few that constitute evidence

1 once they have a particular crime to solve. It would be much easier to deter crime if the authorities could
 2 place video and audio recording devices in every home, and tracking devices on every citizen. Within
 3 that universe of information, there would surely be evidence relevant to multiple crimes. But utility and
 4 efficiency do not trump Constitutional rights. As Justice Scalia noted during oral argument in *Maryland*
 5 *v. King*, 133 S. Ct. 1 (2012):

6 Well that's really good. I'll bet you if you conducted a lot of unreasonable
 7 searches and seizures, you'd get more convictions, too. That proves
 8 absolutely nothing.³

9 Any sufficiently large mass of data inevitably will include *some* evidence relevant to *some* crime,
 10 and thus by the Government's logic may be gathered wholesale.⁴ Indeed, recent reports confirm that this
 11 logic has been applied far beyond just telephony metadata, including bulk warrantless collection of
 12 hundreds of millions of entire documents from the online "cloud" storage systems of Google and Yahoo!.
 13 *See* Barton Gellman, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents*
 14 *say*, WASHINGTON POST, (Oct. 30, 2013).⁵ That wholesale invasion cannot be justified on the basis that,
 15 somewhere in the millions of seized documents, there may be evidence.⁶

16 *Second*, the Government's claim of "balance" turns the process on its head: the point of the
 17 system of FISA courts and warrants is to require a showing of relevance *before* the Government can
 18 execute a seizure. That showing has been reduced to nothing more than a promise (often broken) not to
 19 look too closely at the data once seized. The current system seizes first, and justifies (if at all) later.

20 ³ Adam Liptak, *Justices Wrestle Over Allowing DNA Sampling at Time of Arrest*, N.Y. TIMES (Feb. 26,
 21 2013), <http://www.nytimes.com/2013/02/27/us/supreme-court-hears-arguments-on-dna-sampling.html>
 (last visited Nov. 13, 2013).

22 ⁴ As the nation's foremost association of criminal defense lawyers, Amicus NACDL has a particular
 23 interest in preventing the dilution of the relevance standard that the government seeks to work here. As
 24 Plaintiffs' brief explains, FISA's relevance standard is tied to the scope of a permissible grand jury
 subpoena. Pls.' Br. Summ. J. 9:18-26, Nov. 6, 2013, ECF No. 24. If the government can prevail in
 stripping that standard of meaning here, then one can expect the government next will cite *this* decision
 the next time it must respond to a challenge to an overbroad grand jury subpoena.

25 ⁵ [http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html)
 26 [centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html)
[d89d714ca4dd_story.html](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html) (last visited Nov. 11, 2013).

27 ⁶ This revelation is particularly chilling to any of the millions of citizens who rely on these commercial
 28 document storage systems to store and edit many of their business and personal records. Those citizens
 include NACDL attorneys, many of whom are solo practitioners or practice in firms too small to have
 their own servers and document systems.

1 *Third*, although the Government purports to protect innocent citizens’ data through after the fact
 2 “minimization” procedures, we have no way to assess that claim, as those procedures themselves remain
 3 classified. While the minimization provisions under Section 702 have been declassified,⁷ the Section
 4 215 provisions have not. But if the Section 215 procedures are anything like those used under Section
 5 702, they are plainly inadequate to protect attorney-client privilege, work-product protection, or the right
 6 to counsel. The Section 702 minimization protocols prohibit the acquisition and processing of attorney-
 7 client communications *only* when “it becomes apparent that a communication is between a person who is
 8 known to be *under criminal indictment in the United States* and an attorney who represents that
 9 individual” *Id.*, Section 4 (emphasis added). Any other attorney-client communications are fair
 10 game, and entirely unprotected. And even for the tiny subset of attorney-client communications to and
 11 from clients who are actually under U.S. indictment, those communications may still be “reviewed by the
 12 NSA Office of General Counsel prior to dissemination.” *Id.*

