

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

Jennifer M. Urban (SBN 209845)  
jurban@law.berkeley.edu  
SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC  
UNIVERSITY OF CALIFORNIA,  
BERKELEY, SCHOOL OF LAW  
396 Simon Hall  
Berkeley, CA 94720-7200  
Telephone: (510) 684-7177  
Facsimile: (510) 643-4625

Attorneys for *Amici Curiae*  
EXPERTS IN THE HISTORY OF  
EXECUTIVE SURVEILLANCE: JAMES  
BAMFORD, LOCH JOHNSON, AND PETER  
FENN

**UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION**

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

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

)  
) **EXPERTS IN THE HISTORY OF**  
) **EXECUTIVE SURVEILLANCE’S MOTION**  
) **FOR LEAVE TO FILE BRIEF *AMICUS***  
) ***CURIAE* IN SUPPORT OF PLAINTIFFS’**  
) **MOTION FOR PARTIAL SUMMARY**  
) **JUDGMENT**

) Courtroom 11, 19th Floor  
) Hon. Jeffrey S. White  
)  
)

1 **TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:**

2 PLEASE TAKE NOTICE that the undersigned proposed *Amici Curiae* will and hereby  
3 do move the Court for leave to appear and file the accompanying proposed brief supporting  
4 Plaintiffs in this litigation. Plaintiffs consent to and Defendants do not oppose—but reserve the  
5 right to object on other grounds as appropriate—the filing of this brief.

6 **I. Statement of Interest of *Amici Curiae***

7 The proposed *amici*'s sole interest is to assist this Court in applying Section 215 of the  
8 USA PATRIOT Act by illuminating similarities between the ongoing bulk telephone records  
9 surveillance at issue here and the government's past surveillance activities. *Amici* derive their  
10 expertise from decades of research and from direct experience with executive surveillance  
11 programs and oversight structures.

12 James Bamford served as an intelligence analyst with the United States Navy. In 1982 he  
13 published *The Puzzle Palace*, the first comprehensive history of the National Security Agency  
14 ("NSA"). In three subsequent books and numerous articles he has chronicled the activities of the  
15 NSA from its inception, through the post-9/11 era, to the present day. He is the foremost  
16 historian of the NSA.

17 Loch Johnson served as special assistant to the chair of the Church Committee—which  
18 conducted a comprehensive review of American intelligence programs—and as staff director of  
19 the House Subcommittee on Intelligence Oversight. He also worked with the Chair of the Aspin-  
20 Brown Commission on Intelligence. He is currently Regents Professor of Political Science at the  
21 University of Georgia and the editor of *Intelligence and National Security*.

22 Peter Fenn served as Washington Chief of Staff for Senator Frank Church from and on  
23 the staff of the Senate Intelligence Committee.

24 **II. Issues Addressed by Movants in the Brief**

25 *Amici* seek leave to file the attached *amicus curiae* brief to explain how direct historical  
26 patterns illuminate the inherent dangers in the government's interpretation of Section 215 as a  
27

1 grant of expansive power to the executive to determine the parameters of its surveillance of  
2 Americans.

3 As experts in the history of executive surveillance programs, *amici* are uniquely qualified  
4 to assist the Court in this way. In the brief, *amici* explain patterns from the mid-twentieth  
5 century's era of poorly supervised surveillance that resulted in abusive targeting of  
6 constitutionally protected activities and how these patterns have reemerged in recent years.

7 *Amici* therefore believe the attached brief will help the Court in properly applying Section  
8 215's relevance requirement. They explain that this requirement should be given its natural  
9 reading as a check on, rather than a license for, expansive executive surveillance powers.

10 **CONCLUSION**

11 For the above reasons, *amici* respectfully request this Court's leave to submit the  
12 accompanying brief attached as Exhibit A.

13 Dated: November 15, 2013

14 By: /s/ Jennifer M. Urban

15 Jennifer M. Urban, Esq.  
16 SAMUELSON LAW, TECHNOLOGY  
17 & PUBLIC POLICY CLINIC  
18 UNIVERSITY OF CALIFORNIA,  
19 BERKELEY, SCHOOL OF LAW  
20 396 Simon Hall  
21 Berkeley, CA 94720-7200  
22 Telephone: (510) 684-7177  
23 Facsimile: (510) 643-4625

24 Attorney for *Amici Curiae*  
25 EXPERTS IN THE HISTORY OF  
26 EXECUTIVE SURVEILLANCE:  
27 JAMES BAMFORD, LOCH  
28 JOHNSON, AND PETER FENN

# **EXHIBIT A**

Jennifer M. Urban (SBN 209845)  
jurban@law.berkeley.edu  
SAMUELSON LAW, TECHNOLOGY &  
PUBLIC POLICY CLINIC  
UNIVERSITY OF CALIFORNIA,  
BERKELEY, SCHOOL OF LAW  
396 Simon Hall  
Berkeley, CA 94720-7200  
Telephone: (510) 684-7177  
Facsimile: (510) 643-4625

Attorney for *Amici Curiae*  
EXPERTS IN THE HISTORY OF  
EXECUTIVE SURVEILLANCE: JAMES  
BAMFORD, DR. LOCH JOHNSON, AND  
PETER FENN

On the Brief:  
*Clinical Students*  
Charles Crain  
Samia Hossain  
Jesse Koehler

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*,  
  
Plaintiffs,  
  
v.  
  
NATIONAL SECURITY AGENCY, *et al.*,  
  
Defendants.

) Case No.: 3:13-cv-03287 JSW  
)  
) **BRIEF *AMICUS CURIAE* OF EXPERTS**  
) **IN THE HISTORY OF EXECUTIVE**  
) **SURVEILLANCE: JAMES BAMFORD,**  
) **LOCH JOHNSON, AND**  
) **PETER FENN**  
)  
) Courtroom 11, 19th Floor  
) Hon. Jeffrey S. White  
)

**TABLE OF CONTENTS**

1 **TABLE OF AUTHORITIES**..... ii

2 **INTEREST OF AMICUS CURIAE**..... v

3 **SUMMARY OF ARGUMENT**..... vi

4 **ARGUMENT**..... 1

5 **I. CONGRESS PASSED FISA TO REIN IN PRECISELY THE TYPE OF**

6 **OVERBROAD SURVEILLANCE OF INNOCENT AMERICANS THAT HAS**

7 **REEMERGED SINCE 2001.**..... 1

8 **II. HISTORY DEMONSTRATES THAT, IN THE ABSENCE OF PROPER**

9 **OVERSIGHT, EXECUTIVE SURVEILLANCE PROGRAMS EXPAND IN PURPOSE,**

10 **COLLECT EVER-GREATER VOLUMES OF INFORMATION, AND ARE OPERATED**

11 **WITHOUT SUFFICIENT REGARD FOR THEIR LEGALITY OR EFFECTIVENESS..** 2

12 **A. Without proper oversight, executive surveillance programs naturally expand,**

