

1 CINDY COHN (SBN 145997)
cindy@eff.org
2 LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
3 JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
4 ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
5 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
6 San Francisco, CA 94109
Telephone: (415) 436-9333
7 Fax: (415) 436-9993

8 RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
9 LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
10 San Francisco, CA 94111
Telephone: (415) 433-3200
11 Fax: (415) 433-6382

12
13
14 *Counsel for Plaintiffs*

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

15 **UNITED STATES DISTRICT COURT**
16 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
17 **OAKLAND DIVISION**

18
19 CAROLYN JEWEL, TASH HEPTING,
YOUNG BOON HICKS, as executrix of the
20 estate of GREGORY HICKS, ERIK KNUTZEN
and JOICE WALTON, on behalf of themselves
21 and all others similarly situated,
22 Plaintiffs,
23 v.
24 NATIONAL SECURITY AGENCY, *et al.*,
25 Defendants.

) Case No.: 4:08-cv-4373-JSW
)
)
) **PLAINTIFFS CAROLYN JEWEL, ERIK**
) **KNUTZEN, AND JOICE WALTON'S**
) **NOTICE OF MOTION AND MOTION**
) **FOR PARTIAL SUMMARY JUDGMENT**
) **(Fourth Amendment Violation)**
)
) Date: October 31, 2014
) Time: 9:00 a.m.
) Courtroom 5, Second Floor
) The Honorable Jeffrey S. White

TABLE OF CONTENTS

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

NOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGMENT 1

MEMORANDUM OF POINTS AND AUTHORITIES..... 2

I. INTRODUCTION 2

II. STATEMENT OF FACTS 3

 A. The Government Seizes And Searches Communications Flowing Through The
 Nation’s Internet Backbone 3

 B. Seizure And Searching Of Plaintiffs’ Communications From AT&T’s Internet
 Backbone 9

III. ISSUES FOR DECISION 11

IV. ARGUMENT 11

 A. The Fourth Amendment’s Fundamental Principles—And The Warrant
 Requirement—Apply With Full Force To The Digital World, And Protect
 Plaintiffs’ Private Internet Communications 11

 1. The Fourth Amendment Guarantees Fundamental Personal Privacy By
 Prohibiting Suspicionless, Indiscriminate Government Intrusions Into
 Americans’ Papers And Effects..... 11

 2. The Fourth Amendment’s Warrant Requirement Is The Time-Tested
 Mechanism That Prevents Government Overreaching And Suspicionless
 Searches, And It Applies To Digital Seizure And Searching Of Electronic
 Communications..... 14

 B. Stage One: The Government’s Warrantless, Suspicionless Mass Seizure Of
 Domestic Internet Communications Violates The Fourth Amendment 16

 C. Stage Three: The Government’s Warrantless, Suspicionless Searching Of The
 Contents Of Plaintiffs’ Internet Communications Is Unconstitutional 19

 D. The Government’s Defenses Fail 21

 1. Section 702 Orders Cannot Substitute For Constitutionally-Required
 Warrants 21

 2. The “Special Needs” Exception Cannot Justify The Government’s Dragnet 24

V. CONCLUSION 25

1 **TABLE OF AUTHORITIES**

2 **Federal Cases**

3 *Al Haramain Islamic Foundation, Inc. v. U.S. Department of Treasury,*
686 F.3d 965 (9th Cir. 2011) 24

4

5 *Andresen v. Maryland,*
427 U.S. 463 (1976) 20

6 *Berger v. New York,*
388 U.S. 41 (1967) 13, 15, 17, 23

7

8 *Camara v. Municipal Court of San Francisco,*
387 U.S. 523 (1967) 11

9 *Chandler v. Miller,*
520 U.S. 305 (1997) 24

10

11 *Coolidge v. New Hampshire,*
403 U.S. 443 (1971) 15

12 *Doe 1 v. AOL LLC,*
552 F.3d 1077 (9th Cir. 2009) 13

13

14 *Ex parte Jackson,*
96 U.S. 727 (1877) 12, 14

15 *Florida v. Jardines,*
133 S. Ct. 1409 (2013) 17

16

17 *Go-Bart Importing Co. v. U.S.,*
282 U.S. 344 (1931) 18

18 *Halperin v. Kissinger,*
807 F.2d 180 (D.C. Cir. 1986) 14, 17

19

20 *Hepting v. AT&T Corp.,*
439 F. Supp. 2d 974 (N.D. Cal. 2006) 10, 16

21 *Home Building & Loan Ass'n v. Blaisdell,*
290 U.S. 398 (1934) 25

22

23 *In re Grand Jury Subpoenas Dated Dec. 10, 1987,*
926 F.2d 847 (9th Cir. 1991) 15

24 *Joffe v. Google, Inc.,*
729 F.3d 1262 (9th Cir. 2013) 6

25

26 *Katz v. U.S.,*
389 U.S. 347 (1967) 13, 16, 17

27 *Marcus v. Search Warrant of Property,*
367 U.S. 717 (1961) 12, 18, 20

28

1 *Marron v. U.S.*,
275 U.S. 192 (1927) 15

2

3 *Maryland v. Garrison*,
480 U.S. 79 (1987) 15

4 [Name and docket no. redacted],
2011 WL 10945618 (FISC Oct. 3, 2011) 4, 7, 8

5

6 *Olmstead v. United States*,
277 U.S. 438 (1928) 11, 15

7 *Payton v. New York*,
445 U.S. 573 (1980) 2

8

9 *Riley v. California*,
573 U.S. ___, 134 S. Ct. 2473 (2014) *passim*

10 *Stanford v. Texas*,
379 U.S. 476 (1965) 12, 18

11

12 *Steagald v. U.S.*,
451 U.S. 204 (1981) 20

13 *U.S. v. Abrams*,
615 F.2d 541 (1st Cir. 1980) 17

14

15 *U.S. v. Bridges*,
344 F.3d 1010 (9th Cir. 2003) 15

16 *U.S. v. Choate*,
576 F.2d 165 (9th Cir. 1978) 12

17

18 *U.S. v. Collins*,
845 F.2d 145 (1987) 19

19 *U.S. v. Cotterman*,
709 F.3d 952 (9th Cir. 2013) 12

20

21 *U.S. v. Jones*,
565 U.S. ___, 132 S. Ct. 945 (2012) *passim*

22 *U.S. v. Kow*,
58 F.3d 423 (9th Cir. 1995) 17

23

24 *U.S. v. Tamura*,
694 F.2d 591 (9th Cir. 1982) 17

25 *U.S. v. U.S. District Court (Keith)*,
407 U.S. 297 (1972) 13, 15, 16, 25

26

27 *U.S. v. Van Leeuwen*,
397 U.S. 249 (1970) 12, 14

28

1 *U.S. v. Warshak*,
 631 F.3d 266 (6th Cir. 2010)..... 12

2
 3 *Virginia v. Moore*,
 553 U.S. 164 (2008) 18, 21

4 **Federal Statutes**

5 50 U.S.C. § 1801(e)..... 25

6 50 U.S.C. § 1804(a)..... 22

7 50 U.S.C. § 1805(c)..... 22

8 50 U.S.C. § 1881a..... 21, 22, 25

9 **Constitutional Provisions**

10 U.S. Const., amend. IV..... *passim*

11 **Legislative Materials**

12 S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book*
 13 *II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 at 139 (1976) 18

14 **Other Authorities**

15 Barton Gellman, *How 160,000 Intercepted Communications Led To Our Latest NSA Story*,
 Washington Post, July 11, 2014 4

16 Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far*
 17 *Outnumber The Foreigners Who Are*, Washington Post, July 5, 2014 4

18 Dan York, *IPv4 Exhaustion Gets Real – Microsoft Runs Out Of U.S. Addresses For Azure Cloud –*
Time To Move To IPv6!, Internet Society (June 13, 2014) 7

19 Ingmar Poesse et al., *IP Geolocation Databases: Unreliable?*, ACM SIGCOMM Computer Comm.
 20 *Rev.*, April 2011 7

21 James Bamford, *The Agency That Might Be Big Brother*, New York Times, Dec. 25, 2005 19

22 Michael Barbaro and Tom Zeller, Jr., “A Face Is Exposed for AOL Searcher No. 4417749” (New
 York Times, Aug. 9, 2006)..... 13

23 Sen. Frank Church, Meet the Press, NBC, August 17, 1975..... 19

24 Testimony of the Hon. James Robertson (U.S. District Judge, ret.), “Workshop Regarding
 25 Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section
 702 of the Foreign Intelligence Surveillance Act,” Transcript at 35-37 (July 9, 2013)..... 22

26
 27
 28

1 **NOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGMENT**
2 **(Fourth Amendment Violation, Limited To The Government's Ongoing Seizure And**
3 **Searching Of Internet Communications)**

4 PLEASE TAKE NOTICE that on October 31, 2014 at 9:00 a.m. in Courtroom 5, Second
5 Floor, United States District Court, 1301 Clay Street, Oakland, CA, plaintiffs Carolyn Jewel, Erik
6 Knutzen, and Joice Walton will move for partial summary judgment holding that defendants
7 National Security Agency, United States, Department of Justice, Barack H. Obama, Michael S.
8 Rogers, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their official capacities) (collectively, the
9 "government defendants") have violated the Fourth Amendment rights of plaintiffs Jewel, Knutzen,
10 and Walton by seizing and searching their Internet communications.¹

11 The ground for this motion is that defendants are conducting an ongoing program of bulk,
12 untargeted seizure of the Internet communications of millions of innocent Americans, including
13 plaintiffs Jewel, Knutzen, and Walton, and subsequently searching many of those communications.
14 Plaintiffs' motion is based on the accompanying memorandum and declarations of Carolyn Jewel,
15 Erik Knutzen, Joice Walton, and Richard Wiebe, the filings and pleadings of record in this action
16 and the related action of *Hepting v. AT&T* (No. 06-cv-00672-VRW), and the argument and evidence
17 presented at the hearing of this motion.

