U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2015 JUN 12 PM 5:08
LEEANN FLYNN HALL
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE MOTION IN OPPOSITION TO GOVERNMENT'S REQUEST TO RESUME BULK DATA COLLECTION UNDER PATRIOT ACT SECTION 215

Docket No. Misc. 15-01

RESPONSE TO MOTION IN OPPOSITION TO GOVERNMENT'S REQUEST TO RESUME BULK DATA COLLECTION UNDER PATRIOT ACT SECTION 215

~~The United States of America submits this Response to the Motion in Opposition~~ to Government's Request to Resume Bulk Data Collection Under Patriot Act Section 215. Pursuant to the Court's June 5, 2015, Order, this Response is "limited to the merits of whether the bulk acquisition of non-content call-detail records is lawful under Title V of the Foreign Intelligence Surveillance Act (FISA), as amended by the USA FREEDOM Act of 2015, Public Law No. 114-23, and consistent with the Fourth Amendment to the Constitution."[1] As described more fully below, and in the Memorandum of Law filed by the Government on June 2, 2015, Section 1861 of FISA, as amended by the USA PATRIOT Act and the USA FREEDOM Act, authorizes the Court to approve the

[1] As directed by the Court in its June 5, 2015, Order, this Response does not address whether Movants' have standing under FISA or Article III of the Constitution. The Government, however, does not concede that Movants have standing of any kind.

Government's application for the bulk production to the National Security Agency (NSA) of non-content call detail records for a 180-day transition period, subject to the restrictions and limitations regarding the handling of such data as set forth in this Court's prior Orders. Production of such records pursuant to Section 1861, furthermore, is consistent with the Fourth Amendment to the Constitution.

I. Section 1861 of FISA, as Amended by the USA FREEDOM Act, Authorizes this Court to Approve the Bulk Production of Call Detail Records.

Since 2006, pursuant to Section 215 of the USA PATRIOT Act, this Court has authorized the collection, in bulk, of call detail records (telephony metadata), subject to a number of restrictions, including the limitation that the data can only be queried for foreign intelligence purposes with a selector for which NSA first determined there were facts giving rise to a reasonable, articulable suspicion (RAS) that the selector was associated with a foreign terrorist organization previously identified to the Court as the subject of a counter-terrorism investigation. Since February 2014, the operation of the program was further restricted such that absent an emergency, the Court must first approve any such selectors before the metadata may be queried.

Section 215 of the USA PATRIOT Act amended Section 1861 to expand the types of tangible things that the Government could collect under FISA. This expanded provision was scheduled to sunset on June 1, 2015. Pub. L. 109-177 § 102(b), 120 Stat. 192, 194-95, as amended by Pub. L. 112-14 § 2(a), 125 Stat. 216. Following the June 1,

2015, sunset of Section 215, on June 2, 2015, Congress passed the USA FREEDOM Act, and later that day the President signed it into law. The USA FREEDOM Act, among other things, extends the date for sunset of Section 215 to December 15, 2019, prohibits the bulk collection of tangible things under Section 1861, and provides a new mechanism under which the Government would not collect the call detail records in bulk. Pub. L. 114-23, 129 Stat. 268. Rather, the Government would seek the targeted production of certain call detail records from phone companies provided the Court first determine (except in emergencies), among other things, that there is RAS that a specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or agent of such a foreign power. Id. § 101. The prohibition on bulk production under Section 1861 and the new mechanism for the targeted production of call detail records "shall take effect on the date that is 180 days after the date of the enactment of [the USA FREEDOM Act]." Id. § 109. Until then, however, Section 109(b) of the USA FREEDOM Act expressly provides that "[n]othing in this Act shall be construed to alter or eliminate the authority of the Government to obtain an order under title V . . . as in effect prior to the effective date . . . during the period ending on such effective date." Id.

Thus, for a 180-day period beginning on June 2, 2015, the Government has specific statutory authorization to seek and obtain an order under Section 1861 as in effect prior to the effective date of the relevant amendments to that section. Id. § 109.

Because the USA FREEDOM Act extended the sunset date for Section 215 of the PATRIOT Act, as amended, to December 15, 2019, see id. § 705(a), the version of Section 1861 in effect now is, in pertinent part, the same version in effect at the time the Court approved the Government's application for the bulk production of call detail records in docket number BR 15-24 and prior related dockets.[2]

Congress, however, expressly delayed the restriction on the bulk production of tangible things under Section 1861 for 180 days to allow for the orderly termination of NSA's bulk production program and implementation of the technical capabilities required for targeted production under the new provisions of Sections 101 through 103 of the USA FREEDOM Act. Senator Leahy (one of the principal co-sponsors of the bill) specifically noted, among other things, that "I would also point out that when we drafted the USA FREEDOM Act, we included a provision to allow the government to collect call detail records, CDRs, for a 180-day transition period, as it was doing pursuant to Foreign Intelligence Surveillance Court orders prior to June 1, 2015. This provision was intended to provide as seamless a transition as possible to the new CDR

[2] Although the USA FREEDOM Act was not passed until June 2, Congress recognized that following passage of the bill Section 1861 would return to its pre-June 1 form. See, e.g., 161 CONG. REC. S3439 (daily ed. June 2, 2015) (statement of Sen. Lee, one of the bill's co-sponsors) ("Although we have gone past the June 1 sunset date by a few days, our intent in passing the USA FREEDOM Act is that the expired provisions be restored in their entirety just as they were on May 31, 2015, except to the extent that they have been amended by the USA FREEDOM Act. Specifically, it is both the intent and the effect of the USA FREEDOM Act that the now-expired provisions of the Foreign Intelligence Surveillance Act, FISA, will, upon enactment of the USA FREEDOM Act, read as those provisions read on May 31, 2015, except insofar as those provisions are modified by the USA FREEDOM Act, and that they will continue in that form until December 15, 2019. Extending the effect of those provisions for 4 years is the reason section 705 is part of the act.").

program under section 101 of the USA FREEDOM Act." See 161 CONG. REC. S3440 (daily ed. June 2, 2015) (emphasis added). The specific length of this transition period was also the subject of explicit debate. Before passage of the USA FREEDOM Act, the Senate expressly considered, and rejected, an amendment that would have provided for a twelve month transition period, rather than 180 days. The debate over that amendment further confirms Congress' intent, through Section 109, that the existing program should be allowed to continue until the new regime becomes effective after 180 days. See, e.g., 161 CONG. REC. S3428 (daily ed. June 2, 2015) (statement of Sen. John Cornyn) ("What the amendments that we will vote on this afternoon would do is to slow the transition from NSA storage to the telephone company stewardship from the 6 months prescribed in the underlying bill. For those who believe that the underlying bill is the correct policy, I do not know why they would object to a little bit of extra time so we can make sure that this is going to work as intended.").

This purpose is plain from the USA FREEDOM Act as a whole, and Section 109 in particular. The USA FREEDOM Act prohibits bulk collection under a number of authorities, see §§ 103 (tangible things), 201 (pen register and trap and trace), and 501 (national security letters). The prohibitions against bulk production under Titles II and V of the USA FREEDOM Act (FISA Pen Register and Trap and Trace Reform, and National Security Letter Reform, respectively) became effective immediately upon enactment. But the prohibition on bulk collection of call detail records under Section

1861 does not take effect for 180 days. Id. § 109. The extension of the sunset date of Section 215 coupled with the USA FREEDOM Act's provision for this orderly transition of the bulk metadata program would be meaningless if Congress did not also intend for the USA FREEDOM Act to authorize the existing program during the 180 day transition period. See Corley v. United States, 556 U.S. 303, 314 (2009) ("[O]ne of the most basic interpretive canons" is "that 'a statute should be construed so that effect is given to all its provisions so that no part will be inoperative or superfluous, void, or insignificant.'") quoting Hibbs v. Winn, 542 U.S. 88, 101 (2004)). See also INS v. Stanisic, 395 U.S. 62, 78 (1969) (rejecting an interpretation of a statutory provision that "would, as a practical matter, render [it] useless for the very function it was designed to perform").