13 **creating the risk of misuse.**..... 3

14 i. Prior to the advent of FISA’s protections, initially narrow programs expanded into

15 illegality and began targeting constitutionally protected activities. .... 3

16 ii. Since 2001, surveillance programs have followed this historical pattern by expanding

17 in secret and cataloguing of the activities of innocent Americans. .... 5

18 **B. Ongoing technological advances allow the collection and storage of vast amounts of**

19 **data, increasing the risk that innocent Americans’ records will be acquired, retained,**

20 **and misused.** ..... 7

21 **C. Executive officials responsible for surveillance programs naturally shield their**

22 **activities from scrutiny, encouraging expansion and impeding necessary oversight.**..... 10

23 i. In the pre-FISA era, the executive shielded legally questionable programs from

24 oversight, reducing their effectiveness and permitting misuse..... 10

25 ii. Since 2001 the executive, despite FISA’s oversight requirements, has once again

26 shielded its actions from the other branches of government; as a result intelligence agencies

27 have conducted operations of questionable legality and efficacy..... 12

28 **III. THIS COURT SHOULD PROPERLY INTERPRET SECTION 215’S RELEVANCE**

**REQUIREMENT AS A RESTRAINT ON EXPANSIVE SURVEILLANCE.**..... 14

**CONCLUSION** ..... 15

**TABLE OF AUTHORITIES**

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

**CASES**

Amended Memorandum Opinion, Docket No. BR 13-109 (FISC Aug. 29, 2013) ..... 6

*Berger v. State of N.Y.*, 388 U.S. 41 (1967)..... 6

*Clapper v. Amnesty International*, 132 S. Ct. 2431 (2012) ..... 15

Memorandum Opinion and Order (FISC Oct. 3, 2011)..... 13

Order, Docket No. BR 08-13 (FISC Mar. 2, 2009) ..... 6, 13

Secondary Order, Docket No. BR 13-80 (FISC Apr. 25, 2013)..... 8, 15

**STATUTES**

50 U.S.C. § 1803 (2006) ..... 2

50 U.S.C. § 1805 (2006) ..... 2

50 U.S.C. § 1807 (2006) ..... 2

50 U.S.C. § 1808 (2006) ..... 2

50 U.S.C. § 1861 (2006) ..... 1

**OTHER AUTHORITIES**

Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, Aug. 9, 2013 ..... 1, 8

Andrea Peterson, *Obama says NSA has plenty of congressional oversight. But one congressman says it's a farce*, Wash. Post. (October 9, 2013), <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-congressman-says-its-a-farce/>..... 14

Barton Gellman & Ashkan Soltani, *NSA collects millions of e-mail address books globally*, Wash. Post (Oct. 14, 2013), [http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html) ..... 10

Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, Wash. Post (Oct. 30, 2013), [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](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) ..... 9

Barton Gellman & Matt DeLong, *How the NSA's MUSCULAR program collects too much data from Yahoo and Google*, Wash. Post (Oct. 30, 2013), <http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/>..... 11

1 Barton Gellman, *U.S. surveillance architecture includes collection of revealing Internet, phone*  
*metadata*, Wash. Post (June 15, 2013), [http://articles.washingtonpost.com/2013-06-](http://articles.washingtonpost.com/2013-06-15/news/39993852_1_comey-national-intelligence-intelligence-collection)  
2 [15/news/39993852\\_1\\_comey-national-intelligence-intelligence-collection](http://articles.washingtonpost.com/2013-06-15/news/39993852_1_comey-national-intelligence-intelligence-collection) ..... 5

3 Carol D. Leonnig, *Court: Ability to police U.S. spying program limited*, Wash. Post (Aug. 15,  
4 2013), [http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-](http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html)  
[limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125\\_print.html](http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html)..... 13

5 Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times,  
6 Dec. 24, 2005, at A1 ..... 5

7 H.R. Rep. No. 109-333 (2005) (Conf. Rep.) ..... 13

8 Hearings Before the Senate Select Comm. to Study Governmental Operations with Respect to  
9 Intelligence Activities, 94th Cong., 1st Sess., Vol. 5 (1975)..... 7

10 Jack Goldsmith, *The Terror Presidency* (2009) ..... 12

11 James Ball, *NSA stores metadata of millions of web users for up to a year, secret files show*, The  
12 Guardian (Sept. 30, 2013), [http://www.theguardian.com/world/2013/sep/30/nsa-americans-](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents)  
13 [metadata-year-documents](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents) ..... 8

14 James Bamford, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret*  
15 *Intelligence Organization* (1982). ..... 4

16 James Bamford, *The Shadow Factory: The NSA From 9/11 to the Eavesdropping on America*  
17 (2008)..... 12, 13

18 James Risen & Laura Poitras, *N.S.A. Examines Social Networks Of U.S. Citizens*, N.Y. Times,  
19 Sept. 29, 2013, at A1 ..... 9

20 Kashmir Hill, *Blueprints Of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds*  
21 *Less Info Than Thought*, Forbes (July 24, 2013),  
22 [http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-](http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/)  
23 [suggest-its-storage-capacity-is-less-impressive-than-thought/](http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/) ..... 8

24 Kate Tummarello, *Senators repackage surveillance bills as comprehensive reform*, The Hill (Sept.  
25 25, 2013), [http://thehill.com/blogs/hillicon-valley/technology/324687-senators-repackage-](http://thehill.com/blogs/hillicon-valley/technology/324687-senators-repackage-surveillance-bills-as-comprehensive-reform)  
26 [surveillance-bills-as-comprehensive-reform](http://thehill.com/blogs/hillicon-valley/technology/324687-senators-repackage-surveillance-bills-as-comprehensive-reform) ..... 14

27 L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church Committee's Investigation of*  
28 *NSA*, Stud. Intelligence, Winter 1999–2000 ..... 3, 4

Letter from James Sensenbrenner to Attorney General Eric Holder (Sept. 6, 2013) ..... 13

Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (1985) ..... 5

Offices of the Inspectors General, *Unclassified Report on the President's Surveillance Program*  
(2009) (“PSP IG Group Report”) ..... 12, 14

*Oversight of the Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the*  
*Judiciary*, 113th Cong. (July 17, 2013) ..... 9



1 Peter Fenn, *When the NSA Was Spying on the Congress*, U.S. News & World Rep. (Sept. 27,  
2013), [http://www.usnews.com/opinion/blogs/Peter-Fenn/2013/09/27/when-the-nsa-spied-on-](http://www.usnews.com/opinion/blogs/Peter-Fenn/2013/09/27/when-the-nsa-spied-on-the-congress)  
the-congress ..... 2