18 In this motion, plaintiffs seek a determination that the government defendants are violating
19 the Fourth Amendment by their ongoing seizures and searches of plaintiffs' Internet
20 communications.

21 At this time, plaintiffs do not seek a determination of the government defendants' liability
22 for: a) past Fourth Amendment violations, including during periods that those activities were
23 conducted solely under presidential authority without any Foreign Intelligence Surveillance Court
24 order; b) *past or present* Fourth Amendment violations arising from government activities other than
25 Internet communications seizure or searching; or c) *past or present* violations of statutory and
26 constitutional provisions other than the Fourth Amendment. Those claims are outside the scope of

27 ¹ The other two plaintiffs, Tash Hepting and Young Boon Hicks (as executrix of the estate of
28 Gregory Hicks), are not joining in this motion as they are not current AT&T Internet customers.

1 this motion and are not at issue here. Plaintiffs also do not seek at this time a determination of the
2 appropriate remedy for the government defendants' ongoing Fourth Amendment violations.

3 MEMORANDUM OF POINTS AND AUTHORITIES

4 I. INTRODUCTION

5 The eyes and ears of the government now sit on the Internet. The government
6 indiscriminately copies and searches communications passing through the Internet's key domestic
7 junctions, on what is called the Internet "backbone." By doing so, the government is operating a
8 digital dragnet—a technological surveillance system that makes it impossible for ordinary
9 Americans not suspected of any wrongdoing to engage in a fully private online conversation, to
10 privately read online, or to privately access any online service. Millions of innocent Americans have
11 their communications seized and searched as part of this dragnet even when the government is not
12 targeting them or those with whom they communicate.

13 This unprecedented mass surveillance violates the core purpose of the Fourth Amendment—
14 to protect Americans' privacy against indiscriminate and suspicionless searches and seizures.
15 "Indiscriminate searches and seizures conducted under the authority of 'general warrants' were the
16 immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New*
17 *York*, 445 U.S. 573, 583 (1980); accord *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473, 2494
18 (2014).

19 The government's indiscriminate mass collection of Internet communications creates two
20 separate Fourth Amendment violations:

21 First, the government unconstitutionally seizes plaintiffs' Internet communications.
22 Technology at plaintiffs' Internet service provider, AT&T, automatically creates and delivers to the
23 government a copy of plaintiffs' online activities, along with those of millions of other innocent
24 Americans—including email, live chat, reading and interacting with websites, Internet searching,
25 and social networking.

26 Second, the government unconstitutionally searches the content of much of the
27 communications stream it has seized. The government admits that it searches the content of the
28

1 online communications that it has seized if it believes there is some indication that the origin or
2 destination of the communication is outside the United States.

3 The Fourth Amendment prohibits the government from intercepting, copying, or searching
4 through Americans' communications without a warrant issued by a neutral and detached magistrate,
5 upon probable cause, particularly describing the place to be searched and the things to be seized.
6 The government conducts the seizures and searches at issue here without a Fourth Amendment
7 warrant. While the government does obtain a periodic order from the Foreign Intelligence
8 Surveillance Court (FISC) approving its general "targeting" and "minimization" procedures, those
9 orders are simply not warrants. The FISC does not specify or limit the persons whose
10 communications the government may seize or search, the communications facilities or accounts
11 from which the government may seize communications, or what information the government may
12 search for within the seized communications. The government alone determines these, without any
13 judicial review. The FISC also does not make any determination that there is probable cause or
14 reasonable suspicion to believe that the government's seizures or searches will yield foreign
15 intelligence information.

16 In truth, no valid warrant could authorize the government's admitted practices here. The
17 government's targeting and minimization procedures are no substitute for the fundamental
18 protections that the Constitution guarantees to all Americans. The ongoing dragnet seizure and
19 search of innocent Americans' Internet activities violates the Fourth Amendment.

20 **II. STATEMENT OF FACTS**

21 **A. The Government Seizes And Searches Communications Flowing Through The** 22 **Nation's Internet Backbone**

23 The information revealed by a person's Internet activities paints an intimate and richly
24 detailed portrait of the person's life—often on a day-by-day or minute-by-minute basis. It is
25 precisely this deeply personal information that the government is seizing and searching. The
26 Washington Post recently examined a sample of 160,000 Internet communications intercepted and
27 retained by the NSA. Even after significantly more filtering and minimization than is at issue here,
28 the Post reported: "Many other files, described as useless by the analysts but nonetheless retained,

1 have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit
 2 sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and
 3 disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are
 4 catalogued and recorded nevertheless.”²

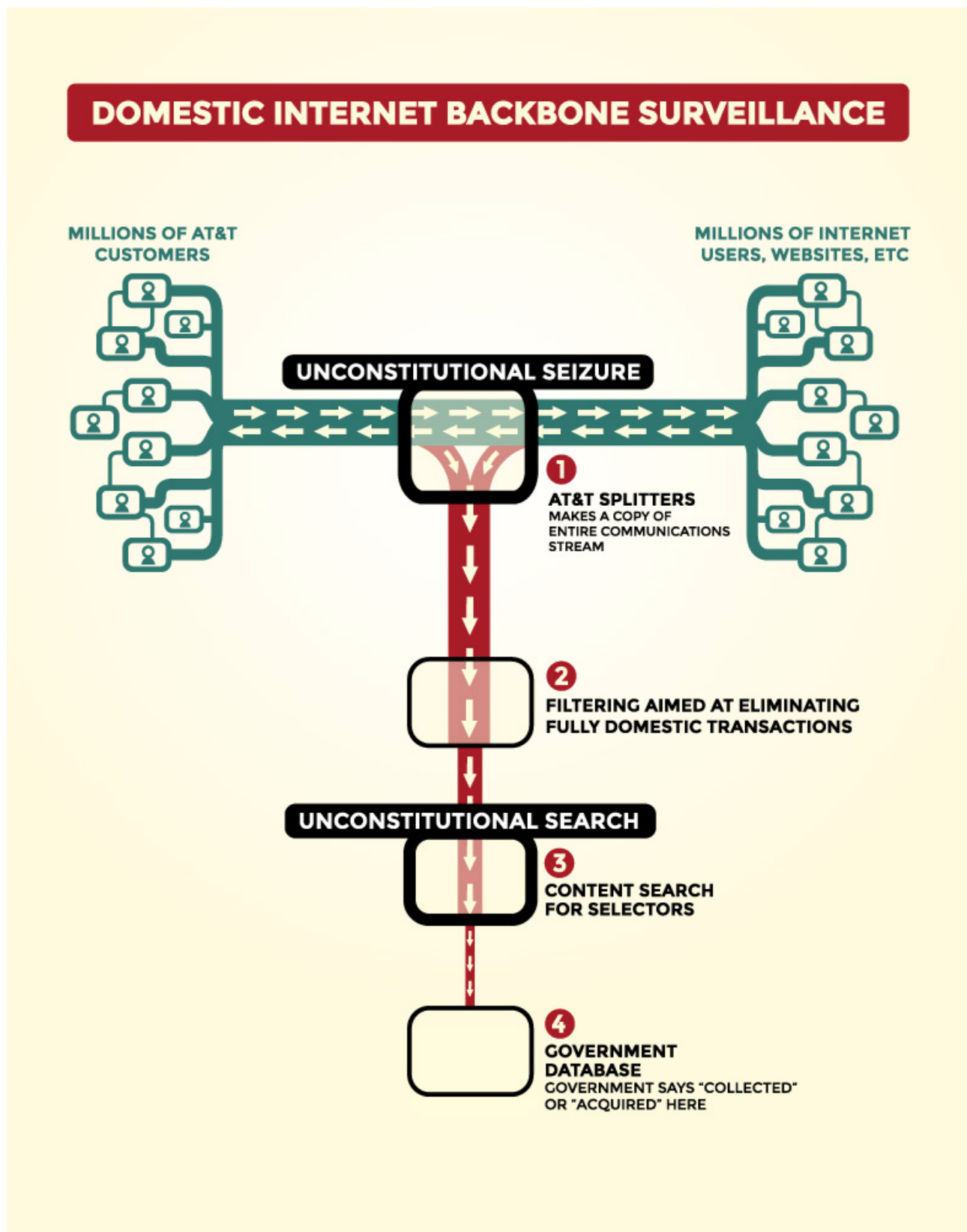
5 The government conducts its domestic surveillance by seizing and searching Internet
 6 communications as they flow through major fiber-optic network junctions on the Internet
 7 “backbone.”³ Almost all ordinary Internet traffic travels at some point over the Internet backbone—
 8 high-capacity, long-distance fiber-optic cables controlled by major Internet providers such as
 9 AT&T. The seizures at issue here occur on the junctions between AT&T and other providers on the
 10 backbone.