13 And *fourth*, the Government’s claim that the current regime represents a “scheme that Congress
 14 adopted” when enacting FISA is made up out of whole cloth. FISA was enacted precisely to *curb* the
 15 prior round of NSA excesses, when it was revealed that the NSA had been illegally collecting domestic
 16 communications of tens of thousands of U.S. citizens in the Sixties and Seventies. As Senator Frank
 17 Church explained in the hearings that resulted in the creation of FISA:

18 In the case of the NSA, which is of particular concern to us today, the rapid
 19 development of technology in the area of electronic surveillance has
 20 seriously aggravated present ambiguities in the law. The broad sweep of
 21 communications interception by NSA takes us far beyond previous fourth
 amendment controversies where particular individuals and specific
 telephone lines were the target.

22 *5 Intelligence Activities: Hearings on S. Res. 21 Before the Select Comm. to Study Governmental*
 23 *Operations with Respect to Intelligence Activities of the United States*, 94th Cong. 9 (1975) (“Church
 24 Committee Report, Vol. 5”), at 65 (statement of Senator Frank Church, Chairman, Select Comm. to
 25

26 ⁷See *Minimization Procedures Used By the NSA in Connection With Acquisitions of Foreign*
 27 *Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as*
 28 *Amended* (July 1, 2008), <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20C%20connection%20with%20FISA%20SECT%20702.pdf> (last visited Nov. 13, 2013).

1 Study Governmental Operations with Respect to Intelligence Activities of the United States of the United
2 States Senate).

3 Then, as now, the NSA sought to justify its bulk collection on the basis that any collection of
4 irrelevant communications was *subsequently* filtered out: General Lew Allen testified that, although the
5 interception was “conducted in such a manner as to minimize the unwanted messages,” the agency
6 nonetheless obtained many unwanted and irrelevant messages. *Id.* at 9. He explained that “[t]he analysis
7 and reporting is accomplished only for those messages which meet specified conditions and requirements
8 for foreign intelligence,” and that “[t]he use of lists of words, including individual names, subjects,
9 locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence
10 value from that which is not of interest.” *Id.* at 9-10.

11 The Church Committee and Congress rejected that “vacuum cleaner” approach to foreign
12 intelligence gathering. Instead, FISA was drafted with a series of specific requirements designed to stop
13 the wholesale invasion of privacy conducted in the name of foreign security. As Senator Edward
14 Kennedy (D-MA) explained at the time: “The abuses of recent history sanctioned in the name of national
15 security highlighted the need for this legislation.” 124 Cong. Rec. 34,845 (1978). Senator Birch Bayh,
16 Jr. (D-IN) echoed Kennedy’s sentiments: “This bill, for the first time in history, protects the rights of
17 individuals from government activities in the foreign intelligence area.” *Id.* Senator Charles Mathais (R-
18 MD) noted that enactment of the legislation would be a milestone, ensuring “that electronic surveillance
19 in foreign intelligence cases will be conducted in conformity with the principles set forth in the fourth
20 amendment.” *Id.* at 35,389.

21 To that end, FISA included a series of protections and requirements designed specifically to stop
22 wholesale fishing expeditions. First, it required a showing that the target of the surveillance was a
23 foreign power or agent of a foreign power *prior* to orders being issued to intercept communications. 50
24 U.S.C. § 1801(a). Second, FISA incorporated a probable cause standard that must be satisfied in order to
25 find that a target is an “agent of a foreign power” for FISA warrant purposes. That definition required
26 not merely that the target be acting on behalf of a foreign power, but that the act at issue be illegal (i.e.,
27 either espionage, terrorism, sabotage, or acts in furtherance of such crimes). 50 U.S.C. § 1801(b). As the
28 House of Representatives explained at the introduction of FISA:

1 This standard requires the Government to establish probable cause that the
 2 prospective target knows both that the person with whom he is conspiring
 3 or whom he is aiding and abetting is engaged in the described activities as
 4 an agent of a foreign power and that his own conduct is assisting or
 5 furthering such activities. The innocent dupe who unwittingly aids a
 6 foreign intelligence officer cannot be targeted under this provision.