3 Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306  
(2004)..... 2

4 Peter Swire, *A Reasonableness Approach to Searches After the Jones GPS Tracking Case*, 64 Stan.  
5 L. Rev. Online 57 (2012) ..... 6

6 *Presidential News Conference*, Wash. Post (Dec. 19, 2005), [http://www.washingtonpost.com/wp-](http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900375.html)  
7 dyn/content/article/2005/12/19/AR2005121900375.html ..... 5

8 Press Release, *Wyden, Udall Statement on the Disclosure of Bulk Email Records Collection*  
*Program* (July 2, 2013)..... 14

9 Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance:  
10 The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 Wm. & Mary Bill  
Rts. J. 147 (2006)..... 8

11 Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities,  
12 Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755 (1976)  
13 (“Church Committee Book II”) ..... *passim*

14 Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities,  
15 Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans  
16 (Book III), S. Rep. No. 94-755 (1976) (“Church Committee Book III”) ..... 4, 5, 7, 11

17 *Time to Rein in the Surveillance State*, ACLU, <https://www.aclu.org/time-rein-surveillance-state-0>  
18 ..... 9

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**INTEREST OF AMICUS CURIAE**

1           *Amici* are experts in the history of executive surveillance in the United States. They believe  
2 that this history sheds light on the origins and importance of the congressional and judicial  
3 oversight structures implicated by this case. *Amici*'s sole interest is to assist this Court in applying  
4 Section 215 of the USA PATRIOT Act by illuminating similarities between the ongoing bulk  
5 telephone records surveillance at issue here and the government's past surveillance activities.

6           *Amicus* James Bamford served as an intelligence analyst with the United States Navy. In  
7 1982 he published *The Puzzle Palace*, the first comprehensive history of the National Security  
8 Agency ("NSA"). In three subsequent books and numerous articles he has chronicled the activities  
9 of the NSA from its inception, through the post-9/11 era, to the present day. As the foremost  
10 historian of the National Security Agency, Mr. Bamford has an unparalleled understanding of the  
11 development and growth of American surveillance programs.

12           *Amicus* Loch Johnson served as special assistant to the chair of the Church Committee and  
13 as staff director of the House Subcommittee on Intelligence Oversight. He also worked with the  
14 Chair of the Aspin-Brown Commission on Intelligence. He is currently Regents Professor of  
15 Political Science at the University of Georgia and the editor of *Intelligence and National Security*.  
16 From his firsthand experiences with the Church Committee investigations and the Aspin-Brown  
17 Commission, Mr. Johnson is directly familiar with the complex features of American intelligence  
18 agencies and their oversight.

19           *Amicus* Peter Fenn served as Washington Chief of Staff for Senator Frank Church during  
20 his committee's intelligence investigation and on the staff of the Senate Intelligence Committee.  
21 Mr. Fenn's work with Senator Church, and his subsequent experience with the first standing Senate  
22 committee dedicated to overseeing intelligence gathering, allow him to speak to the intricacies of  
23 that oversight.

24           *Amici* understand the features, histories, roles, and capabilities of American intelligence  
25 agencies, and therefore understand the necessity of robust intelligence oversight. Thus, *Amici* seek  
26 to assist this Court in understanding the historical and institutional context of this case.  
27  
28

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

### SUMMARY OF ARGUMENT

The central issue facing this Court is whether the government's present interpretation and application of Section 215 of the USA PATRIOT Act ascribes the proper meaning to the term "relevance." As *amici* explain, the government's interpretation of Section 215 grants the executive expansive power to determine the parameters of its surveillance of Americans; historical patterns that have reemerged since 2001 show the dangers of this approach.

As *amici* know from their extensive research and from personal experience, recent surveillance activities, and the executive's justifications for them, share core features with surveillance programs that operated from the 1930s into the 1970s. These features include: expansion of surveillance programs beyond their original purpose; a tendency to collect as much information as possible, with the result that surveillance expands as technology advances; and a preoccupation with secrecy that thwarts an effective evaluation of these programs' effectiveness or legality.

As *amici* also know from their expertise, these features are present even when executive officials act in good faith; they are inherent to secret surveillance programs and can therefore only be addressed through effective oversight. Surveillance in the mid-twentieth century expanded from its original national security focus into bulk collection of Americans' communications data and the targeting of Americans exercising their First Amendment associational rights; modern programs directed at international terrorism have similarly expanded to sweep up Americans' domestic telephone records. Advancing technology exponentially increases the capacity to collect and analyze data, multiplying the risk that Americans' communications will be acquired and misused.

These modern programs must therefore be subject to effective oversight to reduce the risk that secrecy will mask escalating abuse. When Americans, like the members of Plaintiffs' organizations, challenge the executive's acquisition of their communications data, it is the role of the judiciary to apply the appropriate statutory and constitutional limits on executive surveillance. *Amici* therefore respectfully ask this Court to give Section 215's "relevance" requirement its natural reading as a restraint on, and not an invitation for, massive executive surveillance.

**ARGUMENT****I. CONGRESS PASSED FISA TO REIN IN PRECISELY THE TYPE OF OVERBROAD SURVEILLANCE OF INNOCENT AMERICANS THAT HAS REEMERGED SINCE 2001.**

This case asks the Court to decide whether the executive's prospective and ongoing collection and storage of Americans' telephone records is justified on the grounds that the data are "relevant" to an ongoing foreign intelligence investigation as required by Section 215 of the USA PATRIOT Act. Section 215 amended 50 U.S.C. § 1861 to allow the collection of telephone and other records only if "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2)(A) (2006). The executive argues that Section 215 justifies the collection and storage of all Americans' telephone records, "even when any particular record is unlikely to directly bear on the matter being investigated," if "the Government has reason to believe that conducting a search of [those records] will produce counterterrorism information." *See* Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act, Aug. 9, 2013, at 8, 10.

History counsels caution when the executive claims expansive power to set the limits of its own surveillance of Americans. As the committee led by Senator Frank Church found in its definitive investigation of mid-twentieth-century surveillance, "[i]ntelligence collection programs naturally generate ever-increasing demands for new data" and, "[i]n time of crisis, the Government will exercise its power to conduct domestic intelligence activities to the fullest extent." Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans* (Book II), S. Rep. No. 94-755, at 4, 289 (1976) ("Church Committee Book II"). These programs become abusive when constitutional "checks and balances designed . . . to assure accountability have not been applied." *Id.* at 289.