11
 12
 13
 14 ² Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far*
 15 *Outnumber The Foreigners Who Are*, Washington Post, July 5, 2014, available at
 16 http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html; see also Barton Gellman, *How 160,000 Intercepted Communications Led To Our Latest NSA Story*, Washington Post, July 11, 2014, available at
 17 http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html.

18
 19 ³ See, e.g., ECF No. 227 at ¶ 38, 25:14-16 (12/20/13 NSA Deputy Dir. Fleisch Classified Decl.)
 20 (“NSA collects electronic communications with the compelled assistance of electronic
 21 communications service providers as they transit Internet ‘backbone’ facilities within the United
 22 States”); ECF No. 169 at 17 (12/20/13 NSA Deputy Dir. Fleisch Unclassified Decl.); ECF No. 253-3
 23 at 3 (6/27/14 Gilligan Decl., Ex. B (The Intelligence Community’s Collection Programs Under Title
 24 VII of the Foreign Intelligence Surveillance Act)) (“NSA collects telephone and electronic
 25 communications as they transit the Internet ‘backbone’ within the United States”); 7/25/14 Wiebe
 26 Decl., Ex. A at 7, 35-37 (Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (“PCLOB 702 Report”) (July 2, 2014)); ECF No. 174-1 at 26 (1/10/14 Rumold Decl., Ex. 1 (Memorandum Opinion (“9/25/12 FISC Opinion”), [Name and docket no. redacted] (FISC Sept. 25, 2012)); Memorandum Opinion (“10/3/11 FISC Opinion”), [Name and docket no. redacted], 2011 WL 10945618, at *2 n.3 (FISC Oct. 3, 2011); 7/25/14 Wiebe Decl., Ex. B (NSA PRISM slides) at 3-4.

27 As these sources explain, the government also describes its Internet backbone seizures and searches
 28 as “upstream” collection.

1 As relevant to this motion, the government's surveillance process occurs in four stages,
2 illustrated below:



1 First, as shown in stage one, the government taps into the Internet backbone networks of the
2 nation's leading telecommunications carriers, including AT&T, giving it access to the entire stream
3 of domestic and international communications ("communications stream") carried on the fiber-optic
4 cables of those carriers. The communications stream includes *all* varieties of Internet activities,
5 including email, live chat, and Internet telephone and video calls, as well as activities such as web
6 browsing, video viewing, and search queries and results.⁴

7 To accomplish this access while not interrupting or slowing Internet communications carried
8 by AT&T, the communications stream is copied.⁵ The copying is done via a simple technology
9 called a fiber-optic "splitter."⁶ A splitter is a device that "splits" the light signals on a fiber-optic
10 cable, making identical copies of the communications stream carried on the cable.⁷ The splitters
11 installed at AT&T allow one copy of the communications stream to travel as it normally would to its
12 intended destination on the Internet while a second copy of the communications stream is diverted
13 for further processing and searching by the NSA.⁸

14 Second, as shown in stage two above, after the communications stream is copied, the
15 government roughly filters it in an attempt to eliminate wholly domestic communications and leave
16 only communications in which at least one end is located outside the United States.⁹ This filtering

17 ⁴ ECF No. 84-2 at ¶¶ 9, 19, 34 (Mark Klein Decl.). *See also, e.g., Joffe v. Google, Inc.*, 729 F.3d
18 1262, 1264 (9th Cir. 2013) (noting that analogous interception of WiFi network data "includes
19 everything transmitted by a device connected to a Wi-Fi network, such as personal emails,
usernames, passwords, videos, and documents").

20 ⁵ ECF No. 84-2 at ¶¶ 24-34 (Klein Decl.); ECF No. 89 at ¶¶ 56, 62, 72 (J. Scott Marcus Decl.).

21 ⁶ ECF No. 84-2 at ¶¶ 24-34 (Klein Decl.).

22 ⁷ ECF No. 84-2 at ¶¶ 21-22, 23-25 (Klein Decl.); ECF No. 89 at ¶¶ 56-58, 109 (Marcus Decl.).

23 ⁸ ECF No. 84-2 at ¶¶ 25-34 (Klein Decl.); ECF Nos. 84-3, 84-4, 84-5, 84-6 (Klein Decl., Exs. A, B,
24 C); ECF No. 89 at ¶¶ 56, 62, 70-73, 77 (Marcus Decl.); *see also* ECF No. 84-1 at ¶¶ 6, 10-12, 15,
19-23 (AT&T Managing Director-Asset Protection James Russell authenticating Klein Declaration
statements and documents).

25 ⁹ The government says it applies an Internet Protocol ("IP") filter to the seized communications in an
26 attempt to limit its search to only those communications that either terminate or originate abroad.
27 ECF No. 174-5 at 1-2 (1/10/14 Rumold Decl., Ex. 5 ("Procedures Used By The National Security
28 Agency For Targeting . . .")). An IP filter functions by sifting communications based on their
destination "IP address"—a numerical label assigned to each device connected to the Internet. (In
footnote continued on next page)

1 intentionally keeps communications between Americans and persons located abroad. Moreover, this
 2 filtering is imprecise as to purely domestic communications, resulting in a significant amount of
 3 purely domestic traffic in the filtered communications stream.¹⁰

4 Third, as shown in stage three above, the government searches the *entire contents* of the
 5 filtered communications stream for particular “selectors”—email addresses, domain names, phone
 6

7 *(footnote continued from previous page)*

8 the case of a home or business network, many computers or other devices may share the single IP
 9 address on the Internet that is assigned to the modem or router through which they connect to the
 10 Internet and, in some circumstances, it serves as a loose proxy for geographic location. However, IP
 11 filters are only rough indicators of physical location. ECF No. 89 at ¶¶ 110-11 (Marcus Decl.);
 12 Ingmar Poese, *et al.*, *IP Geolocation Databases: Unreliable?*, ACM SIGCOMM Computer Comm.
 Rev., April 2011, at 56 (reporting 2-4% error rates in country geolocation with commercial
 databases), available at <http://www.sigcomm.org/sites/default/files/ccr/papers/2011/April/1971162-1971171.pdf>.

13 Recently, for example, communications sent by accountholders on Microsoft servers in the United
 14 States appeared to IP geolocation filters to be communications that were originating from South
 15 America, not the United States. Dan York, *IPv4 Exhaustion Gets Real – Microsoft Runs Out Of U.S.
 16 Addresses For Azure Cloud – Time To Move To IPv6!*, Internet Society (June 13,
 2014), <http://www.internetsociety.org/deploy360/blog/2014/06/ipv4-exhaustion-gets-real-microsoft-runs-out-of-u-s-addresses-for-azure-cloud-time-to-move-to-ipv6>.

17 ¹⁰ One reason why the government’s filtering fails to exclude domestic communications is the
 18 inaccuracy of IP geolocation. See n.9 above. Another reason is that the pathway a communication
 19 takes on the Internet from its origin to its destination is unpredictable and can change with every
 20 transmission. A communication between two domestic parties can follow a path that takes it outside
 21 the United States for part of its journey; thus, as the FISC noted, “NSA’s upstream collection devices
 22 will acquire a wholly domestic ‘about’ [communication] if it is routed internationally.”
 23 10/3/11 FISC Opinion, 2011 WL 10945618, at *11. A third reason is that the websites and Internet
 24 services that appear to be domestic may be located anywhere in the world unbeknownst to the user.
 25 As the President’s Review Group noted: “Today, and unbeknownst to US users, websites and cloud
 26 servers may be located outside the United States. Even for a person in the US who never knowingly
 27 sends communications abroad, there may be collection by US intelligence agencies outside of the
 28 US.” 7/25/14 Wiebe Decl., Ex. F at 183 (President’s Review Group on Intelligence and
 Communications Technologies, *Liberty and Security in a Changing World*). The providers of
 Internet services may back up or store a user’s data on servers anywhere in the world. For example,
 Yahoo! provides the AT&T-branded email services that plaintiffs Knutzen and Walton use. Knutzen
 Decl. at ¶ 5; Walton Decl. at ¶ 5. The NSA has intercepted massive bulk shipments of user email
 accounts by Yahoo! between its United States and overseas servers, shipments that are completely
 unknown to the user. 7/25/14 Wiebe Decl., Ex. C at 2-3 (Special Source Operations Weekly,
 3/14/13 edition).