Only one court, a Second Circuit panel in ACLU v. Clapper, 959 F.Supp. 2d 724 (S.D.N.Y. 2013), vacated and remanded, No. 14-42-CV, 2015 WL 2097814 (2d Cir. May 7, 2015), has concluded that the pre-USA FREEDOM Act version of Section 1861 did not authorize the bulk telephone metadata collection program. The court's statutory analysis, however, was conducted and issued before enactment of the USA FREEDOM

Act,[3] which as described above, provides specific statutory authorization for an orderly transition of the bulk production program for 180 days.[4]

In addition, as described in the Government's June 2, 2015 Memorandum of Law, this Court is not bound by the Second Circuit's decision, and this Court's analysis of the relevance standard under Section 1861 to permit bulk production reflects the better interpretation of the statute. See, e.g., In Re Application of the FBI for an Order Requiring the Production of Tangible Things, docket no. BR 13-109, Amended Mem. Op., 2013 WL 5741573 (FISA Ct. Aug. 29, 2013) (Eagan, J.); In Re Application of the FBI for an Order Requiring the Production of Tangible Things, docket no. BR 13-158, Mem. (FISA Ct. Oct. 11, 2013) (McLaughlin, J.); In Re Application of the FBI for an Order Requiring the Production of Tangible Things, docket no. BR 14-96, Mem. Op. (FISA Ct. June 19, 2014) (Zagel, J.). As this Court has recognized, relevance in the context of national security investigations must be considered in light of the special nature, purpose, and scope of such investigations. See In re Application of the FBI, 2013 WL 5741573, at *7 (holding that "the Section 215 provisions are designed to permit the

[3] On June 9, 2015, the Second Circuit issued an order directing the parties to that litigation to submit by July 24, 2015 supplemental briefs regarding the effect of the USA FREEDOM Act on the case and "in particular whether any or all of the claims asserted by the plaintiffs-appellants have been rendered moot as a result of that legislation." ACLU v. Clapper, No. 14-42-CV, Doc. No. 190, Order (2d Cir. June 9, 2015) The order also stayed issuance of the court's mandate pending the parties' supplemental briefing and extended the deadline for the submission of any petitions for rehearing.

[4] There are two cases involving Constitutional challenges to the legality of the bulk acquisition of non-content call detail records pending before federal appellate courts, Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013), argued No. 14-5004 (D.C. Cir. Nov. 4, 2014), and Smith v. Obama, 24 F.Supp.3d 1005 (D. Idaho 2014), argued No. 14–35555 (9th Cir. Dec. 8, 2014).

government wide latitude to meet its national security responsibilities"); cf. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946) ("relevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry"). The key purpose of counterterrorism investigations is to prevent terrorist attacks before they occur. National security investigations often have substantial breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, intended targets, and means of attack, many of which are often unknown to the intelligence community at the outset. See CIA v. Sims, 471 U.S. 159, 171 (1985) ("[F]oreign intelligence [gathering] consists of securing all possible data pertaining to ... the national defense and security of the United States.") (internal quotation omitted). National security investigations thus require means of information-gathering commensurate with the goal of shedding light on suspected terrorist organizations, their size and composition, recruitment, geographic reach, relation to foreign powers, financial resources, past acts, goals, and capacity for carrying out their plans.

In enacting Section 215, these unique aspects of counter-terrorism investigations were well understood by Congress. See H.R. Rep. No. 109-174(1) at 129 (statement of Rep. Lungren) ("This is in the nature of trying to stop terrorists before they act, not in the nature of a regular criminal investigation .... and it strikes ... precisely at when a 215 order is most useful."); see also 152 CONG. REC. S1325, 1330 (Feb. 15, 2006)

(statement of Sen. Feingold). The purpose underlying the USA PATRIOT Act, and Section 215 in particular, was to provide the intelligence community the enhanced investigatory tools needed to bring terrorist activities to light before they culminate in a loss of life and property. See H.R. Rep. No. 109-174(2) at 4 ("[M]any of the core enhanced authorities of the [Patriot Act] are fundamentally intelligence authorities intended to gather information to counter threats to national security from terrorists."); S. Rep. No. 109-85 at 40 (Additional and Minority Views) (noting "critical" nature and "broad reach" of authority conferred by Section 215). This Court has properly interpreted the language of Section 215 in accordance with these purposes.

Moreover, contrary to the Second Circuit's holding and the arguments of Movants, the Government's position does not "read the 'authorized investigation' language out of the statute." Movt's Mot. at 7-8. Rather, as this Court is well aware, the Government seeks Orders from this Court by submitting detailed applications explaining that the records are sought for specified investigations to protect against international terrorism that concern specified foreign terrorist organizations identified in the application. Therefore this Court's authorization of the Section 1861 orders in support of such investigations has been and remains consistent with the terms of the statute.

In sum, as described above, the USA FREEDOM Act makes clear Congress' intent to allow the Government to continue, with this Court's approval, the bulk

collection of call detail records for a 180-day period while the Government transitions to a new system that will provide similar counterterrorism capabilities, and, in any event, this Court, and not the Second Circuit, which did not have the benefit of the USA FREEDOM Act when it conducted its statutory analysis, has interpreted Section 1861 correctly.

II. Bulk Production of Call Detail Records Under Section 1861 is Consistent with the Fourth Amendment to the Constitution.

The Supreme Court has rejected the premise of Movants' Fourth Amendment argument, holding that there is no reasonable expectation of privacy in the telephone numbers a person dials in order to place a telephone call. In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court held that the government's recording of the numbers dialed from an individual's home telephone, through the installation of a pen register at a telephone company, is not a search under the Fourth Amendment. Id. at 743-44. With the exception of the district court in Klayman v. Obama, supra, every federal court to have adjudicated Fourth Amendment issues regarding the bulk call detail record program has found Smith v. Maryland to be controlling precedent, and relying on Smith, has held that the acquisition from telecommunications companies of their own business records consisting of bulk telephony metadata is not a Fourth Amendment "search."[5] See In Re Application of the FBI, 2013 WL 5741573 at *3 ("In

[5] Because it concluded that the bulk call detail record program was not authorized by statute, the Second Circuit's recent panel opinion in ACLU v. Clapper did not adjudicate constitutional issues.

sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, Smith v. Maryland compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in [REDACTED] and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise."); In Re Application of the FBI, docket no. BR 13-158, Mem. at 4 (under Smith v. Maryland the production of call detail records to the National Security Agency does not constitute a search under the Fourth Amendment, and the Supreme Court's decision in United States v. Jones does not compel a different conclusion); In Re Application of the FBI for an Order Requiring the Production of Tangible Things, docket no. BR 14-01, Op. and Order, 2014 WL 5463097 at *4-6 (FISA Ct. Mar. 20, 2014) (Collyer, J.) (Smith v. Maryland remains controlling precedent notwithstanding the district court's opinion in Klayman); ACLU v. Clapper, 959 F.Supp.2d at 749-52; U.S. v. Moalin, No. 10cr4246 JM, 2013 WL 6079518 at *7-*8 (S.D. Cal. Nov. 18, 2013); and Smith v. Obama, 24 F.Supp.3d at 1009 ("Because Jones does not apply, the weight of the authority favors the NSA. The Supreme Court's decision in Smith, supplemented by the [9th] Circuit's decisions in [U.S. v. Reed, 575 F.3d 900, 914 (9th Cir. 2009), U.S. v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008), and U.S. v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012)], and the two District Court decisions on point, Clapper

and Moalin, support a finding that there is no Fourth Amendment violation here."). As Smith and numerous cases that followed have consistently held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." 442 U.S. at 743-44.