The Church Committee found that, by the 1970s, executives of both parties had conducted surveillance targeting "numerous individuals and groups who engaged in no criminal activity and

1 who posed no genuine threat to the national security.” *Id.* at 12. Targets included Supreme Court  
2 Justice William O. Douglas; members of the civil rights movement, including Martin Luther King,  
3 Jr.; Senator Adlai Stevenson and Congressman Abner Mikva; White House advisers and  
4 congressional staff members; “journalists and newsmen;” and ordinary “teachers, writers, and  
5 publications.” *Id.* at 8–12, 17, 49. Recent disclosures by the NSA even add Senator Frank Church  
6 himself to that list of targets. Peter Fenn, *When the NSA Was Spying on the Congress*, U.S. News &  
7 World Rep. (Sept. 27, 2013), [http://www.usnews.com/opinion/blogs/Peter-Fenn/2013/09/27/when-](http://www.usnews.com/opinion/blogs/Peter-Fenn/2013/09/27/when-the-nsa-spied-on-the-congress)  
8 [the-nsa-spied-on-the-congress](http://www.usnews.com/opinion/blogs/Peter-Fenn/2013/09/27/when-the-nsa-spied-on-the-congress).

9 Congress responded by asserting its oversight role—first by conducting investigations and  
10 then by passing legislation. In 1978, Congress created the Foreign Intelligence Surveillance Act  
11 (“FISA”) oversight regime to end the four-decade era of expansive and abusive surveillance  
12 detailed by the Church Committee. *See* Peter P. Swire, *The System of Foreign Intelligence*  
13 *Surveillance Law*, 72 *Geo. Wash. L. Rev.* 1306, 1320–25 (2004). FISA imposed both congressional  
14 oversight and judicial review by the Foreign Intelligence Surveillance Court (“FISC”) to provide  
15 checks on executive surveillance programs. *See* 50 U.S.C. §§ 1803, 1805, 1807, 1808 (2006).

16 Recent disclosures show that patterns from the pre-FISA era have reemerged since the 9/11  
17 terrorist attacks. These developments are troubling but unsurprising—they follow a clear historical  
18 pattern. In the absence of effective oversight, surveillance programs expand, with abuse following  
19 and eventually flourishing. This Court should give Section 215’s “relevance” requirement its  
20 natural reading as a check on, rather than a license for, expansive executive surveillance powers.  
21 This is consistent with the language of the statute, the lessons of history, and FISA’s protective  
22 regime.

23 **II. HISTORY DEMONSTRATES THAT, IN THE ABSENCE OF PROPER OVERSIGHT,**  
24 **EXECUTIVE SURVEILLANCE PROGRAMS EXPAND IN PURPOSE, COLLECT**  
25 **EVER-GREATER VOLUMES OF INFORMATION, AND ARE OPERATED**  
26 **WITHOUT SUFFICIENT REGARD FOR THEIR LEGALITY OR EFFECTIVENESS.**

27 *Amici* seek to highlight the central lesson of the pre-FISA era: the expansion of executive  
28 surveillance programs creates an inherent and grave risk that, over time, those programs will be

1 misused to monitor Americans' constitutionally protected activities.

2 Post-9/11 surveillance programs share core features with the programs criticized by the  
3 Church Committee in its report: a drift by agencies into overbroad collection practices; a continual  
4 expansion of surveillance fueled by increases in technological capacity; and a preoccupation with  
5 secrecy that makes it difficult to assess either the programs' effectiveness or whether they have  
6 expanded beyond legal and constitutional limits.

7 Importantly, history shows that these features do not result from the isolated decisions of  
8 ill-intentioned officials. Rather, these problems are inherent to secret surveillance programs—  
9 including those created by well-intentioned officials for appropriate purposes—and are exacerbated  
10 by insufficient transparency and oversight.

11 These features led to the growth and misuse of executive surveillance in the mid-twentieth  
12 century and persisted until Congress addressed them with FISA's structural protections. Today,  
13 they have reemerged in the bulk collection of communications records at issue here and in the  
14 government's defenses of this practice.

15 **A. Without proper oversight, executive surveillance programs naturally expand, creating the  
16 risk of misuse.**

17 The history of executive surveillance in the twentieth century demonstrates that programs  
18 operating without robust external and internal oversight expand beyond their original purposes,  
19 often into illegal conduct. Features of post-9/11 programs follow this pattern.

20 *i. Prior to the advent of FISA's protections, initially narrow programs expanded into  
21 illegality and began targeting constitutionally protected activities.*

22 Operation SHAMROCK, which monitored millions of telegrams sent by Americans  
23 between 1947 and 1975, is a striking example of the overbroad surveillance documented by the  
24 Church Committee. As former Central Intelligence Agency ("CIA") Inspector General L. Britt  
25 Snider reported, the operation that would become the dragnet SHAMROCK program began with a  
26 clear national security purpose—monitoring and censoring information leaving the country during  
27 World War II. *See* L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church  
28 Committee's Investigation of NSA*, Stud. Intelligence, Winter 1999–2000, at 45, 48–49. After the

1 war, however, the agency that would later become the NSA continued and expanded the  
2 monitoring program through secret arrangements with three major telecommunications companies.  
3 *See id.* at 48–49; *see also* James Bamford, *The Puzzle Palace: Inside the National Security Agency,*  
4 *America's Most Secret Intelligence Organization* 302–15 (1982).

5 By the time SHAMROCK was terminated in 1975, it had grown to become “probably the  
6 largest governmental interception program affecting Americans ever undertaken,” with NSA  
7 analysts using new computing methods to review about 150,000 telegrams per month—including  
8 the majority of the international telegrams leaving New York City. Senate Select Comm. to Study  
9 Governmental Operations with Respect to Intelligence Activities, Supplemental Detailed Staff  
10 Reports on Intelligence Activities and the Rights of Americans (Book III), S. Rep. No. 94-755, at  
11 765 (1976) (“Church Committee Book III”); Snider, *supra*, at 45. Telegrams were picked up daily  
12 and fed into a computer that “kick[ed] out” full texts of any telegrams containing key words,  
13 phrases, names, locations, or addressees. *See* Bamford, *The Puzzle Palace, supra*, at 313.

14 SHAMROCK’s purpose expanded along with its data collection and it eventually targeted  
15 many Americans exercising their First Amendment rights, including Black Power movement  
16 participants and Vietnam War opponents. *See id.* at 317–22. Congress’s investigation found that  
17 the program violated laws against domestic spying and laws “protecting the privacy of the mails  
18 and forbidding the interception of communications.” Church Committee Book II at 58.