1 numbers, or other identifiers.¹¹ The government intentionally includes Americans' international
2 communications, including those of plaintiffs, in these searches. As noted above, the searches also
3 include many wholly domestic Internet communications.

4 In stage four, the results of the seizing and searching described above are then deposited into
5 government databases for retention.¹² It is only at this fourth stage in the process that the
6 government deems the information "collected" or "acquired."¹³ And it is only these retained
7 communications that the government takes into account in asserting that its Internet backbone
8 seizures and searches are "targeted," ignoring the first three stages outlined above. The

9
10 ¹¹ ECF No. 227 at ¶ 64, p. 45:6-9 (12/23/13 NSA Deputy Dir. Fleisch Classified Decl.);
11 7/25/14 Wiebe Decl., Ex. D at 7 (12/8/11 Monaco/Inglis/Litt Joint Statement); 10/3/11 FISC
12 Opinion, 2011 WL 10945618, at *5-*6; ECF No. 253-3 at 4 (The Intelligence Community's
13 Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act); ECF No. 254-1
14 at 8 (Corrected Defs. Reply Br. Re Preservation Orders) (citing 10/3/11 FISC Opinion,
15 2011 WL 10945618, at *10, *27); ECF No. 174-1 at 26 (9/25/12 FISC Opinion).

16 As these sources note, the government sometimes refers to communications whose contents contain
17 a reference to a selector as "about" communications.

18 ¹² The PCLOB 702 Report acknowledges: "The NSA's 'upstream collection' (described elsewhere
19 in this Report) may require access to a larger body of international communications than those that
20 contain a tasked selector." 7/25/14 Wiebe Decl., Ex. A at 111 n.476 (PCLOB 702 Report).

21 ¹³ See, e.g., 7/25/14 Wiebe Decl., Ex. A at 37 (PCLOB 702 Report), describing "acquired" as the
22 point of "ingest[ion] into government databases."

23 The government consistently uses terms like "collection" and "acquired" in its public discussions not
24 as ordinary people use those terms, but very specifically to mean a point *after* the government has
25 actual custody or control over communications. For instance, Department of Defense regulations
26 provide that information is considered to be *collected* only after it has been "received for use by an
27 employee of a DoD intelligence component," and that "[d]ata acquired by electronic means is
28 'collected' only when it has been processed into intelligible form," without regard to when the
information was initially acquired by a surveillance device. DOD 5240 1-R, Procedures Governing
the Activities of DOD Intelligence Components that Affect United States Persons § C.2.2.1 at 15
(Dec. 1982), provided in Plaintiffs' Federal Rule of Evidence Section 1006 Summary of Voluminous
Evidence, ECF No. 113 at 46:9-18. [Vol. II, Ex. 24, p.1070]. Similarly, DNI Clapper later explained
his Senate testimony in which, in response to a direct question from Senator Wyden, he denied
"collecting" data on millions or hundreds of millions of Americans by stating: "[T]here are honest
differences on the semantics when someone says 'collection' to me, that has a specific meaning,
which may have a different meaning to him [Senator Wyden]." Interview by Andrea Mitchell with
DNI James R. Clapper (June 8, 2013), *available at*
[http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-
2013/874-director-james-r-clapper-interview-with-andrea-mitchell](http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell).

1 communications the government retains at stage four are not at issue here. Instead, this motion
 2 challenges the constitutionality of the initial seizure and search: *stage one*, the wholesale seizure of
 3 the stream of Internet communications; and *stage three*, the searching, post-IP-filtering, of the
 4 contents of those communications for selectors.

5 The PCLOB 702 Report describes the overall process as follows, explicitly adopting the
 6 government's use of the term "acquire" as only occurring at stage four:

7 Once tasked, selectors used for the acquisition of upstream Internet transactions are
 8 sent to a United States electronic communication service provider to acquire
 9 communications that are transiting through circuits that are used to facilitate
 10 Internet communications, what is referred to as the "Internet backbone." The
 11 provider is compelled to assist the government in acquiring communications across
 12 these circuits. To identify and acquire Internet transactions associated with the
 Section 702-tasks selectors on the Internet backbone, Internet transactions are
 first filtered to eliminate potential domestic transactions, and then are screened to
 capture only transactions containing a tasked selector. Unless transactions pass
 both these screens, they are not ingested into government databases.

13 7/25/14 Wiebe Decl., Ex. A at 36-37 (PCLOB 702 Report) (citations omitted).¹⁴ As the PCLOB
 14 noted, "[n]othing comparable [to the government's Internet backbone surveillance] is permitted as a
 15 legal matter or possible as a practical matter with respect to analogous but more traditional forms of
 16 communication." *Id.* at 122.

17 **B. Seizure And Searching Of Plaintiffs' Communications From AT&T's Internet**
 18 **Backbone**

19 Plaintiffs Jewel, Knutzen, and Walton are AT&T Internet service subscribers. Jewel Decl. at
 20 ¶¶ 2-3; Knutzen Decl. at ¶¶ 2-3; Walton Decl. at ¶¶ 2-3. Each of them relies on the Internet to send
 21 and receive personal and professional emails, to stay in touch with friends and loved ones, and to
 22 conduct private activities including web browsing and social media. Jewel Decl. at ¶¶ 4-5, Knutzen
 23 Decl. at ¶¶ 4, 6; Walton Decl. at ¶¶ 4, 6. Plaintiff Carolyn Jewel is a novelist who communicates
 24 online with fans and members of the publishing industry and uses the Internet to research the

25 ¹⁴ "Nevertheless, the government has no ability to examine or otherwise make use of this larger body
 26 of communications, except to promptly determine whether any of them contain a tasked selector.
 27 Only those communications (or more precisely, 'transactions') that contain a tasked selector go into
 government databases." 7/25/14 Wiebe Decl., Ex. A at 111 n.476 (PCLOB 702 Report).

1 settings for her fiction. Jewel Decl. at ¶¶ 1, 5, 7. Plaintiff Erik Knutzen is a writer who blogs about
2 urban homesteading, staying in touch with others in his field via various online mediums. Knutzen
3 Decl. at ¶¶ 1, 7. Plaintiff Joice Walton is a recording artist who promotes her music on her
4 website and through social media and email. Walton Decl. at ¶¶ 1, 7-8.

5 As described above, at stage one, AT&T allows the government to seize the entire
6 communications stream of its customers carried on a portion of the Internet backbone. Thus, the
7 government has seized the electronic communications of each of these three plaintiffs. Additionally,
8 each of them has had their communications searched, as described in stage three above. At a
9 minimum, this includes their international communications since, like nearly all Internet users, each
10 plaintiff has routinely communicated with persons whose email service is hosted abroad (*see* Jewel
11 Decl. at ¶ 6; Knutzen Decl. at ¶ 8; Walton Decl. at ¶ 7), and each has visited websites that are hosted
12 abroad (*see* Jewel Decl. at ¶ 8; Knutzen Decl. at ¶ 9; Walton Decl. at ¶ 9).

13 No genuine issue of material fact exists that plaintiffs' provider AT&T is one of the Internet
14 backbone providers at issue. Even on the much more limited record that existed eight years ago, this
15 Court in *Hepting* (per Walker, C.J.) found that "AT&T and the government have for all practical
16 purposes already disclosed that AT&T assists the government in monitoring communication
17 content." *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 991-92 (N.D. Cal. 2006). The Klein and
18 Marcus evidence, described above, demonstrates the NSA's bulk seizure of the content of plaintiffs'
19 AT&T Internet communications from the Internet backbone.¹⁵ ECF No. 84-2 (Klein Decl.); ECF
20 No. 89 at ¶¶ 56-58, 62, 70-73, 77 (Marcus Decl.). The NSA Draft OIG Report also demonstrates
21 AT&T's participation. ECF No. 147, Ex. A (NSA Draft OIG Report). Specifically, the NSA Draft
22 OIG Report describes in detail the NSA's relationship with two telecommunications companies
23 described as "Company A" and "Company B" in the report, and observes that the NSA's
24 relationship with each company gives NSA access to large volumes of communications "transiting
25 the United States through fiber-optic cables, gateway switches, and data networks." *Id.* at 27-29, 33-

26
27 ¹⁵ AT&T's continuing participation in Internet seizure and collection was confirmed again in 2013
28 by the Wall Street Journal. ECF No. 174-2; *see also* ECF No. 174-4.