Movants argue that they have a reasonable expectation of privacy in call detail records based, in particular, on statutes enacted since Smith v. Maryland and contracts or policies adopted by telecommunications companies. None of these arguments has merit. As described more fully in the attached reply brief in support of the Government's motion to dismiss plaintiffs' claims in Paul v. Obama, No. 1:14-cv-262-RJL (D.D.C) – a matter in which Movant Cuccinelli is lead counsel for plaintiffs – any rights conferred by statute do not create a reasonable expectation of privacy for purposes of the Fourth Amendment, and in any event, the statutes cited by Movants contain exceptions indicating that records may be disclosed to the Government as required by law. Reply Brief, Exh. A hereto, at 10-11.[6] The corporate policies to which Movants refer also do not create privacy rights or possessory interests for subscribers in

[6] As noted above, this Court already has adjudicated relevant Fourth Amendment issues regarding the bulk call detail record program and found Smith v. Maryland to be controlling precedent. In addition, Movants' arguments before this Court are substantively identical to those made by plaintiffs before the U.S. District Court for the District of Columbia in response to the Government's motion to dismiss in Paul v. Obama. Because the Government's responses to Movants' Constitutional arguments were previously briefed in connection with that motion to dismiss, and the Government's position has not changed since that filing, the Government respectfully attaches and incorporates by reference its reply in support of its motion to dismiss the Paul case; specifically; its arguments concerning the merits of the Fourth Amendment claim on pages 6 through 25 of the reply. The government further notes that on September 22, 2014, the district court, by minute order, granted a Government motion for stay of all proceedings in Paul v. Obama, 1:14-cv-262-RJL pending resolution of the appeal in Klayman v. Obama.

the companies' business records as a factual matter – on the contrary, they advise customers that their records may be shared with the Government as required by law. Id. at 12-14. In any event, such policies are irrelevant as a legal matter because subscribers assume the risk that the companies will disclose the records to the Government. Id. at 15-16.

Finally, even if obtaining bulk call detail records from telecommunications companies were a Fourth Amendment search, as explained in the Government's reply brief in the Paul case, it would be constitutionally permissible under the Supreme Court's special needs doctrine. The balance of the Government's counter-terrorism interests furthered by the telephony metadata program, and the privacy interests at stake, decisively favors the program's constitutionality, because even if the Supreme Court were to reconsider the holding of Smith, at minimum any privacy interest in records created by third parties would be minimal; any privacy interest would be mitigated by the substantial restrictions on review and dissemination of metadata that are core features of the program; the governmental interest in identifying and tracking terrorist operatives to prevent terrorist attacks is overwhelmingly important; and the telephony metadata program is an effective way of advancing that interest.[7]

[7] Movants have requested oral argument. Movt's Mot. at 6. Given the unresolved issues regarding Movants' standing in this matter, the fact that the statutory and relevant Fourth Amendment issues have been fully briefed (and in some respect previously considered and adjudicated by this Court, as well as other federal courts), and the national security equity in ensuring expeditious consideration of the Government's application to re-initiate the telephony metadata program (see 50 U.S.C. § 1803(c)), the Government submits that oral argument at this time is neither necessary nor appropriate.

III. Conclusion

For the foregoing reasons, the Government respectfully submits that Section 1861 of FISA, as amended by the USA PATRIOT Act and the USA FREEDOM Act, authorizes the Court to approve the Government's application for the bulk production of non-content call detail records for a 180-day transition period, subject to the restrictions and limitations regarding the handling of such data as set forth in this Court's prior Orders, and that the production of such records pursuant to Section 1861 is consistent with the Fourth Amendment to the Constitution.

Respectfully submitted,

John P. Carlin
Assistant Attorney General

6/12/15
Date

By: Stuart J. Evans

Stuart J. Evans
Deputy Assistant Attorney General

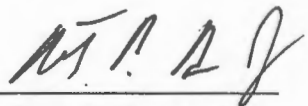
Robert P. Boyer, Jr.
Deputy Section Chief, Operations
Matthew A. Anzaldi
Deputy Unit Chief, Operations
Michelle Bazu
Attorney
Michael P. Daly
Attorney
Office of Intelligence

National Security Division
U.S. Department of Justice

CERTIFICATE OF SERVICE

I hereby certify that, on June 12, 2015, a true and correct copy of the Response to Motion in Opposition to Government's Request to Resume Bulk Data Collection Under Patriot Act § 215, filed by the United States of America on June 12, 2015, was submitted, by hand delivery, to a Litigation Security Officer, for delivery to the following counsel of record for Movants:

KENNETH T. "KEN" CUCCINELLI, II
KCuccinelli@CuccinelliAndAssociates.com
Cuccinelli & Associates, PLLC
13881 Jordan Meadows Lane
Nokesville, VA 20181
Ph: (804) 286-2550
No fax number
Counsel for Movants



Robert P. Boyer, Jr.
Deputy Section Chief, Operations
Office of Intelligence
National Security Division
U.S. Department of Justice

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

RAND PAUL, *et al.*, Plaintiffs, v. BARACK OBAMA, President of the United States, Defendants.	No. 1:14-cv-262-RJL

DEFENDANTS' REPLY BRIEF IN SUPPORT OF MOTION TO DISMISS

Dated: June 5, 2014

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
JULIA A. BERMAN
Trial Attorney

United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Counsel for Defendants

TABLE OF CONTENTS

PAGE

INTRODUCTION 1

ARGUMENT 1

I. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING BECAUSE THEY HAVE NOT SET FORTH FACTS DEMONSTRATING THAT RECORDS OF THEIR TELEPHONE CALLS HAVE BEEN COLLECTED, OR REVIEWED, BY GOVERNMENT ANALYSTS 1

II. PLAINTIFFS' FOURTH AMENDMENT CLAIM SHOULD BE DISMISSED 6

A. *Smith* and the Third-Party Doctrine Are Applicable, and Require That This Case Be Dismissed 6

B. Plaintiffs Have No Reasonable Expectation of Privacy in Telephony Metadata 9

1. The statutes cited by Plaintiffs do not create Fourth Amendment expectations of privacy 10

2. Privacy policies unilaterally adopted by telecommunications service providers do not alter the analysis under *Smith* 12

3. Characterizations of telephony metadata as "highly personalized" are irrelevant, as they were in *Smith* 16

4. *Smith* and the third-party doctrine control here, not Plaintiffs' views about societal expectations of privacy in 1792 18

C. Even if Plaintiffs Had a Legitimate Expectation of Privacy in Telephony Metadata, They Have Not Alleged an Unreasonable Search of Information About Their Telephone Calls 21

1. Plaintiffs have not alleged an invasion of any privacy interest they may have in metadata pertaining to their calls 21

2. Even assuming a search of metadata pertaining to Plaintiffs' calls occurs, it would be reasonable under the "special needs" doctrine 21

CONCLUSION 25

TABLE OF AUTHORITIES

CASES **PAGE(S)**

ACLU v. Clapper,
959 F. Supp. 2d 724 (S.D.N.Y. 2013).....24

Afshar v. Dep't of State,
702 F.2d 1125 (D.C. Cir. 1983).....3

Ala. Power Co. v. FPC,
511 F.2d 383 (D.C. Cir. 1974).....4

Alderman v. United States,
394 U.S. 165 (1969).....19

Anderson v. Hannaford Bros. Co.,
659 F.3d 151 (1st Cir. 2011).....8

In re Application of U.S. for Order Authorizing Disclosure of Location Info. of Specified Wireless Telephone, 849 F. Supp. 2d 526 (D. Md. 2011).....9

In re Application of U.S. for Order Directing Provider of Elec. Commc'n Servs. to Disclose Records, 620 F.3d 304 (3d Cir. 2010).....9

Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls,
536 U.S. 822 (2002).....24

Bissonette v. Haig,
800 F.2d 812 (8th Cir. 1986).....11, 12

Bond v. United States,
529 U.S. 334 (2000).....8

Brown v. FBI,
792 F. Supp. 2d 368 (D.D.C. 2011).....2

California v. Ciraolo,
476 U.S. 203 (1986).....19

Chandler v. Miller,
520 U.S. 305 (1997).....23

City of Indianapolis v. Edmond,
531 U.S. 32 (2000).....22

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013) 2, 3, 4

Claridge v. RockYou, Inc.,
785 F. Supp. 2d 855 (N.D. Cal. 2011) 8

Cmte. for GI Rights v. Callaway,
518 F.2d 466 (D.C. Cir. 1975) 4

Cronin v. FAA,
73 F.3d 1126 (D.C. Cir. 1996) 4

Ctr. for Law & Educ. v. Dep't of Educ.,
396 F.3d 1152 (D.C. Cir. 2005) 4

Douglas v. Dobbs,
419 F.3d 1097 (10th Cir. 2005) 8

El-Masri v. Tenet,
479 F.3d 296 (4th Cir. 2007) 3

Elec. Privacy Info. Center v. DHS,
653 F.3d 1 (D.C. Cir. 2011) 22

Ferguson v. City of Charleston,
308 F.3d 380 (4th Cir. 2002) 7

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 7

Flores v. Dist. of Columbia,
437 F. Supp. 2d 22 (D.D.C. 2006) 2

Frugone v. CIA,
169 F.3d 772 (D.C. Cir. 1999) 3

Georgia v. Randolph,
547 U.S. 103 (2006) 16

Goldman v. United States,
316 U.S. 129 (1942) 18

Griswold v. Connecticut,
381 U.S. 479 (1965) 8

Harpole v. Architects, P.C. v. Barlow,
668 F. Supp. 2d 68 (D.D.C. 2009) 2

ICG Communications, Inc. v. Allegiance Telecom,
211 F.R.D. 610 (N.D. Cal. 2002) 11