7 H.R. REP. NO. 95-1283, pt. 1 at 44 (1978).

8 And third, FISA incorporated an express obligation to “minimize” not just the *use* but the
 9 *acquisition and retention* of communications:

10 “Minimization procedures”, with respect to electronic surveillance,
 11 means— (1) specific procedures, which shall be adopted by the Attorney
 12 General, that are reasonably designed in light of the purpose and technique
 13 of the particular surveillance, to *minimize the acquisition and retention*,
 14 and prohibit the dissemination, of nonpublicly available information
 15 concerning unconsenting United States persons

16 50 U.S.C. § 1801(h). This provision was enacted in response to, and specifically rejected, the NSA’s
 17 position at the time that excessive and improper *acquisition* of data could be cured by *subsequent* sorting
 18 of that data based on keywords or other technological means. Under FISA, minimization is a
 19 *prerequisite* to the issuance of a warrant, not a palliative to be applied, after the fact and after FISA court
 20 review and approval, as the NSA sees fit.

21 The enactment of the Patriot Act did not change these fundamental principles. Even if one
 22 accepts the Government’s assertion that telephony records are “tangible things” subject to Section 215—
 23 and, as briefed by the parties, they plainly are not—the Patriot Act’s expansion of FISA included
 24 substantially the same principles: the “tangible things” sought must be “relevant to an authorized
 25 investigation,” and the relevance standard of Section 215 is based on whether the identified target is “a
 26 foreign power or agent of a foreign power,” the “activities of a suspected agent,” or “an individual in
 27 contact with” such an agent. Moreover, just as in the original FISA, Section 215 requires minimization
 28 procedures that limit not just the use but the “*retention . . . of nonpublicly available information*
 concerning unconsenting United States persons” 50 U.S.C. § 1861. Minimization of *retention*, not
 just use or dissemination, is thus a prerequisite to issuance of Section 215 warrants as well.

And yet we have now come full circle. Thirty-five years later, the Government defends the
 current program in precisely the same terms that Congress rejected in fashioning FISA’s rules, arguing

1 again that relevance and minimization limit only the permissible *use* of indiscriminately collected mass
 2 data, not the *collection* and *retention* of that data in the first place. Nothing in the law supports that view,
 3 and the history of FISA’s enactment makes clear that—to the contrary—Congress crafted both FISA and
 4 the Patriot Act expressly to prohibit the “seize the haystack and then look for the needle” approach the
 5 NSA again advocates.

6 **III. CONCLUSION**

7 Mass indiscriminate seizure of telephony records has no basis in the law, and impermissibly
 8 impinges on the First Amendment right of free association, as well as the Fourth and Fifth Amendments.
 9 Each of the named Plaintiff groups suffers these chilling effects. But for criminal defense counsel and
 10 their clients in particular, the NSA’s program also impinges on the Sixth Amendment right to counsel.
 11 That right means little if the very act of consulting with the counsel of one’s choice places the fact and
 12 details of that consultation, and all subsequent communications by both attorney and client, in the hands
 13 of the Government.

14 Dated: November 18, 2013

DURIE TANGRI LLP

15
 16 Of Counsel:

By: /s/ Michael H. Page

RAGESH K. TANGRI
 MICHAEL H. PAGE

17 David M. Porter, CA State Bar #127024
 18 9th Circuit Vice-chair, NACDL Amicus Committee
 19 801 I Street, 3rd Floor
 20 Sacramento, CA 95814
 Telephone: (916) 498-5700
 Facsimile: (916) 498-5710
 E-mail: david_porter@fd.org

Attorneys for *Amicus Curiae*
 NATIONAL ASSOCIATION OF CRIMINAL
 DEFENSE LAWYERS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I certify that all counsel of record who has consented to electronic notification is being served on November 18, 2013 with a copy of this document via the Court’s CM/ECF system. I further certify that I mailed the foregoing document and the notice of electronic filing by first-class mail to all non-CM/ECF participants.

/s/ Michael H. Page
MICHAEL H. PAGE