19 As SHAMROCK grew, the NSA also began focusing its surveillance efforts on “watch list”  
20 names submitted by other federal agencies. This intelligence-sharing program expanded piecemeal  
21 and over time into abuse. Watch-list surveillance initially focused on protecting the President and  
22 other government officials and on Federal Bureau of Investigation (“FBI”) requests, in light of the  
23 embargo against Cuba, that the NSA flag communications of American companies “doing business  
24 with individuals in Cuba and the Cuban government” and the “personal messages” of individuals  
25 traveling to or from that country. Church Committee Book III at 744–45. But the watch list soon  
26 developed into a wide-ranging domestic surveillance program that targeted law-abiding citizens.  
27 *See id.* at 747–50. In 1967, responding to pressure from the executive, the Department of the Army  
28

1 established a “civil disturbance unit” that used the NSA to monitor American civil rights and  
2 antiwar organizations for “foreign involvement.” *Id.* Between 1966 and 1973, the NSA intercepted  
3 messages of 1680 Americans and activist groups—not because of evidence of wrongdoing, but  
4 because the NSA had been given the “unprecedented” task of hunting for evidence that activists  
5 were under foreign influence. Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence*  
6 *Investigation* 105 (1985); Church Committee Book III at 746.

7 The NSA conducted watch list surveillance without a charter until formalizing the program  
8 as “MINARET” in 1969. The NSA created MINARET’s secret charter both to formalize watch list  
9 procedures and to hide the agency’s tracking of Americans. Church Committee Book III at 748–49.

10 *ii. Since 2001, surveillance programs have followed this historical pattern by expanding in*  
11 *secret and cataloguing of the activities of innocent Americans.*

12 Despite the additional oversight required by the FISA regime, post-9/11 executive  
13 surveillance programs have similarly expanded beyond legal limits, creating a serious and ongoing  
14 risk that they will be used for illegal monitoring and targeting.

15 The President’s Surveillance Program (“PSP”), a warrantless surveillance operation  
16 approved by President George W. Bush after 9/11, began with a clear national security purpose—  
17 targeting international calls of people with known links to terrorist groups. *Presidential News*  
18 *Conference*, Wash. Post (Dec. 19, 2005), [http://www.washingtonpost.com/wp-](http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900375.html)  
19 [dyn/content/article/2005/12/19/AR2005121900375.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900375.html). But the PSP expanded into what some  
20 officials described as “a large data-mining operation,” collecting and analyzing a vast quantity of  
21 international and domestic Internet and telephone communications. Eric Lichtblau & James Risén,  
22 *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times, Dec. 24, 2005, at A1. By 2004,  
23 the Attorney General and the FBI Director had concluded that the PSP’s warrantless bulk  
24 collection of Internet metadata was illegal and threatened to resign if it continued without FISC  
25 approval. See Barton Gellman, *U.S. surveillance architecture includes collection of revealing*  
26 *Internet, phone metadata*, Wash. Post (June 15, 2013), [http://articles.washingtonpost.com/2013-06-](http://articles.washingtonpost.com/2013-06-15/news/39993852_1_comey-national-intelligence-intelligence-collection)  
27 [15/news/39993852\\_1\\_comey-national-intelligence-intelligence-collection](http://articles.washingtonpost.com/2013-06-15/news/39993852_1_comey-national-intelligence-intelligence-collection).

28 Despite subsequent moves to subject executive surveillance to congressional and judicial



1 scrutiny, these programs have continued to expand. The bulk, prospectively authorized collection  
2 of telephone records at issue here—an outgrowth of the PSP—epitomizes this trend. In the FISC’s  
3 March 2009 Order reviewing the records program and addressing Section 215’s relevance  
4 requirement, Judge Walton noted that nearly all the collected telephone records pertained to “non-  
5 U.S. persons who are *not* the subject of an FBI investigation to obtain foreign intelligence  
6 information,” “U.S. persons who are *not* the subject of an FBI investigation to protect against  
7 international terrorism or clandestine intelligence activities,” and “data that otherwise could not be  
8 legally captured in bulk by the government.” Order, Docket No. BR 08-13, at 11–12 (FISC Mar. 2,  
9 2009). The court could only approve such a program, Judge Walton explained, based on “the  
10 government’s explanation, under oath,” of how the collection was vital to national security and on  
11 its use of constitutionally required minimization procedures restricting access to the collected  
12 metadata. *Id.* at 12; *see* Peter Swire, *A Reasonableness Approach to Searches After the Jones GPS*  
13 *Tracking Case*, 64 Stan. L. Rev. Online 57 (2012) (citing *Berger v. State of N.Y.*, 388 U.S. 41, 59  
14 (1967)) (explaining Congress’s enshrinement of *Berger*’s constitutional requirements in statutory  
15 minimization procedures).

16 However, the court noted that “[f]rom the inception of this . . . program, the NSA’s data  
17 accessing technologies and practices were never adequately designed to comply with the governing  
18 minimization procedures,” that there had been “repeated inaccurate statements made in the  
19 government’s submissions,” and that court-imposed safeguards had “been so frequently and  
20 systemically violated that it can fairly be said that this critical element of the overall . . . regime has  
21 never functioned effectively.” Order, Docket No. BR 08-13, at 11, 14–15 (FISC Mar. 2, 2009).  
22 Judge Walton concluded that “[t]o approve such a program, the Court must have every confidence  
23 that the government is doing its utmost to ensure that those responsible for implementation fully  
24 comply with the Court’s orders. The Court no longer has such confidence.” *Id.* at 12. *But see*  
25 Amended Memorandum Opinion, Docket No. BR 13-109, at 5 n.8 (FISC Aug. 29, 2013).

26 As the trajectory of pre-FISA and post-9/11 surveillance demonstrates, it is simply the  
27 nature of such programs—even when led by well-intentioned officials—to incrementally expand  
28

1 and begin collecting data outside their legitimate scope.

2 **B. Ongoing technological advances allow the collection and storage of vast amounts of data,**  
3 **increasing the risk that innocent Americans' records will be acquired, retained, and**  
4 **misused.**

5 The Church Committee further concluded that Project MINARET suffered from a  
6 “multiplier effect.” Church Committee Book III at 750. The NSA collected as much information as  
7 possible to be analyzed later, resulting in the expansion of the number of targeted individuals and  
8 organizations as well as surveillance of people who simply came into contact with those who ended  
9 up on watch lists. *See id.* Thus, MINARET surveilled innocent Americans, from “members of  
10 radical political groups” to “citizens involved in protests against their Government.” *Id.* at 749-50.  
11 Communications collected by the NSA included, for example, those “discussing a peace concert”  
12 and “a pro-Vietnam war activist’s invitations to speakers for a rally.” *Id.* at 750.