Ex Parte Jackson,
96 U.S. 727 (1878) 20

Jones v. United States,
362 U.S. 257 (1960) 16

Katz v. United States,
389 U.S. 347 (1967) 15, 19

Kerns v. Bader,
663 F.3d 1173 (10th Cir. 2011) 8

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013) 14

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 5

Kyllo v. United States,
533 U.S. 27 (2001) 5, 18

MacWade v. Kelly,
460 F.3d 260 (2d Cir. 2006) 22, 23

In re Michaels Stores PIN Pad Litig.,
830 F. Supp. 2d 518 (N.D. Ill. 2011) 8

Michigan Dep't of State Police v. Sitz,
496 U.S. 444 (1990) 24

NRDC v. EPA,
464 F.3d 1 (D.C. Cir. 2006) 4

O'Connor v. Ortega,
480 U.S. 709 (1987) 8

On Lee v. United States,
343 U.S. 747 (1952) 20

Payton v. New York,
445 U.S. 573 (1980) 16

Pisciotta v. Old Nat'l Bancorp,
499 F.3d 629 (7th Cir. 2007) 5

Pub. Citizen, Inc. v. NHTSA,
489 F.3d 1279 (D.C. Cir. 2007) 4

Rakas v. Illinois,
439 U.S. 128 (1978) 16

Reporters Cmte. for Freedom of the Press v. AT&T,
593 F.2d 1030 (D.C. Cir. 1978) 20

Silverman v. United States,
365 U.S. 505 (1961) 18, 19

In re Smartphone Geolocation Data Application,
2013 WL 5583711 (E.D.N.Y. May 1, 2013) 13

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

Smith v. Obama,
No. 13-cv-257-BLW 6, 20

Steagald v. United States,
451 U.S. 204 (1981) 5

Stoner v. California,
376 U.S. 483 (1964) 8

Tenet v. Doe,
544 U.S. 1 (2005) 3

Tunica-Biloxi Tribe of La. v. United States,
577 F. Supp. 2d 382 (D.D.C. 2008) 2

United States v. Choate,
576 F.2d 165 (9th Cir. 1978) 20

United States v. De Poli,
628 F.2d 779 (2d Cir. 1980) 20

United States v. Hartwell,
436 F.3d 174 (3d Cir. 2006).....22

United States v. Hinton,
222 F.3d 664 (9th Cir. 2000).....20

United States v. Jacobsen,
466 U.S. 109 (1984).....21, 22

United States v. Jones,
132 S. Ct. 945 (2012).....11, 17, 18

United States v Karo,
468 U.S. 705 (1984).....18

United States v. Kington,
801 F.2d 733 (5th Cir. 1986).....10

United States v. Knotts,
460 U.S. 276 (1983).....19

United States v. Mann,
829 F.2d 849 (9th Cir. 1987).....10

United States v. Martinez-Fuerte,
428 U.S. 543 (1976).....24

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010).....*passim*

United States v. Miller,
425 U.S. 435 (1976).....*passim*

United States v. Osunegbu,
822 F.2d 472 (5th Cir. 1987).....20

United States v. Payner,
447 U.S. 727 (1980).....10

United States v. Place,
462 U.S. 696 (1983).....5, 21

United States v. White,
401 U.S. 745 (1971).....19, 20

United States v. Ziegler,
456 F.3d 1138 (9th Cir. 2006) 11, 15

United States v. Ziegler,
474 F.3d 1184 (9th Cir. 2007) 15

Vernonia Sch. Dist. 47J v. Acton,
515 U.S. 646 (1995) 24

STATUTES

18 U.S.C. § 1039(b)(1), (c)(1), (g) 11

18 U.S.C. § 2703(c)(1)(B) 11

50 U.S.C. § 1861 11

Right to Financial Privacy Act,
12 U.S.C. § 3401 *et seq* 10

Telecommunications Act of 1996,
47 USC § 222 ..... 11, 14

MISCELLANEOUS

In re Application of the FBI for an Order Requiring the Prod. of Tangible Things,
BR 09-09, Aug. 17, 2009 25

In re Application of the FBI for an Order Requiring the Production of Tangible Things,
Dkt. No., BR 13-158 (FISC Oct. 11, 2013) 12

INTRODUCTION

Plaintiffs' arguments in opposition to Defendants' motion to dismiss, while plentiful, are lacking in merit and fail to establish that the complaint adequately pleads standing or a claim on which relief can be granted. Regarding standing, Plaintiffs fail to rebut the Government's evidence that the bulk telephony metadata program does not capture information on all (or virtually all) telephone calls made and/or received in the United States, nor have they adequately alleged or offered evidence of other facts demonstrating that records about their calls have ever been or are imminently likely to be collected, let alone reviewed by Government analysts.

On the merits, this case is controlled by *Smith v. Maryland*, 442 U.S. 735 (1979), as the District of Idaho just held in dismissing a claim identical to Plaintiffs'. *Smith* holds that there is no reasonable expectation of privacy in telephone numbers dialed because the caller voluntarily turns this information over to the phone company. Plaintiffs' multiple attempts to escape the force of that holding all fail. Nothing that Plaintiffs point to—not the statutes, corporate privacy policies, the metadata's theoretical potential to reveal personal information, or supposed expectations of privacy in 1792—provides a sound reason to deviate from *Smith*, or the third-party doctrine. Plaintiffs' arguments against the reasonableness of the program under the special needs doctrine are also unpersuasive. Accordingly, the complaint should be dismissed.

ARGUMENT

I. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING BECAUSE THEY HAVE NOT SET FORTH FACTS DEMONSTRATING THAT RECORDS OF THEIR TELEPHONE CALLS HAVE BEEN COLLECTED, OR REVIEWED, BY GOVERNMENT ANALYSTS.

Plaintiffs' contention that they have standing because records pertaining to their telephone calls have been collected under the NSA's bulk telephony metadata program is premised on their supposition that "all major telecommunications companies operating in the United States provide [the] NSA … telephone metadata for all telephone calls on their networks

in, to or from the United States ...." *See* First Am. Compl., ¶¶ 4, 5, 16. Defendants have now shown, through the introduction of competent evidence, that this assumption is incorrect: the telephony metadata program has never captured information on all (or virtually all) telephone calls made and/or received in the United States. *See* Defs.' Mem. (ECF No. 22-1) at 16-17, 20-21, citing, *inter alia*, *Paul* Shea Decl. ¶ 8 (ECF No. 22-3). In the face of Defendants' factual challenge to Plaintiffs' allegations of standing, their allegations were no longer entitled to an assumption of truth, and it became Plaintiffs' burden, as the parties invoking the Court's subject matter jurisdiction under Article III, to establish the factual predicate of their standing by additional well-pleaded allegations or evidence demonstrating that records of their communications have been collected. *Harpole Architects, P.C. v. Barlow*, 668 F. Supp. 2d 68, 78 (D.D.C. 2009); *Tunica-Biloxi Tribe of La. v. United States*, 577 F. Supp. 2d 382, 398 (D.D.C. 2008); *Flores v. Dist. of Columbia*, 437 F. Supp. 2d 22, 29 (D.D.C. 2006); *see Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1149 (2013). Plaintiffs have not carried their burden.