1 34. The report says that Company A and Company B were the two largest providers of international
 2 telephone calls into and out of the United States when surveillance began in 2001. *Id.* at 27. Federal
 3 Communications Commission records confirm that AT&T and MCI/Worldcom (now Verizon) were
 4 the country’s two largest international telephone call providers at that time. 7/25/14 Wiebe Decl.,
 5 Ex. E (Common Carrier Bureau, FCC, 1999 International Telecommunications Data at 29, fig. 9
 6 (Dec. 2000)).

7 **III. ISSUES FOR DECISION**

8 1. Does the warrantless, suspicionless seizure of plaintiffs’ communications as part of a
 9 mass seizure and copying of Internet communications violate the Fourth Amendment?

10 2. Does the warrantless, suspicionless searching of the contents of plaintiffs’ Internet
 11 communications violate the Fourth Amendment?

12 **IV. ARGUMENT**

13 **A. The Fourth Amendment’s Fundamental Principles—And The Warrant 14 Requirement—Apply With Full Force To The Digital World, And Protect Plaintiffs’ Private Internet Communications**

15 **1. The Fourth Amendment Guarantees Fundamental Personal Privacy By 16 Prohibiting Suspicionless, Indiscriminate Government Intrusions Into Americans’ Papers And Effects**

17 The Fourth Amendment is a fundamental guarantee of personal privacy, “a right of the
 18 people which ‘is basic to a free society.’” *Camara v. Municipal Court of San Francisco*, 387 U.S.
 19 523, 528 (1967). The Supreme Court has emphasized in “countless decisions” that “[t]he basic
 20 purpose of this Amendment . . . is to *safeguard the privacy and security of individuals against*
 21 *arbitrary invasions* by governmental officials.” *Id.* (emphasis added). As Justice Brandeis explained
 22 in his famous dissent in *Olmstead v. United States*, the Founders “sought to protect Americans in
 23 their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the
 24 government, the right to be let alone . . .” 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

25 Protecting privacy in personal communications such as plaintiffs’ Internet communications is
 26 one of the core principles of the Fourth Amendment. The Fourth Amendment expressly designates a
 27 person’s “papers” and “effects” as two of the four categories it shields from government intrusion.
 28 U.S. Const., amend. IV. The Amendment “embod[ies] a particular concern for government trespass

1 upon the areas (‘persons, houses, papers, and effects’) it enumerates.” *U.S. v. Jones*, 565 U.S. ___,
2 132 S. Ct. 945, 950 (2012). The Founders’ special protection for papers and effects stems directly
3 from their determination to prohibit the indiscriminate, suspicionless rummaging and seizure of any
4 person’s papers that the English Crown had conducted using “general warrants”—warrants that
5 failed to specify the papers that were sought, the person whose papers could be searched and seized,
6 or the place to which the search for the papers was limited. *Riley*, 134 S. Ct. at 2494; *Stanford v.*
7 *Texas*, 379 U.S. 476, 480-85 (1965); *Marcus v. Search Warrant of Property*, 367 U.S. 717, 726-29
8 & n.22 (1961).

9 The Fourth Amendment protects a person’s information in digital as well as physical form.
10 “The papers we create and maintain not only in physical but also in digital form reflect our most
11 private thoughts and activities.” *U.S. v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).
12 The Ninth Circuit has held *en banc* that emails “implicate[] the Fourth Amendment’s specific
13 guarantee of the people’s right to be secure in their ‘papers.’ The express listing of papers ‘reflects
14 the Founders’ deep concern with safeguarding the privacy of thoughts and ideas—what we might
15 call freedom of conscience—from invasion by the government.’ These records are expected to be
16 kept private and this expectation is ‘one that society is prepared to recognize as “reasonable.”’” *Id.*
17 at 964 (citations omitted); *accord U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

18 The Fourth Amendment also protects a person’s communications when they are in transit, as
19 are plaintiffs’ Internet communications here. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (“Whilst in
20 the mail, [letters] can only be opened and examined under like warrant, issued upon similar oath or
21 affirmation, particularly describing the thing to be seized, as is required when papers are subjected to
22 search in one’s own household.”); *accord U.S. v. Van Leeuwen*, 397 U.S. 249, 251 (1970); *U.S. v.*
23 *Choate*, 576 F.2d 165, 174 (9th Cir. 1978).

24 Even apart from the Fourth Amendment’s specific protection of “papers” and “effects,”
25 plaintiffs’ electronic communications are protected because plaintiffs have a reasonable expectation
26
27
28

1 of privacy in them.¹⁶ *Berger v. New York*, 388 U.S. 41, 51 (1967); *see also U.S. v. U.S. District*
2 *Court (Keith)*, 407 U.S. 297, 313 (1972) (hereinafter, “*Keith*”); *Katz v. U.S.*, 389 U.S. 347, 353
3 (1967).

4 The Supreme Court recently affirmed that the government’s search and seizure of digital
5 information implicates core Fourth Amendment values and triggers the warrant requirement. *Riley*,
6 134 S. Ct. at 2495 (“The fact that technology now allows an individual to carry such information in
7 his hand does not make the information any less worthy of the protection for which the Founders
8 fought.”). The Court specifically noted the protectable privacy interests one has in her Internet
9 browsing records, explaining, “Internet search and browsing history, for example, can be found on
10 an Internet-enabled phone and could reveal an individual’s private interests or concerns—perhaps a
11 search for certain symptoms of disease, coupled with frequent visits to WebMD.”¹⁷ *Id.* at 2490. The
12 Court went on to detail how a person’s digital information gives a complete picture of a person’s
13 most private thoughts and actions—even beyond what a general search of their home might reveal.
14 *Id.* at 2489-91.

15 The Supreme Court’s conclusion that the digital information in cell phones is protected by
16 the Fourth Amendment because, “[w]ith all they contain and all they may reveal, they hold for many
17 Americans ‘the privacies of life’” (*Id.* at 2494-95) is equally, if not more, applicable to the digital
18 information plaintiffs transmit over the Internet. The Court noted:

19 First, a cell phone collects in one place many distinct types of information—an
20 address, a note, a prescription, a bank statement, a video—that reveal much more in
21 combination than any isolated record. Second, a cell phone’s capacity allows even
just one type of information to convey far more than previously possible. The sum of

22 ¹⁶ The “reasonable expectation of privacy test” is the alternative test for the scope of Fourth
23 Amendment protections. *See U.S. v. Jones*, 132 S. Ct. at 950, 953; *id.* at 954-55 (Sotomayor, J.,
concurring); *id.* at 959-60 (Alito, J., concurring).

24 ¹⁷ The power of browsing and search history to reveal a person’s life was demonstrated in 2006
25 when AOL inadvertently released the three-month search history of over 650,000 AOL users. *Doe I*
26 *v. AOL LLC*, 552 F.3d 1077, 1079 (9th Cir. 2009). Even though AOL did not release the names of
27 the users, it was an easy task for reporters to use an individual’s browsing history to identify and
track down the individual. Michael Barbaro and Tom Zeller, Jr., “A Face Is Exposed for AOL
Searcher No. 4417749” (New York Times, Aug. 9, 2006), *available at*
<http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all>.

1 an individual's private life can be reconstructed through a thousand photographs
2 labeled with dates, locations, and descriptions; the same cannot be said of a
3 photograph or two of loved ones tucked into a wallet. Third, the data on a phone can
4 date back to the purchase of the phone, or even earlier. A person might carry in his
pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of
all his communications with Mr. Jones for the past several months, as would routinely
be kept on a phone.

5 *Id.* at 2489. This same information about a person can be determined from their stream of
6 communications flowing through the Internet backbone. Indeed, the Court noted that much of the
7 information it was protecting in *Riley* is increasingly not stored on phones themselves but in the
8 Internet "cloud," with phones used to access the information over the Internet. *Id.* at 2491. Thus, the
9 Fourth Amendment privacy interests in digital information that the Supreme Court recognized in
10 *Riley* are fully applicable to the Internet activities of plaintiffs that the government is seizing—
11 emails, web browsing and searching, live chat, voice calls, social networking, photos, videos, or
12 otherwise.