13 Technological advances contributed to this multiplier effect. Telegraph companies’ move to  
14 magnetic tapes from paper made it possible for the NSA to search quickly for particular names;  
15 thereafter, “telegrams to or from, or even mentioning, U.S. citizens whose names appeared on the  
16 watch list . . . would have been sent to NSA’s analysts, and many would subsequently be  
17 disseminated to other agencies.” Hearings Before the Senate Select Comm. to Study Governmental  
18 Operations with Respect to Intelligence Activities, 94th Cong., 1st Sess., Vol. 5, at 59 (1975). The  
19 Church Committee specifically warned that “the technological capability of Government  
20 relentlessly increases,” that “the potential for abuse is awesome,” and that Congress must create  
21 “restraints which not only cure past problems but anticipate and prevent the future misuse of  
22 technology.” Church Committee Book II at 289.

23 The committee was prescient. Since the mid-1970s, increasing technological capacity to  
24 collect and store data has enormously magnified the risk that innocent Americans will be surveilled  
25 and later improperly targeted. Advances in storage capacity and “data mining” techniques allow the  
26 NSA to collect and analyze immense amounts of information. This includes “all call detail records  
27 or ‘telephony metadata’ created by Verizon for communications . . . [including those] wholly  
28 within the United States, including local telephone calls,” Secondary Order, Docket No. BR 13-80,

1 at 2 (FISC Apr. 25, 2013), as well as a year's worth of records of the online activities of millions of  
2 Internet users. James Ball, *NSA stores metadata of millions of web users for up to a year, secret*  
3 *files show*, The Guardian (Sept. 30, 2013), [http://www.theguardian.com/world/2013/sep/30/nsa-](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents)  
4 [americans-metadata-year-documents](http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents).

5 Repeating—and dwarfing—the NSA's impulse to warehouse MINARET watch list data, a  
6 recent government white paper argues that the NSA's "analytic tools . . . require the collection and  
7 storage of a large volume of metadata," necessitating that aggregated call records be available for  
8 five years. See Administration White Paper: Bulk Collection of Telephony Metadata Under Section  
9 215 of the USA PATRIOT Act, Aug. 9, 2013, at 13. The NSA's storage capacity has become  
10 almost unfathomably large; Internet infrastructure experts estimate that a new \$2 billion Utah  
11 facility can store between twelve exabytes and five zettabytes of communication information.  
12 Kashmir Hill, *Blueprints Of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds*  
13 *Less Info Than Thought*, Forbes (July 24, 2013), [http://www.forbes.com/sites/kashmirhill/](http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought)  
14 [2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-](http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-)  
15 [than-thought](http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-). Even under the lower estimate, this single facility could store full voice recordings of  
16 every U.S. phone call for the next forty years. See *id.*

17 Events since 2001 have also demonstrated the extraordinarily difficult challenge the  
18 executive faces in attempting to limit its use of such a vast trove of Americans' communications  
19 data. Just as MINARET ensnared people only tangentially related to investigations, the PSP—  
20 which initially sought to intercept telephone numbers and email addresses from members of al-  
21 Qaeda—"naturally expanded to include individuals linked more and more tenuously with the  
22 originally identified targets." Robert Bloom & William J. Dunn, *The Constitutional Infirmary of*  
23 *Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth*  
24 *Amendment*, 15 Wm. & Mary Bill Rts. J. 147, 156 (2006).

25 Still, no known pre-9/11 program collected as much of the communications data of so many  
26 Americans as the ongoing telephone records collection at issue here. See Secondary Order, No. BR  
27 13-80, at 2 (FISC Apr. 25, 2013). Yet recent disclosures also reveal that the NSA is directly  
28

1 targeting far more people's data than previously understood or disclosed. During a July 2013  
2 hearing before the House Committee on the Judiciary, NSA Deputy Director John C. Inglis  
3 confirmed that NSA analysts perform *three-hop* queries for phone record analysis, rather than the  
4 one- or two-hop analysis previously disclosed. *Oversight of the Administration's Use of FISA*  
5 *Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (July 17, 2013). This  
6 means that, once the agency identifies a suspect, it reviews all of that person's contacts, then all of  
7 these first-hop people's contacts, and finally all of *those* people's contacts. The NSA thus routinely  
8 examines the calling records of Americans with no direct relationship to an investigation's target.  
9 By targeting a single person whose call history includes 40 contacts, it can sweep the phone  
10 records of roughly 2.5 million people into the review. *See Time to Rein in the Surveillance State*,  
11 ACLU, <https://www.aclu.org/time-rein-surveillance-state-0> (last visited Nov. 5, 2013).

12 Recently disclosed NSA documents demonstrate that this dragnet collection has grown to  
13 pose a tangible threat to the constitutional rights of an unknown number of Americans. Since late  
14 2011, the NSA has been conducting "'large-scale graph analysis on very large sets of  
15 communications metadata without . . . check[ing] foreignness' of every e-mail address, phone  
16 number, or other identifier," generating sophisticated maps of Americans' associational  
17 connections. James Risen & Laura Poitras, *N.S.A. Examines Social Networks Of U.S. Citizens*,  
18 N.Y. Times, Sept. 29, 2013, at A1.

19 Further, the NSA—authorized only by executive order—has been tapping the internal  
20 communications links that connect both Google's and Yahoo's data centers into worldwide private  
21 networks, allowing it to collect metadata, text, audio, and video "at will from hundreds of millions  
22 of user accounts, many of them belonging to Americans." *See* Barton Gellman & Ashkan Soltani,  
23 *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, Wash.  
24 Post (Oct. 30, 2013), [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](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). And, according to NSA documents, last year the agency  
25 intercepted 500,000 email address books and instant messaging "buddy lists" per day, likely  
26  
27  
28

1 acquiring the contacts of millions or tens of millions of Americans. *See* Barton Gellman & Ashkan  
2 Soltani, *NSA collects millions of e-mail address books globally*, Wash. Post (Oct. 14, 2013),  
3 [http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html)  
4 [books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html).

5 Thus, the multiplier effect—a natural phenomenon greatly accelerated by technological  
6 advances—has already resulted in the collection of enormous and growing amounts of innocent  
7 Americans’ personal information, ensnaring them in a searchable catalogue. History shows, and  
8 present NSA practices confirm, that this information is vulnerable to misuse and targeted abuse.

9 **C. Executive officials responsible for surveillance programs naturally shield their activities  
10 from scrutiny, encouraging expansion and impeding necessary oversight.**

11 A review of executive surveillance programs shows that even well-meaning public servants,  
12 acting in good faith, are not in the best position to judge their own actions or account for the  
13 behavior of the massive bureaucracies they supervise. The executive’s priority is to conduct  
14 sensitive intelligence operations in secret. Accordingly, executive officials naturally limit outside  
15 scrutiny of their actions. But secrecy has historically veiled the scope of executive surveillance  
16 programs and risked their expansion and eventual misuse.