Plaintiffs argue in opposition that "the public record establishes that, in fact, both Verizon and AT&T"—Plaintiffs' telecommunications service providers—"*admit* they are participants" in the bulk telephony metadata program. Pls' Opp. (ECF No. 27) at 4. The public documents Plaintiffs cite for this proposition, however, do not come close to supporting it. Plaintiffs rely on recent "transparency reports" posted online by Verizon and AT&T to provide their customers information about the number of national security letters (NSLs) and FISC orders they received in 2013 for "content" and "non-content" information regarding subscribers' communications. Verizon Transparency Report (Exh. 1, hereto); AT&T Transparency Report (Exh. 2, hereto).[1] *See also* Letter from James M. Cole to Colin Stretch, *et al.* (Jan. 27, 2014) (Exh. 3, hereto). The

[1] Respectively *available at* http://transparency.verizon.com/us-data/national-security (last visited May 27, 2014); http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited May 27, 2014).

Verizon report states that the figures contained therein do not reflect "other matters, such as any orders [Verizon companies] may have received related to the bulk collection of non-content information," on which reporting "remains prohibited." Exh. 1 at 1. Plaintiffs would have the Court construe this statement as an admission that "Verizon" is a participant in the telephony metadata program, reasoning that otherwise the disclaimer would be unnecessary. Pls.' Opp. at 4. But the report cannot shoulder the evidentiary weight that Plaintiffs seek to lay on it.

First, Plaintiffs cite no similar statement in the AT&T report, and it contains none. Pls.' Opp. at 4; *see generally* Exh. 2. Second, the disclaimer in the Verizon Transparency Report does not mean what Plaintiffs claim it means. It merely advises the reader that the reported numbers of NSLs, FISC orders, and affected customer accounts should not be understood to reflect bulk production of communications metadata (or "other matters")—a noteworthy clarification whether or not any Verizon company is required by FISC orders to produce such information. Moreover, even if the disclaimer were also susceptible of the interpretation Plaintiffs suggest, it is the United States that controls the disclosure of national security information, and an ambiguous statement from an unofficial source cannot be taken as official confirmation by the United States that any provider is now or ever has been a participant in the NSA's bulk telephony metadata program. *See, e.g., Frugone v. CIA* , 169 F.3d 772, 774 (D.C. Cir. 1999); *Afshar v. Dep't of State*, 702 F.2d 1125, 1134 (D.C. Cir. 1983); *see also Tenet v. Doe,* 544 U.S. 1, 9 -10 (2005); *El-Masri v. Tenet,* 479 F.3d 296, 308-09 (4th Cir. 2007). At bottom, Plaintiffs' attempt to coax tenuous inferences from a single equivocal remark in a Verizon transparency report cannot substitute for well-pleaded allegations or evidence of the specific facts necessary to establish their standing. *Amnesty Int'l*, 133 S. Ct. at 1149; *see also* Defs.' Mem. at 21-22.

In recognition, perhaps, that they cannot carry their burden, Plaintiffs attempt to shirk it, arguing that they "need only show the[ir] [alleged] injury is probable." Pls.' Opp. at 5, citing

NRDC v. EPA, 464 F.3d 1 (D.C. Cir. 2006).[2] However, to ensure fidelity to Article III's requirement of actual or imminent injury, the Court of Appeals has applied the "substantial probability" standard that Plaintiffs seek to invoke only to claims of increased health or environmental risk, injuries that "often are purely probabilistic." *Id.* at 5-6. *See Pub. Citizen, Inc. v. NHTSA*, 489 F.3d 1279, 1294-96 (D.C. Cir. 2007); *Ctr. for Law & Educ. v. Dep't of Educ.*, 396 F.3d 1152, 1161 (D.C. Cir. 2005) ("[o]utside of increased exposure to environmental [or health] harms, hypothesized 'increased risk' has never been deemed sufficient 'injury'"). Moreover, Plaintiffs are not claiming increased risk of harm, but actual injury because records containing information about their calls allegedly have been and continue to be collected under a Government foreign intelligence program. In this context, their burden is to plausibly allege or adduce evidence of specific facts demonstrating that to be true.[3]

---

[2] For the same evident purpose, Plaintiffs accuse Defendants of "duplicity," "hypocrisy," and "semantic evasions" for questioning their standing. Pls.' Opp. at 3. Unfortunately, these aspersions typify several of Plaintiffs' arguments—long on *ad hominem* attacks but short on merit. *See also id.* at 6 n.3, 41 (accusing the Government of "material misrepresentations," a "pattern of dishonesty," and "lie[s]" to the courts and Congress). What Plaintiffs appear to misunderstand is that it is "not the Government's burden to disprove [their] standing by revealing details" of its intelligence activities, *Amnesty Int'l*, 133 S. Ct. at 1149 n.4, but rather their burden to allege or adduce proof of sufficient facts demonstrating that information about their telephone calls has been collected under the challenged program. Plaintiffs cite *Alabama Power Co. v. FPC*, 511 F.2d 383, 391 n.4 (D.C. Cir. 1974), for the proposition that "[a] party having control of information bearing upon a disputed issue may be given the burden of bringing it forward and suffering an adverse inference from failure to do so." Pls.' Opp. at 3. But *Amnesty International* makes clear that this principle has no application in circumstances where a party bearing the burden of proof on an issue seeks to cast on the Government the burden of disproving that party's allegations by revealing classified information.

[3] Plaintiffs' reliance on *Cronin v. FAA*, 73 F.3d 1126 (D.C. Cir. 1996), and *Committee. for GI Rights v. Callaway*, 518 F.2d 466 (D.C. Cir. 1975), *see* Pls.' Opp. at 5, is also badly misplaced. Both *Cronin* and *GI Committee* held that parties seeking to contest the legality of Government alcohol- and drug-testing regulations had standing to bring suit because in each case the plaintiffs (or the persons they represented) were members of a class that was subject to the regulations on their face. *See Cronin*, 73 F.3d at 1130; *GI Cmte.*, 518 F.2d at 471-72. Here, the scope of the Government intelligence program at issue remains classified, and Plaintiffs have adduced no evidence that they are members of any identifiable class within its reach.

Even if Plaintiffs had demonstrated that metadata pertaining to their communications have been collected, it would still remain the case that their allegations of injury are too speculative to support their standing, because they have neither alleged nor offered evidence that records containing information about their calls have ever been or are imminently likely to be reviewed by Government analysts. *See* Defs.' Mem. at 18-20. Plaintiffs insist that records of their calls are "searched" each time the metadata are queried using a suspected-terrorist selector, likening the process to inspection of a person's luggage. That person, they observe, has been subjected to a search "even if the inspection turns up no contraband. " Pls.' Opp. at 5-6 & n.5. The analogy does not hold, however, because queries to which no records of Plaintiffs' calls are responsive do not expose their contents to inspection by NSA analysts, or anyone else, as does "an officer's rummaging through the contents" of a person's luggage. *United States v. Place*, 462 U.S. 696, 707 (1983). Rather, such queries are more analogous to a canine sniff of luggage for concealed narcotics, which "does not expose noncontraband items" to public view, and for which reason does not constitute a Fourth Amendment search. *See id.* Plaintiffs' attempt to equate queries of the metadata to thermal-imaging of a house, as in *Kyllo v. United States*, 533 U.S. 27 (2001), also fails. Pls.' Opp. at 6 n.5. *Kyllo* held that thermal imaging constitutes a search because it reveals information regarding the interior of the home, 533 U.S. at 34-35 n.2, where the Fourth Amendment "draw[s] a firm line." *Steagald v. United* States, 451 U.S. 204, 212 (1981). Here, absent queries to which records of Plaintiffs' telephone calls are responsive, the Government learns no information about Plaintiffs' contacts.[4]

[4] Plaintiffs argue further that even if records of their calls are never reviewed, the alleged collection of the records alone constitutes an injury sufficient for purposes of Article III. Pls.' Opp. at 5. Here, as above, they cite cases that do not stand for the proposition asserted. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141-43 (9th Cir. 2010), and *Pisciotta v. Old National Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007), held that the plaintiffs in those cases had standing to sue over the mass theft of digital records containing highly personal information (including their names, addresses, and social security numbers) that exposed them to credible

For the reasons above, and those set forth in Defendants' opening brief, Plaintiffs have not established their standing as required by Article III, and this case must therefore be dismissed for lack of subject-matter jurisdiction.