13 **2. The Fourth Amendment's Warrant Requirement Is The Time-Tested**
14 **Mechanism That Prevents Government Overreaching And Suspicionless**
15 **Searches, And It Applies To Digital Seizure And Searching Of Electronic**
16 **Communications**

16 Like other "papers" and "effects," plaintiffs' electronic communications can only be seized
17 and searched with a warrant issued by a neutral and detached judicial officer, supported by probable
18 cause and describing with particularity the communications to be seized. *See Ex parte Jackson*, 96
19 U.S. at 733; *Van Leeuwen*, 397 U.S. at 251. National security does not excuse the need for a warrant
20 to intercept or search plaintiffs' communications. "It is now clear that [the warrant] requirement
21 attaches to national security wiretaps that are not directed against foreign powers or suspected agents
22 of foreign powers." *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986) (Scalia, Circuit
Justice, for the court).

23 The warrant requirement is not a dusty formalism but *the* tested method for protecting
24 Americans' privacy against government intrusion. The Supreme Court recently affirmed: "Our
25 cases have historically recognized that the warrant requirement is an 'important working part of our
26 machinery of government,' not merely an 'inconvenience to be somehow weighed against'" the
27 government's interest in proceeding without a warrant. *Riley*, 134 S. Ct. at 2493 (citations omitted).
28

1 Its two components are probable cause and the particularity requirement, both judged before any
2 search or seizure occurs by an independent and detached judicial officer. U.S. Const., amend. IV.

3 The probable cause requirement ensures that no search occurs where there is less than
4 probable cause or, worse, no suspicion at all. *Keith*, 407 U.S. at 316 (“The further requirement of
5 ‘probable cause’ instructs the magistrate that baseless searches shall not proceed.”); *Coolidge v. New*
6 *Hampshire*, 403 U.S. 443, 467 (1971) (same). It also serves to limit the scope of the search. *In re*
7 *Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9th Cir. 1991).

8 The particularity requirement ensures that “those searches deemed necessary [are] as limited
9 as possible.” *Coolidge*, 403 U.S. at 467. The “need for particularity” “is especially great in the case
10 of [electronic] eavesdropping” because it “involves an intrusion on privacy that is broad in scope.”
11 *Berger*, 388 U.S. at 56. It ensures that “the search will be carefully tailored to its justifications,”
12 eliminating the threat of “general searches.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The
13 particularity requirement also makes general searches “impossible” by ensuring that when it comes
14 to what can be searched or seized, “nothing is left to the discretion of the officer executing the
15 warrant.” *Marron v. U.S.*, 275 U.S. 192, 195-96 (1927); *see also Berger*, 388 U.S. at 49-50, 56, 58-
16 59; *U.S. v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003) (“Search warrants . . . are fundamentally
17 offensive to the underlying principles of the Fourth Amendment when they are so bountiful and
18 expansive in their language that they constitute a virtual, all-encompassing dragnet of personal
19 papers and property to be seized at the discretion of the State.”).

20 Judicial warrants based on particularity and probable cause are especially crucial in
21 electronic surveillance, where searches and seizures occur without leaving a trace and where the
22 threat to privacy is especially great. *Keith*, 407 U.S. at 313 (“the broad and unsuspected
23 governmental incursions into conversational privacy which electronic surveillance entails necessitate
24 the application of Fourth Amendment safeguards”). “Few threats to liberty exist which are greater
25 than that posed by the use of eavesdropping devices.” *Berger*, 388 U.S. at 63; *accord Olmstead*, 277
26 U.S. at 476 (1928) (Brandeis, J., dissenting) (“writs of assistance and general warrants are but puny
27 instruments of tyranny and oppression when compared with wire-tapping”). Because electronic
28

1 seizures of communications occur by stealth, they can easily “evade[] the ordinary checks that
2 constrain abusive law enforcement practices.” *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

3 The warrant requirement is therefore essential: the alternative of “bypassing a neutral
4 predetermination of the scope of a search leaves individuals secure from Fourth Amendment
5 violations ‘only in the discretion of the [government].’” *Katz*, 389 U.S. at 358-59. “[P]ost-
6 surveillance review would never reach the surveillances which failed to result in prosecutions. Prior
7 review by a neutral and detached magistrate is the time-tested means of effectuating Fourth
8 Amendment rights.” *Keith*, 407 U.S. at 318 (citation omitted). This concern is heightened in the
9 case of mass surveillance, where the overwhelming majority of those whose communications are
10 seized and searched are not even suspected of a crime or of being an agent of a foreign power. As
11 the Supreme Court recently affirmed: “[A] warrant ensures that the inferences to support a search
12 are ‘drawn by a neutral and detached magistrate instead of being judged by the officer engaged in
13 the often competitive enterprise of ferreting out crime.’” *Riley*, 134 S. Ct. at 2482.¹⁸

14 **B. Stage One: The Government’s Warrantless, Suspicionless Mass Seizure Of**
15 **Domestic Internet Communications Violates The Fourth Amendment**

16 The government’s seizure of the contents of the Internet activities of plaintiffs and millions
17 of other Americans at the Internet backbone facilities of AT&T—the first stage of the government’s
18 surveillance—is unconstitutional. It is a general seizure that is not, and never could be, authorized
19 by a valid warrant. As this Court (per Walker, C.J.) previously concluded: “Because the alleged
20 dragnet here encompasses the communications of ‘all or substantially all of the communications
21 transmitted through [AT&T’s] key domestic telecommunications facilities,’ it cannot reasonably be
22 said that the program as alleged is limited to tracking foreign powers. Accordingly, AT&T’s alleged
23 actions here violate the constitutional rights clearly established in *Keith* [requiring a warrant for
24 electronic surveillance of persons who are not agents of foreign powers].” *Hepting*, 439 F. Supp. 2d
25 at 1010.

26 ¹⁸ As described further in Section D(1) below, the Supreme Court also firmly rejected the notion that
27 government protocols alone could substitute for a warrant: “[T]he Founders did not fight a
28 revolution to gain the right to government agency protocols.” *Riley*, 134 S. Ct. at 2491.

1 The Court's conclusion remains correct. Because the contents of plaintiffs' communications
2 fall within the Fourth Amendment's categorical protection of a person's "papers" and "effects," the
3 warrantless copying done at the Internet backbone is *per se* a Fourth Amendment violation. *See*
4 *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) ("When the Government obtains information by
5 physically intruding on persons, houses, papers, or effects, a search within the original meaning of
6 the Fourth Amendment has undoubtedly occurred." (internal quotation marks omitted)); *Jones*, 132
7 S. Ct. at 950 n.3. Independently, plaintiffs also have a reasonable expectation of privacy in their
8 communications, which is violated when the government seizes their communications without a
9 warrant. *Katz*, 389 U.S. at 353, 356-59; *Berger*, 388 U.S. at 55-64; *Halperin v. Kissinger*, 807 F.2d
10 at 185.

11 No warrant could justify the mass, suspicionless seizures occurring here. Even in cases of
12 seizures under valid warrants, the Ninth Circuit has routinely invalidated wholesale seizure of
13 documents as a violation of the Fourth Amendment. Although the Court has noted that "all items in
14 a set of files may be inspected during a search" in order to find the particular documents described in
15 a warrant whose seizure is supported by probable cause, "the wholesale *seizure* for later detailed
16 examination of records not described in a warrant is significantly more intrusive" and is precisely
17 "the kind of investigatory dragnet that the fourth amendment was designed to prevent."
18 *U.S. v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (quoting *U.S. v. Abrams*, 615 F.2d 541, 543
19 (1st Cir. 1980)) (italics original).

20 Similarly, in *U.S. v. Kow*, 58 F.3d 423 (9th Cir. 1995), the Ninth Circuit found that a search
21 warrant that "contained no limitations on which documents . . . could be seized or suggested how
22 they related to specific criminal activity" failed the particularity requirement. 58 F.3d at 427. The
23 Court held that "generalized seizure" of a large group of documents may be justified only if there is
24 a showing that there is probable cause that the entire set of records are likely to show evidence of
25 criminal activity. *Id.*

26 In the Fourth Amendment, the Founders "emphasize[d] the purpose to protect against all
27 general searches. Since before the creation of our government, such searches have been deemed
28 obnoxious to fundamental principles of liberty. . . . The need of protection against them is attested

1 alike by history and present conditions.” *Go-Bart Importing Co. v. U.S.*, 282 U.S. 344, 357 (1931).
2 “Opposition to such searches was in fact one of the driving forces behind the Revolution itself.”
3 *Riley*, 134 S. Ct. at 2494. “The immediate object of the Fourth Amendment was to prohibit the
4 general warrants and writs of assistance that English judges had employed against the colonists,”
5 *Virginia v. Moore*, 553 U.S. 164, 168-69 (2008), and its words “reflect the determination of those
6 who wrote the Bill of Rights that the people of this new Nation should forever ‘be secure in their
7 persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the
8 unbridled authority of a general warrant,” *Stanford*, 379 U.S. at 481-82.