17 *i. In the pre-FISA era, the executive shielded legally questionable programs from  
18 oversight, reducing their effectiveness and permitting misuse.*

19 Before FISA’s implementation, the executive routinely failed to provide accurate  
20 information to Congress about the scope of its domestic surveillance, instead shrouding its  
21 activities in secrecy. Upon the outbreak of World War II, Attorney General Robert Jackson gave  
22 Congress an inaccurate account of the FBI’s national security role. Jackson wrote that the FBI  
23 would “confine its activities to the investigation of violation of Federal statutes [and] the collecting  
24 of evidence in cases in which the United States is or may be a party in interest.” Church Committee  
25 Book II at 30. But, as Jackson himself later said, the FBI was actually conducting “steady  
26 surveillance” of people “likely” to break the law due to sympathies for foreign dictatorships. *Id.*

27 Similarly, after World War II, the Truman Administration ramped up its surveillance  
28 programs while providing only partial and contradictory information to Congress. The Secretary of

1 Defense approached the House and Senate Judiciary Committees in an effort to put SHAMROCK  
2 on firm legal ground; but the Defense Department was reluctant to have the issue discussed by the  
3 whole Congress and ultimately abandoned the effort. *See* Church Committee Book III at 769–70.

4 The executive eventually prioritized secrecy over concern for the programs' effectiveness.  
5 As noted above, the Church Committee found that the NSA subjected MINARET to more stringent  
6 secrecy than other programs in part “to conceal [the NSA’s] involvement in activities which [went]  
7 beyond its regular mission,” and instead targeted domestic American activities. *Id.* at 749.

8 Such secrecy prevented Congress from evaluating the efficacy of programs like  
9 SHAMROCK and MINARET. When the Church Committee finally viewed the whole of the  
10 surveillance programs, it raised significant doubts about their supposed benefits. It found that  
11 “[b]etween 1960 and 1974, the FBI conducted over 500,000 separate investigations of persons and  
12 groups under the ‘subversive’ category ... [y]et not a single individual or group [had] been  
13 prosecuted since 1957 under the laws which ... [were] the main alleged statutory basis for such  
14 FBI investigations.” Church Committee Book II at 19. Compared to the FBI’s other investigatory  
15 methods, the committee found, “domestic intelligence surveillance programs . . . produced  
16 surprisingly few useful returns in view of their extent,” and were sometimes even a nuisance  
17 because they distributed information without first vetting its usefulness. *See id.* at 18, 259.

18 Recent NSA materials discussing its tapping of Google and Yahoo data centers echo the  
19 Church Committee’s findings that the collection of vast troves of electronic surveillance data was  
20 often counterproductive. NSA analysts felt that the “relatively small intelligence value [some data]  
21 contain[] does not justify the sheer volume of data collected,” complaining that it “‘dilut[ed]’ their  
22 workflow.” Barton Gellman & Matt DeLong, *How the NSA’s MUSCULAR program collects too*  
23 *much data from Yahoo and Google*, Wash. Post (Oct. 30, 2013),  
24 [http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-](http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543)  
25 [data-from-yahoo-and-google/543](http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543).

26 Thus, even as executive surveillance programs expand to target groups and individuals  
27 protected by the First Amendment, they become less useful as tools for protecting national security.

1 Secrecy masks this ineffectiveness until scandals draw congressional and public attention.

2 *ii. Since 2001 the executive, despite FISA's oversight requirements, has once again*  
3 *shielded its actions from the other branches of government; as a result intelligence*  
4 *agencies have conducted operations of questionable legality and efficacy.*

5 Like their predecessors, executive officials since 9/11 have been reluctant to allow adequate  
6 scrutiny—whether internal, by courts, or by Congress—of their activities. This excessive secrecy  
7 has made assessing these programs difficult or impossible, inviting waste and abuse.

8 Jack Goldsmith, who headed the Justice Department's Office of Legal Counsel for seven  
9 months during the Bush Administration, noted that "[f]rom the beginning the administration could  
10 have taken ... steps to ramp up terrorist surveillance in indisputably lawful ways that would have  
11 minimized the likelihood of a devastating national security leak. But . . . [t]he White House had  
12 found it much easier to go it alone, in secret." Jack Goldsmith, *The Terror Presidency* 182 (2009).  
13 This choice grew partially from an understandable desire to move as quickly as possible in light of  
14 new threats and partially from a desire to protect the executive's prerogatives against what  
15 administration officials viewed as needless interference from other branches. *See id.* at 181.

16 This secrecy hampered attempts, even by executive officials themselves, to evaluate the  
17 appropriateness and legality of post-9/11 programs. The Justice Department denied the NSA  
18 inspector general's request to see the legal analysis supporting the President's Surveillance  
19 Program. James Bamford, *The Shadow Factory: The NSA From 9/11 to the Eavesdropping on*  
20 *America* 116 (2008). Outside of the FBI, only the Attorney General and two other Justice  
21 Department officials knew the details of the PSP, and one attorney had sole responsibility for  
22 evaluating its legality. *Id.* This lack of review created the risk of mistakes. An unclassified 2009  
23 internal report found that, when other Justice Department attorneys eventually reviewed the legal  
24 justification for the PSP, they found that it failed to address seminal case law, ignored FISA  
25 language restraining warrantless surveillance, and misstated the scope of the program. *See* Offices  
26 of the Inspectors General, *Unclassified Report on the President's Surveillance Program* 11–13  
27 (2009) ("PSP IG Group Report").

28 The executive has also shielded the full extent of the PSP and other programs from judicial

1 and congressional oversight. For example, at first the FISC was not consulted about the PSP's legal  
2 footing; only the presiding judge was told, and then only that it was a presidential decision.  
3 Bamford, *The Shadow Factory*, *supra*, at 116. Since the executive submitted to FISC oversight, the  
4 FISC has criticized it for repeatedly providing inaccurate reports of its activities. As FISC Chief  
5 Judge Walton recently noted, the court cannot independently investigate issues of noncompliance  
6 and must instead rely on the accuracy of information provided to it by the government. Carol D.  
7 Leonnig, *Court: Ability to police U.S. spying program limited*, Wash. Post (Aug. 15, 2013),  
8 [http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-](http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html)  
9 [limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125\\_print.html](http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html).

10 In his March 2009 Order, Judge Walton criticized the NSA for misleading the court for  
11 nearly three years about the scope and use of the telephone records collection. Order, Docket No.  
12 BR 08-13, at 8–9 (FISC Mar. 2, 2009). Judge Walton found that the government's inaccurate  
13 testimony prevented the NSA and the FISC “from taking steps to remedy daily violations of the  
14 minimization procedures set forth in FISC orders and designed to protect . . . call detail records  
15 pertaining to telephone communications of U.S. persons located within the United States . . . whose  
16 call detail information could not otherwise have been legally captured in bulk.” *Id.* at 9; *see also*  
17 Memorandum Opinion and Order, at 16 n.14 (FISC Oct. 3, 2011) (assessing the NSA's Internet  
18 communications records collection and noting that key inaccuracies comprised “the third instance  
19 in less than three years in which the government has disclosed a substantial misrepresentation  
20 regarding the scope of a major collection program”).