II. PLAINTIFFS' FOURTH AMENDMENT CLAIM SHOULD BE DISMISSED.

Plaintiffs effectively acknowledge, as they must, that *Smith* remains the law and could only be overruled by the Supreme Court itself. Pls.' Opp. at 30-31 & n.38. As the District of Idaho just held in dismissing an identical Fourth Amendment challenge to the NSA's bulk telephony metadata program, *Smith* is binding and requires dismissal of claims such as Plaintiffs' here. *Smith v. Obama*, No. 13-cv-257-BLW, Mem. Decision, 8 (D. Idaho June 3, 2014) (Exh. 4, hereto). Plaintiffs devote their opposition to a series of attempts to avoid that straightforward conclusion, but each effort fails.

A. *Smith* and the Third-Party Doctrine Are Applicable, and Require That This Case Be Dismissed.

As set forth in Defendants' opening brief, *Smith* controls this case because the pen-register metadata at issue in *Smith* are indistinguishable from the telephony metadata acquired here, and because *Smith*'s rationale—that there is no reasonable expectation of privacy in information voluntarily turned over to a third party—is squarely applicable. In their motion to dismiss, Defendants addressed the various factual differences between the Section 215 program and *Smith* alleged by Plaintiffs in their First Amended Complaint, and explained why none of those differences are material to the reasoning of *Smith*. Defs.' Mem. at 28-35. In response, Plaintiffs merely reiterate those factual differences, practically verbatim from the complaint, without responding to Defendants' arguments. Pls.' Opp. at 23-25, 35. For instance, Plaintiffs provide no response to the points that the records produced to the Government under the

---

threats of identity theft and other forms of economic injury. Plaintiffs here do not allege any plausible threat that records of their calls will be accessed by Government analysts for purposes of inflicting any comparable injury upon them.

program are generated and maintained by the telecommunications companies for their own pre-existing business purposes, rather than being collected by the companies for the Government's law enforcement purposes, Defs.' Mem. at 30; that the large volume of metadata collected is irrelevant to the Fourth Amendment analysis under settled law, *id.* at 31-32; and that the additional functions performed by cell phones are also constitutionally irrelevant because those functions do not generate any information that is obtained by the NSA under the telephony metadata program, *id.* at 30-31.

Plaintiffs instead seek to chip away at the third-party doctrine, arguing that it is not absolute, *id.* at 25-28, but the support tendered for the argument is not persuasive. In *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), relied upon by Plaintiffs, the Supreme Court held that a state hospital's program of testing patients' urine to gather evidence of drug use for law enforcement purposes—which the state conceded constituted a search—did not fit within the Court's "special needs" doctrine and was unreasonable. There was no voluntary disclosure of information involved, because the case was presented and decided on the assumption that the patients did *not* voluntarily turn over their urine to the state hospital (and was thereafter remanded for a decision on the consent issue). *Id.* at 76 (assuming for purposes of decision "that the searches were conducted without the informed consent of the patients."). Moreover, the case did not involve disclosure of information by the patients *to a third party*, because, as the Supreme Court noted, the hospital was a state institution whose staff was acting in collaboration with local law enforcement authorities. *Id.* at 76, 78 n.13, 85.[5]

[5] This point was underscored on remand, where the Fourth Circuit applied a heightened "informed consent" standard requiring that patients know their urine samples would be used for law enforcement purposes, because the hospital was actually collecting the samples as agents of local law enforcement authorities. *Ferguson v. City of Charleston*, 308 F.3d 380, 397 (4th Cir. 2002). As the Government noted in its opening brief, there is no evidence of a similar circumstance here—*i.e.*, that the telecommunications companies that receive Section 215 FISC orders are collecting telephony metadata for law enforcement purposes. Defs.' Mem. at 30.

Nor do the other cases Plaintiffs cite, Pls' Opp. at 26, hold that a person has a legitimate expectation of privacy "in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44. Merely giving permission to enter one's hotel room, *Stoner v. California*, 376 U.S. 483, 489 (1964), or office, *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987), does not amount to voluntarily turning information over to third parties. A telephone caller fully divulges the numbers he dials to the phone company, unlike the employee in *O'Connor* who did not share his desk or file cabinets with any other employee and therefore had a reasonable expectation of privacy in them, *id.* at 718, or the bus passenger in *Bond v. United States*, 529 U.S. 334, 338 (2000), who sought to preserve the privacy of the contents of his carry-on bag by using an opaque bag and placing it directly above his seat, and therefore had a reasonable expectation of privacy in it. *See* Mar. 20, 2014 FISC Order at 16 n.8. *Douglas v. Dobbs*, 419 F.3d 1097 (10th Cir. 2005), also cited by Plaintiffs, found that individuals have a privacy interest in prescription drug records held by a pharmacy. But that was so, the court held, because the contents of medical records are otherwise constitutionally protected under the right to privacy, flowing from *Griswold v. Connecticut*, 381 U.S. 479 (1965), that the Court has recognized in certain personal information, including matters of health. *Douglas*, 419 F.3d at 1101-02. The Tenth Circuit has since noted that *Douglas* did not require a warrant for law enforcement to obtain medical records held by a third party, and noted the tension between *Douglas* and the Supreme Court's third-party doctrine. *Kerns v. Bader*, 663 F.3d 1173, 1184 (10th Cir. 2011).[6]

[6] Plaintiffs also cite cases involving state-law claims for breach of implied contract against private companies for failing to safeguard personal data. Pls.' Opp. at 27 (citing *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011); *In re Michaels Stores PIN Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011)). Plaintiffs cite no authority for the proposition that the existence of these state-law claims determines what society accepts as a reasonable expectation of privacy for Fourth Amendment purposes. As Plaintiffs themselves put it, these cases do not "hinge on Fourth Amendment issues," *id.*, and certainly do not support the notion that the Supreme Court has retreated from the third-party doctrine.

Lastly, Plaintiffs point to cases involving the Government's obtaining cell-site location information (CSLI) as undermining the third-party doctrine. CSLI is not collected under the Section 215 telephony metadata program, Defs.' Mem. at 7, and contrary to Plaintiffs' purpose in citing these cases, they actually solidify *Smith*'s applicability to the program Plaintiffs challenge. In *In re Application of U.S. for Order Directing Provider of Electronic Communication Services to Disclose Records*, 620 F.3d 304, (3d Cir. 2010), the court distinguished *Smith* as follows: "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, *when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed* and there is no indication to the user that making that call will also locate the caller . . . ." *Id.* at 317 (emphasis added and alterations omitted). *See also In re Application of U.S. for Order Authorizing Disclosure of Location Info. of Specified Wireless Tel.*, 849 F. Supp. 2d 526, 538 n.6 (D. Md. 2011) (similarly distinguishing Smith). Whatever the merits of the court's analysis regarding whether cell-site location information is voluntarily turned over to third parties, it is clear that the Section 215 telephony metadata program, which collects phone numbers dialed and other non-CSLI, non-content telephony metadata, is controlled by *Smith*, not the CSLI cases cited by Plaintiffs.

B. Plaintiffs Have No Reasonable Expectation of Privacy in Telephony Metadata.

Plaintiffs next raise a number of arguments to the effect that they have a legitimate expectation of privacy in telephony metadata, notwithstanding *Smith* and the third-party doctrine. None of these arguments has merit.

1. The statutes cited by Plaintiffs do not create Fourth Amendment expectations of privacy.

Plaintiffs first argue that statutes restricting telecommunications carriers from disclosing records related to their customer's calls create a reasonable expectation of privacy in those records that did not exist at the time of *Smith*. Pls.' Opp. at 10-13. It is worth noting, as an initial matter, that Plaintiffs are not suing telecommunications carriers under any of the statutes that they invoke in this argument; their claim is instead a constitutional one, under the Fourth Amendment, against the Government.[7] Plaintiffs provide no authority for the proposition that rights conferred by statute determine whether a subjective expectation of privacy is reasonable for purposes of the Fourth Amendment. The law is in fact to the contrary.