9 The government’s indiscriminate, suspicionless bulk seizure of plaintiffs’ Internet activities
10 here is the modern-day equivalent of the hated “general warrants” that the Fourth Amendment was
11 meant to stamp out forever. As the Supreme Court explained in *Marcus*, it was precisely this power
12 to seize papers and effects indiscriminately, in bulk, and without particularized suspicion—the same
13 conduct the government is engaging in here—that made general warrants objectionable as “totally
14 subversive of the liberty of the subject.” *Marcus*, 367 U.S. at 728-29. This is equally true today, as
15 the Supreme Court recently reaffirmed in *Riley*.

16 Because of this clear historical antipathy towards general warrants, the nation has never had
17 to address dragnet surveillance anything like the government’s practices here. The most analogous
18 situation was the NSA’s post-World War II “Operation Shamrock,” where, with the cooperation of
19 the telegraph companies, the NSA collected copies of each and every international telegram that was
20 sent into and out of the United States from 1945 to 1975. The constitutionality of that mass
21 collection was never considered by the courts, but Congress did address it and the Church
22 Committee, charged with investigating the mass surveillance, concluded that it violated the Fourth
23 Amendment rights of those who sent telegrams. S. Select Comm. to Study Governmental
24 Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of*
25 *Americans*, S. Rep. No. 94-755 at 139 (1976).¹⁹ Indeed, Senator Church warned:

26
27 _____
28 ¹⁹ Available at http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf.

1 [The government's] capability at any time could be turned around on the American
 2 people, and no American would have any privacy left, such is the capability to
 3 monitor everything: telephone conversations, telegrams, it doesn't matter. There
 4 would be no place to hide.²⁰

5 Such surveillance alters "the relationship between citizen and government in a way that is inimical
 6 to a democratic society," *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citation omitted), by
 7 creating the specter that the government can peer into its citizens' private communications at any
 8 moment.

9 If the Fourth Amendment means anything, it means that the government may not engage in
 10 indiscriminate, suspicionless, mass surveillance of its own citizens. But that is exactly what the
 11 government has done here, by sitting on the Internet and seizing plaintiffs' communications as they
 12 pass through AT&T's facilities. That seizure violates the Fourth Amendment.

13 **C. Stage Three: The Government's Warrantless, Suspicionless Searching Of The
 14 Contents Of Plaintiffs' Internet Communications Is Unconstitutional**

15 The Fourth Amendment is independently violated by the government's warrantless and
 16 indiscriminate content searching of plaintiffs' Internet communications after it seizes them—stage
 17 three of the government's surveillance.²¹ To find targeted "selectors," *i.e.*, email addresses, websites
 18 or similar identifiers of one or multiple persons or entities, the government undisputedly searches the
 19 contents of vast numbers of innocent Americans' Internet activities, both international and
 20 domestic.²² This includes plaintiffs, none of whom has been suspected of any wrongdoing but each

21 ²⁰ Sen. Frank Church, Meet the Press, NBC, August 17, 1975, *available at* <http://www.nbcnews.com/video/meet-the-press/52669547#52669547>, at 5:50 to 6:40, and *quoted in* James Bamford, *The Agency That Might Be Big Brother*, New York Times, Dec. 25, 2005, *available at* <http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=print>.

22 ²¹ Seizing and searching the communications of known foreign terrorists, even if constitutional, does
 23 not give the government license to circumvent the warrant requirement in searching *plaintiffs'*
 24 communications. The Fourth Amendment does not sanction "constitutionality by proximity:" a
 25 warrant to search your neighbor's house does not validate a search of your house. *See U.S. v.*
 26 *Collins*, 845 F.2d 145, 145-46 (1987).

27 ²² As noted above, the government's filtering (stage two in the figure on page 5) for some indication
 28 of foreignness is imperfect. *See supra* at nn. 9-10. But even if stage two filtering were completely
 effective, the stage three searching is intended to, and does, search the contents of communications
 of plaintiffs and millions of other "United States persons" within the United States who are not
 surveillance targets and who are not suspected of being agents of a foreign power or possessing
 (*footnote continued on next page*)

1 of whom has attested to communications with people abroad and visiting websites hosted abroad.
2 See Jewel Decl. at ¶¶ 6, 8; Knutzen Decl. at ¶¶ 8, 9; Walton Decl. at ¶¶ 8, 9. Because these
3 suspicionless searches of plaintiffs’ Internet activities are conducted without a warrant, they violate
4 the Fourth Amendment.

5 Like the unconstitutional seizures discussed above, the government’s warrantless searching
6 of the communications of persons suspected of no wrongdoing is nothing more than a suspicionless
7 and unconstitutional general search at the government’s discretion. It is the same “general,
8 exploratory rummaging” that the Fourth Amendment prohibits. *Andresen v. Maryland*, 427 U.S.
9 463, 480 (1976). Like general warrants, searching the communications stream of millions of
10 persons for “selectors” (without any suspicion of the persons whose communications are searched)
11 gives the government “the most general discretionary authority,” *Marcus*, 367 U.S. at 726; has no
12 limits on place or duration, *id.* at 729 n.22; and “provide[s] no judicial check on the determination of
13 the executing officials that the evidence available justifie[s] an intrusion,” *Steagald v. U.S.*, 451 U.S.
14 204, 220 (1981).

15 Moreover, the searches here are more extensive than even the broadest general warrant, since
16 the government performs its content searches on the entire post-filtering communications stream.
17 Searching of the communications stream means that hundreds of millions of communications are
18 searched that do *not* contain the selectors along with the relatively few that do. These
19 communications that are searched and found not to contain the selectors are the communications of
20 millions of innocent Americans with no connection to any surveillance target. For comparison, for
21 the colonial general warrants to be the equivalent of the searches here, the British troops would have
22 had to search *every* home that ever received a package from abroad. This fact is elided in the
23 government’s assertions regarding its collection from the Internet backbone, in which it claims, for
24 instance, that it ultimately retains only roughly 22 million electronic communications in 2011. See

25
26 *(footnote continued from previous page)*

27 foreign intelligence information. Whether the searching is of all plaintiffs’ communications or only
28 their international or internationally transiting communications after stage two filtering does not
change the conclusion of unconstitutionality.

1 ECF No. 254-1 at 7:16-17. As described above, the government here is only counting the
2 communications it retains at the end (stage four in the figure above), not all those it searches (stage
3 three). This is akin to the British only counting the homes where they found some evidence of
4 smuggling, not all of those they searched pursuant to their general warrants.

5 The government's searches are unconstitutional because the government has no warrant
6 authorizing its content searching, and because the searches are indiscriminate and suspicionless
7 general searches that no warrant could properly authorize.

8 **D. The Government's Defenses Fail**

9 **1. Section 702 Orders Cannot Substitute For Constitutionally-Required** 10 **Warrants**

11 The government's chief affirmative defense for the legality of its domestic Internet backbone
12 seizures and content searching has been that it currently conducts these activities under color of a
13 FISC Order under section 702 of the FISA Amendments Act (50 U.S.C. § 1881a). This defense
14 fails.

15 The section 702 orders upon which the government relies to conduct its Internet backbone
16 seizures and searches are nothing like warrants, and they do not satisfy the Fourth Amendment.
17 Section 702 orders only approve protocols for future seizures by the government. But as the
18 Supreme Court explained in *Riley*: “[T]he Founders did not fight a revolution to gain the right to
19 government agency protocols.” *Riley*, 134 S. Ct. at 2491. And of course, neither section 702, nor
20 any order issued under it, can relax the Fourth Amendment's requirements. The Fourth Amendment
21 is not merely a “redundant guarantee of whatever limits on search and seizure legislatures might
22 have enacted.” *Virginia v. Moore*, 553 U.S. at 168.

23 Section 702 orders have none of the features required for a valid, constitutional warrant. In
24 sharp contrast to the particularity and probable cause requirements of warrants, section 702 orders
25 are periodic administrative approvals by the FISC of very generalized targeting and minimization
26 procedures. Under section 702, the government proposes these procedures and then negotiates their
27 terms with the FISC if it raises any objections. In doing so, the FISC acts in essence as an
28

1 administrative agency engaged in prospective rulemaking, not as a court issuing a warrant.²³ Indeed,
2 unlike a warrant or a traditional FISA order, a FISC order under section 702 does not authorize the
3 search or seizure of anything from anyone. Rather, the Executive subsequently decides what
4 communications to seize and compels the seizure by issuing directives to telecommunications
5 providers. 50 U.S.C. § 1881a(h)(1).