21 Nor has Congress been able to provide an effective check. As Rep. James Sensenbrenner—  
22 the Chairman of the House Judiciary Committee when Section 215 was passed—recently explained  
23 in a letter to the Attorney General, “The administration's interpretation to allow for bulk collection  
24 is at odds with Congressional intent [to limit access to specific records] and with both the plain and  
25 legal meanings of ‘relevance.’” Letter from James Sensenbrenner to Attorney General Eric Holder  
26 (Sept. 6, 2013); *see also* H.R. Rep. No. 109-333, at 90 (2005) (Conf. Rep.). Rep. Justin Amash  
27 recently described how excessive secrecy thwarts congressional oversight efforts: “You don't  
28



1 know what questions to ask because you don't know what . . . kind of things are going on. . . .  
2 [Y]ou just have to guess and it becomes a totally ridiculous game of 20 questions.” Andrea  
3 Peterson, *Obama says NSA has plenty of congressional oversight. But one congressman says it's a*  
4 *farce*, Wash. Post. (October 9, 2013), [http://www.washingtonpost.com/blogs/the-](http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-congressman-says-its-a-farce)  
5 [switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-](http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-congressman-says-its-a-farce)  
6 [congressman-says-its-a-farce](http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-congressman-says-its-a-farce).

7 Excessive secrecy also encourages needlessly overbroad collection and makes it practically  
8 impossible to evaluate the efficacy of today's programs. For instance, the Justice Department's  
9 inspector general “found it difficult to assess or quantify the overall effectiveness of the PSP” in  
10 FBI counterterrorism efforts; the CIA's inspector general also “was unable to independently draw  
11 any conclusion on the [program's] overall effectiveness.” PSP IG Group Report at 33–34.

12 Senate Intelligence Committee members Ron Wyden and Mark Udall recently explained  
13 that, contrary to the government's statement that it ended its nationwide bulk Internet and email  
14 records collection program in 2011 for operational and resource reasons, the program was actually  
15 terminated because senators “spent a significant portion of 2011 pressing intelligence officials to  
16 provide evidence of its effectiveness” and those officials “were unable to do so.” Press Release,  
17 *Wyden, Udall Statement on the Disclosure of Bulk Email Records Collection Program* (July 2,  
18 2013). Nor, Senator Udall said, has the bulk telephone records program “provided unique value” in  
19 stopping threats; he criticized the executive's attempts to demonstrate the program's successes as  
20 “not stand[ing] up to scrutiny.” Kate Tummarello, *Senators repackage surveillance bills as*  
21 *comprehensive reform*, The Hill (Sept. 25, 2013), [http://thehill.com/blogs/hillicon-](http://thehill.com/blogs/hillicon-valley/technology/324687-senators-repackage-surveillance-bills-as-comprehensive-reform)  
22 [valley/technology/324687-senators-repackage-surveillance-bills-as-comprehensive-reform](http://thehill.com/blogs/hillicon-valley/technology/324687-senators-repackage-surveillance-bills-as-comprehensive-reform).

23 **III. THIS COURT SHOULD PROPERLY INTERPRET SECTION 215'S RELEVANCE**  
24 **REQUIREMENT AS A RESTRAINT ON EXPANSIVE SURVEILLANCE.**

25 Post-9/11 surveillance programs, including the bulk telephone records collection at issue in  
26 this case, are following a historical pattern by expanding to challenge legal and constitutional  
27 limits. Congress designed the modern oversight regime to check just such a renewed expansion.

28 When the FISA oversight process breaks down and Americans challenge the executive's

1 acquisition of their communications data, it is the role of the judiciary to apply statutory and  
 2 constitutional limits to executive surveillance. Unlike in previous cases, *see, e.g., Clapper v.*  
 3 *Amnesty International*, 132 S. Ct. 2431 (2012), the Court is no longer limited by a lack of detail  
 4 about the contested surveillance. *See* Secondary Order, Docket No. BR 13-80 (FISC Apr. 25,  
 5 2013). The expansion and abuse of executive surveillance detailed by the Church Committee—and  
 6 the troubling recent reemergence of similar activities and trends—counsels a different course from  
 7 that requested by the government. The present situation should guide this Court to order the  
 8 executive to limit its surveillance activities to what is allowed under a proper application of Section  
 9 215, consistent with FISA’s safeguards.

### 10 CONCLUSION

11 *Amici* thus respectfully request that this Court apply Section 215’s “relevance” requirement  
 12 as a restraint on expansive surveillance, in light of the plain meaning of the statute, historical  
 13 patterns of surveillance expansion, and lessons learned in the aftermath of previous abuses.

14 DATED: November 15, 2013

Respectfully submitted,

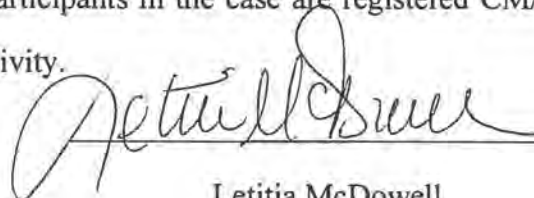
15 By:           /s/ Jennifer M. Urban          

16 Jennifer M. Urban  
 17 SAMUELSON LAW, TECHNOLOGY &  
 18 PUBLIC POLICY CLINIC  
 19 UNIVERSITY OF CALIFORNIA,  
 20 BERKELEY, SCHOOL OF LAW  
 396 Simon Hall  
 Berkeley, CA 94720-7200  
 Telephone: (510) 684-7177  
 Facsimile: (510) 643-4625

21 Attorney for *Amici Curiae*  
 22 EXPERTS IN THE HISTORY OF EXECUTIVE  
 23 SURVEILLANCE: JAMES BAMFORD,  
 24 LOCH JOHNSON, AND PETER FENN

**CERTIFICATION OF SERVICE**

1 I hereby certify that on November 15, 2013, I electronically filed the foregoing EXPERTS IN THE  
2 HISTORY OF EXECUTIVE SURVEILLANCE'S MOTION FOR LEAVE TO FILE BRIEF  
3 *AMICUS CURIAE* IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY  
4 JUDGMENT with the Clerk of Court for the United States District Court for the Northern District  
5 of California by using the ECF system. All participants in the case are registered CM/ECF users  
6 and will be served with a Notice of Docket Activity.

7   
8 \_\_\_\_\_  
9 Letitia McDowell

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28