After the Supreme Court held in *United States v. Miller*, 425 U.S. 435 (1976), that bank customers have no legitimate Fourth Amendment expectation of privacy in the records of their accounts maintained by banks, Congress passed the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq.*, to provide a statutory right to privacy in bank records. But this "expansion" of individuals' right to privacy in bank records was held not to be "of constitutional dimensions. The rights created by Congress are statutory, not constitutional." *United States v. Kington*, 801 F.2d 733, 737 (5th Cir. 1986). Courts have also rejected the argument that foreign statutes protecting bank records from disclosure created a protectable Fourth Amendment privacy interest notwithstanding *Miller*. The foreign statutes were "hedged with exceptions," *United States v. Payner*, 447 U.S. 727, 732 n.4 (1980), preventing a reasonable expectation of privacy in the bank records because "the customer knows that his records may be revealed in a variety of situations." *United States v. Mann,* 829 F.2d 849, 852 (9th Cir. 1987).

[7] Similarly, Plaintiffs are not suing under any state constitutional provisions of the sort they refer to in footnote 39 of their brief. Pls.' Opp. at 31 n.39.

In the same vein, subscribers to telecommunications services know that records related to their calls may be disclosed under various exceptions to the privacy statutes on which Plaintiffs rely. Those statutes contain a host of exceptions, including that the records may be disclosed to the Government "as required by law," or upon "court order" (not specifying based on probable cause or individualized suspicion). *See* 18 U.S.C. § 2703(c)(1)(B) (Stored Communications Act); 47 U.S.C. § 222(c)(1), (d), (e), (g) (Telecommunications Act of 1996); 18 U.S.C. § 1039(b)(1), (c)(1), (g) (Telephone Records and Privacy Protection Act of 2007 (TRPPA)).[8] The "except as required by law" qualification to the Telecommunications Act's general duty of telecommunications carriers to protect the confidentiality of customer proprietary network information, 47 U.S.C. § 222(c)(1), includes court orders. *ICG Commc'ns, Inc. v. Allegiance Telecom*, 211 F.R.D. 610, 612-14 (N.D. Cal. 2002) (discovery order meets "except as required by law" exception in section 222(c)(1)). Here, of course, the Government obtained court orders from the FISC pursuant to 50 U.S.C. § 1861, for the production of the telephony metadata. The availability of such business records under that statute—not challenged here—further undermines Plaintiffs' argument of a reasonable expectation of privacy derived from statutes.[9]

---

[8] Subsection (g) of 18 U.S.C. § 1039, titled "Nonapplicability to law enforcement agencies," explicitly provides that the statute "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States … or of an intelligence agency of the United States."

[9] The cases Plaintiffs rely upon for the related proposition that legislative action constitutes relevant evidence of what society considers reasonable are not third-party doctrine cases. Pls.' Opp. at 21 & n.26 (citing *Bissonette v. Haig*, 800 F.2d 812 (8th Cir. 1986) (en banc) (claim that U.S. Army unconstitutionally seized plaintiffs by occupying the Village of Wounded Knee, South Dakota) and *United States v. Ziegler*, 456 F.3d 1138 (9th Cir. 2006) (claim that search of defendant's workplace computer violated his Fourth Amendment rights)); *id.* at 35 n.41 (citing *United States v. Maynard*, 615 F.3d 544, 564 (D.C. Cir. 2010) (claim that police's attaching GPS tracker to defendant's car violated his Fourth Amendment rights), *aff'd on other grounds*, *United States v. Jones*, 132 S. Ct. 945 (2012)). Under *Smith*, society is not prepared to recognize as reasonable expectations of privacy in phone numbers dialed because the caller voluntarily turns this information over to the telephone company; legislative action or public opinion polls are simply not relevant to this analysis.

2. Privacy policies unilaterally adopted by telecommunications service providers do not alter the analysis under *Smith*.

Plaintiffs next attempt to ground both a possessory interest and a legitimate expectation of privacy in policies adopted by their telecommunications service providers governing the use and disclosure of customer information. Pls.' Opp. at 15-18, 32-34. According to Plaintiffs, they have "affirmatively" sought to protect metadata pertaining to their telephone calls by entering into contracts with their providers "containing provisions for the very purpose of excluding others, *including the Government*, from accessing such records." *Id.* at 1 (emphasis added); *see also id.* at 15 (Plaintiffs "have entered into contracts explicitly intended to provide [privacy] protection" for records of their calls). Plaintiffs view these "explicit contractual terms" as giving them a "possessory interest" in the call detail records that their service providers create and maintain for their own business purposes, and that this possessory interest includes a right to "exclude" others, including the Government, from "accessing" them. *Id.* at 16-17, 32. Plaintiffs also contend that these "explicit contract terms" endow them with a "legitimate expectation of privacy" in metadata about their calls for purposes of the Fourth Amendment. *Id.* at 18, 20, 32-36. The argument is elaborately constructed but lacks foundation in fact or law.

Notably, Plaintiffs do not attach to their opposition or reproduce therein the terms of the privacy policies on which they so heavily rely. Defendants, however, have attached hereto the

---

Nor do these cases support the proposition that mere bills proposed by individual legislators, as opposed to duly enacted laws, are evidence of what society as a whole regards as reasonable. *Bissonette*, 800 F.2d at 814 (considering "[a]cts of Congress" as evidence of what society as a whole regards as reasonable); *Maynard*, 615 U.S. at 546 (considering state laws as evidence of what society recognizes as reasonable). Additionally, legislation that, according to Plaintiffs, forecloses state and local government from obtaining cell phone tracking information without a warrant (Pls.' Opp. at 22), is entirely beside the point. The Section 215 telephony metadata program challenged here does not involve monitoring by the Government of individuals' locations. *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. No. BR 13-158, at 5 (FISC Oct. 11, 2013); *see also* Defs.' Mem. at 33.

Verizon and AT&T privacy policies to which Plaintiffs refer. Exhs. 5 and 6, respectively.[10] It is readily apparent that these are not contracts that Plaintiffs "affirmatively" bargained for to guarantee a right to protect information about their calls from disclosure. Rather, they are standardized corporate policies, unilaterally developed by Plaintiffs' telecommunications service providers, that Plaintiffs (and all other subscribers) must accept as conditions of service. AT&T Privacy Policy at 5 ("[u]se of our products and services … [is] subject to this Privacy Policy"); Verizon Privacy Policy at 3 ("[t]his policy applies to Verizon customers in the United States"); *see* Verizon Wireless Customer Agreement (Exh. 7, hereto) at 1 ("[b]y entering this Agreement you consent to our data collection, use, and sharing practices described in our Privacy Policy"); AT&T Wireless Customer Agreement (Exh. 8, hereto) at 1 ("This Agreement, including the AT&T Privacy Policy … make up the complete Agreement between you and AT&T").[11] *See also In re Smartphone Geolocation Data Application*, No. 13-ms-242, 2013 WL 5583711, at *10-11 & n.29 (E.D.N.Y. May 1, 2013) (noting standard practice among telecommunications companies, including Verizon, of requiring customers to agree to terms and conditions of privacy policies governing the companies' use of personal information).

These corporate privacy policies, the terms of which Plaintiffs had no choice but to accept, also contain none of the rights-creating language that Plaintiffs suggest. Rather, they inform subscribers of the "many ways" in which the providers have unilaterally determined they will collect, use, and store customer information, including "call records," and share it with various entities. *See* AT&T Privacy Policy at 1-2, 8-10; Verizon Privacy Policy at 4, 5, 10-12. They advise customers, moreover, that the policies are subject to change by the providers at any

---

[10] Respectively *available at* http://www.verizon.com/about/ privacy/policy/#insideVz and http://www.att.com/gen/privacy-policy?pid=2506 (last visited May 23, 2014).