6 For comparison, under a traditional FISA order, the government would be required in
7 support of its application to specify to the FISC its surveillance targets, what evidence supports the
8 belief that the targets are agents of a foreign power and that surveillance of their communications is
9 likely to yield foreign intelligence information, what communications facilities it will subject to
10 surveillance, and what information the government's surveillance is seeking. 50 U.S.C. § 1804(a);
11 *see* 7/25/14 Wiebe Decl., Ex. A at 24 (PCLOB 702 Report). The order would be limited to
12 surveillance of the communications of particular identified targets and could not authorize mass
13 suspicionless seizures as are occurring here. 50 U.S.C. § 1805(c).

14 In contrast, the decisions about the actual surveillance conducted pursuant to a section 702
15 order are made by the Executive without any judicial review. A section 702 order does not specify
16 or limit the persons whose communications the government may seize or search, the
17 communications facilities or accounts from which the government may seize communications, or
18 what information the government may search for within the seized communications. 50 U.S.C.
19 § 1881a(i)(1)(A), (i)(2), (i)(3)(A); 7/25/14 Wiebe Decl., Ex. A at 24-25, 27 (PCLOB 702 Report).
20 The FISC never determines whether there is probable cause (or any level of suspicion) that seizing
21 the communications from a particular Internet backbone facility will yield the communications of a
22 non-U.S. person located outside the United States who possesses foreign intelligence information.
23 7/25/14 Wiebe Decl., Ex. A at 24-25, 27 (PCLOB 702 Report). As to searching of the seized
24 communications, the FISC never determines whether there is probable cause (or any level of
25

26 ²³ *See, e.g.,* Testimony of the Hon. James Robertson (U.S. District Judge, ret.), “Workshop
27 Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and
28 Section 702 of the Foreign Intelligence Surveillance Act,” Transcript at 35-37 (July 9, 2013),
available at <http://www.pclob.gov/All Documents/July 9, 2013 Workshop Transcript.pdf>.

1 suspicion) that each (or even any) of the communications the government is searching will yield
2 evidence of wrongdoing or foreign intelligence information, or that the persons whose
3 communications are searched are non-U.S. persons located outside the United States. *Id.* No court
4 ever reviews the selectors that the government uses to search the contents of communications of
5 persons like plaintiffs not suspected of anything. ECF No. 253-3 at 2-3 (The Intelligence
6 Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act).
7 The Executive alone makes all of these decisions without judicial oversight. These are
8 impermissible general seizures and searches.

9 Section 702 involves far less judicial scrutiny than even the electronic surveillance statute the
10 Supreme Court found constitutionally inadequate in *Berger*, the case that launched the application of
11 the Fourth Amendment to electronic surveillance. In *Berger*, the Supreme Court considered a state
12 statute that authorized electronic surveillance and required prior judicial approval, but did not
13 require as part of that approval either probable cause or a description of the particular conversations
14 to be seized. Among its deficiencies, the Court noted that naming the surveillance target “does no
15 more than identify the person whose constitutionally protected area is to be invaded rather than
16 ‘particularly describing’ the communications, conversations, or discussions to be seized.” 388 U.S.
17 at 59. The Court found the electronic surveillance statute in *Berger* unconstitutional, even though it
18 required prior judicial approval, because it authorized “indiscriminate use of electronic devices” and
19 “actually permits general searches by electronic devices.” *Id.* at 58.

20 The Fourth Amendment requires a warrant before plaintiffs’ Internet activities may be seized
21 from the Internet backbone and searched because the personal privacy interests the Fourth
22 Amendment protects are at their zenith here. Only enforcement of the warrant requirement—by
23 requiring a particularized description of the communications to be seized and the places from which
24 they are to be seized, and by requiring a judicial determination that probable cause exists to support
25 the seizure and search—can adequately protected plaintiffs’ privacy interests in their Internet
26 activity.

2. The “Special Needs” Exception Cannot Justify The Government’s Dragnet

“In most circumstances, searches and seizures conducted without a warrant are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Al Haramain Islamic Foundation, Inc. v. U.S. Department of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011) (quoting *Katz*, 389 U.S. at 357).

The warrantless, suspicionless mass seizures of communications occurring here cannot be justified under the “special needs” exception to the warrant requirement. *See Chandler v. Miller*, 520 U.S. 305, 313-14 (1997). As the Supreme Court has explained, “When such ‘special needs’—concerns other than crime detection—are alleged in justification of a Fourth Amendment intrusion, courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties.” *Id.* (internal citations omitted).

The “special needs” exception is a “closely guarded category.” *Chandler*, 520 U.S. at 309. Its requirements are rigorous: “In limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of [individualized] suspicion.” *Id.* at 314.

Here, the suspicionless mass seizure of Americans’ Internet communications fails the first prong of the “special needs” exception. Plaintiffs’ privacy interest in their Internet activities, far from being “minimal,” lies at the heart of the Fourth Amendment. As previously described, a person’s Internet activities encompass a vast array of intimate details about that person’s private life. The government intrudes massively on plaintiffs’ privacy interest in their Internet activities by copying every single one of plaintiffs’ communications passing through the Internet backbone. It also does so by content-searching a subset of plaintiffs’ Internet activity filtered by IP address, without any individualized suspicion.

Nor does the important purpose of the government’s surveillance overcome its massive intrusion into the privacy of plaintiffs and millions of other Americans. Although “the government’s interest in preventing terrorism . . . is extremely high,” the importance of that interest “is no excuse for the dispensing altogether with domestic persons’ constitutional rights.” *Al Haramain Islamic*

1 *Foundation*, 686 F.3d at 993; *see also Keith*, 407 U.S. at 316-21 (rejecting government’s argument
 2 that national security required dispensing with the warrant requirement in domestic security
 3 surveillance cases). “Emergency does not create power. Emergency does not increase granted
 4 power or remove or diminish the restrictions imposed upon power granted or reserved. . . . [¶] . . .
 5 [E]ven the war power does not remove constitutional limitations safeguarding essential liberties.”
 6 *Home Building & Loan Ass’n v. Blaisdell*, 290 U.S. 398, 425-26 (1934). Allowing even legitimate
 7 national security concerns to override the most fundamental of Fourth Amendment protections—the
 8 prohibition on the modern-day equivalent of the despised “general warrant”—would turn the
 9 Constitution on its head and destroy the basic civil liberties that the Founders fought to protect.²⁴

10 **V. CONCLUSION**

11 The government’s indiscriminate, suspicionless seizures and content searches at issue here
 12 violate the fundamental privacy rights of plaintiffs and millions of other Americans, as guaranteed
 13 by the Fourth Amendment. The Fourth Amendment requires that the government must obtain a
 14 warrant by showing individualized suspicion, probable cause, and a particularized description of the
 15 communications to be seized or searched. Enforcing those bedrock Fourth Amendment
 16 requirements here is necessary to keep the government within constitutional bounds, and to preclude
 17 the general searches and seizures the government is now conducting.

18 For the foregoing reasons, plaintiffs respectfully request that the Court rule that (1) the
 19 government’s seizure of plaintiffs’ Internet communications violates the Fourth Amendment
 20 and (2) the government’s content searching of plaintiffs’ Internet communications violates the
 21 Fourth Amendment.

22 ²⁴ Moreover, the government’s purpose is far broader than simply addressing terrorist threats.
 23 Section 702 permits collection of any “foreign intelligence information,” a broadly-defined category
 24 that includes information that relates to national defense or foreign affairs. 50 U.S.C. § 1801(e).
 25 And even as to that category, section 702 requires only that foreign intelligence be a *significant*
 26 purpose of the investigation, not the sole or even primary purpose. 50 U.S.C. § 1881a(g)(2)(A)(v).
 27 This is far beyond the limited category of important government interests that could justify
 28 dispensing with the warrant requirement of the Fourth Amendment. In addition, the fruits of section
 702 seizures and searches are admittedly used for even more remote purposes. They include, as a
 “routine practice,” searching by the FBI in ordinary criminal cases, thus rendering the special needs
 exception inapplicable. *See* 7/25/14 Wiebe Decl., Ex. A at 137-38 (PCLOB 702 Report).

1 Dated: July 25, 2014

Respectfully submitted,

2
3 /s/ Richard R. Wiebe

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

4
5 CINDY COHN
6 LEE TIEN
7 KURT OPSAHL
8 JAMES S. TYRE
9 MARK RUMOLD
10 ANDREW CROCKER
11 DAVID GREENE
12 ELECTRONIC FRONTIER FOUNDATION

13 THOMAS E. MOORE III
14 ROYSE LAW FIRM

15 RACHAEL E. MENY
16 MICHAEL S. KWUN
17 BENJAMIN W. BERKOWITZ
18 AUDREY WALTON-HADLOCK
19 JUSTINA K. SESSIONS
20 PHILIP J. TASSIN
21 KEKER & VAN NEST LLP

22 ARAM ANTARAMIAN
23 LAW OFFICE OF ARAM ANTARAMIAN

24
25
26
27
28
Counsel for Plaintiffs