[11] Respectively *available at* http://www.verizonwireless.com /b2c/support/customer-agreement and http://www.att.com/shop/en/legalterms.html?toskeywirelessCustomerAgreement (last visited May 26, 2014).

time. *See* Verizon Privacy Policy at 18 ("we reserve the right to make changes to this Privacy Policy"); AT&T Privacy Policy at 1 "[w]e will always provide you with notice of material changes to this policy"). They contain no terms providing subscribers themselves a right to determine who will be "excluded from" access to provider records containing information about their calls, or that could remotely be construed as giving subscribers a "possessory" interest in what are indisputably the providers' own business records.[12] This Court concluded in *Klayman v. Obama* that the plaintiffs there "ha[d] not offered any theory as to how they could have a possessory interest in the phone data held by [their telecommunications service provider]." 957 F. Supp. 2d 1, 30 n.41 (D.D.C. 2014). As it turns out, neither have Plaintiffs here.

Most devastating for Plaintiffs' argument, however, the "explicit contract terms" of both policies state plainly that the companies will share customer information *with government entities to comply with court orders.* The AT&T Privacy Policy states that, "There are … occasions when we provide Personal Information to … other entities, *such as government agencies*, … without your consent, "including sharing to … *[c]omply with court orders*." Exh. 6 at 9-10 (emphasis added). The Verizon Privacy Policy advises customers that, "We may disclose information that individually identifies our customers … in certain circumstances, such as … to comply with valid legal process, *including court orders*." Exh. 5 at 11 (emphasis added). Of course, providers participating in the NSA's bulk telephony metadata program produce call detail records containing metadata about their customers' telephone calls in compliance with

[12] Both the AT&T and Verizon policies inform customers that the companies share customer proprietary network information (CPNI) within their respective corporate families for marketing purposes, and that customers may choose to opt out of such sharing of their CPNI on request. AT&T Privacy Policy at 21-22; Verizon Privacy Policy at 9-10, 12-13. These statements merely acknowledge and reprise the statutory rights conferred on subscribers by the Telecommunications Act of 1996, 47 U.S.C. § 222, and do not represent an independent source of contractual rights that Plaintiffs bargained for. As noted *supra*, at 11, section 222(c)(1) expressly allows for the disclosure of CPNI "as required by law," and creates no legitimate expectation that CPNI will not be produced to the Government in response to court orders.

court orders issued by the FISC. Thus, regardless of whatever else the privacy policies cited by Plaintiffs may contain, they cannot be the source of a reasonable expectation that information about Plaintiffs' calls will not be turned over to the Government to comply with FISC orders, because their "explicit contract terms" say just the opposite.[13]

In the final analysis, however, regardless of what the corporate privacy policies cited by Plaintiffs may contain, they are legally irrelevant to the question of whether Plaintiffs have a reasonable expectation of privacy in telephony metadata. This is so for two reasons. First, *Smith* already rejected the very argument that Plaintiffs endeavor to make here. *See* Defs.' Mem. at 28-29. *Smith* held, in accordance with a long line of precedent before and since, that persons who turn over information to third parties, such as telephone users who convey dialing information to providers, can have no legitimate expectation of privacy in the information thus revealed, and "'take[ ] the risk ... that the information will be conveyed by that [third party] to the Government ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'" 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443). Thus, even if Plaintiffs' "confidence" in their providers' privacy policies were not wholly unwarranted in the circumstances here, they could still claim no legitimate expectation of privacy. *Id.* at 743-44.[14]

---

[13] Plaintiffs' cite *Ziegler*, 456 F.3d at 1144-46, for the proposition that "community norms" may give rise to reasonable expectations of privacy. Pls.' Opp. at 21 n.26. That decision was, however, withdrawn and replaced by an opinion that did not adopt the type of "community norms" analysis that Plaintiffs invoke. *United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007). In any event, so far as the privacy policies cited by Plaintiffs reflect industry norms in the telecommunications sector, they tend to defeat, not support, expectations of privacy under the circumstances of this case.

[14] For the same reason, Plaintiffs' reliance on *Katz v. United States,* 389 U.S. 347, 351-52 (1967), for the proposition that what a person "seeks to preserve as private ... may be constitutionally protected," *see* Pls.' Opp. at 16, 20, is also misguided. As the Court in *Smith* explained, the conduct of a person who places a telephone call "[can] not have been calculated to preserve the privacy of the number [she] dialed." 442 U.S. at 743.

Second, it was argued in *Smith* that because it was not the ordinary practice of telephone companies, for billing purposes, to keep records of local calls such as Smith had made, his expectation of privacy in the numbers he had dialed was legitimate. *Id.* at 745. The Court rejected this argument for the reason, *inter alia*, that it would make a "crazy quilt of the Fourth Amendment" to hinge its protections in each case "on the billing practices of a private corporation." *Id.* So, too, here, the protections afforded by the Fourth Amendment should not be made to ebb and flow unpredictably according to the terms of individual corporate privacy policies that may differ from one to the next, and may be altered at any time.[15]

3. Characterizations of telephony metadata as "highly personalized" are irrelevant, as they were in *Smith*.

Plaintiffs also point to the "highly personalized" nature of telephony metadata, citing congressional findings in TRPPA such as "'call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more'" and "'the information contained in call logs may include a wealth of personal data.'" Pls.' Opp. at 12-15 (quoting Pub. L. 109-476, § 2, Jan. 12, 2007, 120 Stat. 3568). Under the telephony metadata program, however, "the name, address, or financial information of a subscriber or customer," or any party to a call, is explicitly *excluded* from the telephony metadata produced to the NSA. Primary

[15] The foregoing discussion also dispenses of Plaintiffs' labored attempt to equate the production of information from a corporate storehouse of business records with the physical search of an individual's dwelling as challenged in *Jones v. United States*, 362 U.S. 257 (1960). *See* Pls.' Opp. at 19-20. In *Jones*, the Court held that the petitioner's temporary use of an absent friend's apartment, with the friend's permission, gave rise to a legitimate expectation of privacy in the apartment that was invaded by the Government's search of the premises. 362 U.S. at 259, 265-67; *see also Rakas v. Illinois*, 439 U.S. 128, 142-43 (1978) (construing *Jones*). It should not require explanation that nothing in Plaintiffs' commercial relationship with their telephone companies, including the companies' privacy policies, creates a legitimate expectation of privacy in the companies' business records such as an occupant may claim in his dwelling place, the "sanctity of [which] is "embedded in our traditions" and accorded "special protection" by the Fourth Amendment. *Payton v. New York*, 445 U.S. 573, 585-86, 601 (1980); *Georgia v. Randolph*, 547 U.S. 103, 115 (2006). Moreover, *Jones* did not involve the third-party doctrine. The case concerned a search of an apartment that Jones occupied, not the acquisition of information that he had disclosed to his friend (or anyone else).

Order at 3 n.1 (Shea Decl. Exh A); Secondary Order at 2 (Shea Decl. Exh. B). And the Government is strictly prohibited under current FISC orders from ascertaining identifying information associated with any metadata beyond two hops from a suspected-terrorist selector, a very small percentage of the total. *See* Def.'s Mem. at 8-9. Thus, while such information may be "easily available," Pls.' Opp. at 13, the Government is extremely constrained in its ability to find it out. These restrictions also prevent the type of intrusive tracking of individuals' personal lives that concerned the justices concurring in *Jones*, 132 S. Ct. 945. *See* Pls.' Opp. at 28-30.

Even more fundamentally, Plaintiffs' argument about the "highly personalized" nature of telephony metadata was rejected by *Smith* itself. The potential for telephone call records and bank records to reveal personal information was recognized in the dissenting opinions in both *Smith* and *Miller*, and the Court nonetheless found no reasonable expectation of privacy in either type of record. *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) (a list of the numbers dialed from a private telephone "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."); *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) ("the totality of bank records provides a virtual current biography."). There is nothing new or controversial about this argument that requires an "empirical analysis" or evidentiary support by a Professor of Computer Science. Pls.' Opp. at 13-15. Compare *id.* at 13-14 ("'[M]etadata is often a proxy for content.'") (quoting Declaration of Professor Edward Felton); with *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) ("The numbers dialed from a private telephone . . . are not without 'content.'"). Thus, even where the police know the identity of the caller, and there are no restrictions on their ability to find out who the phone numbers the caller dials belong to, there is still no reasonable expectation of privacy in the numbers dialed under the Fourth Amendment.

4. *Smith* and the third-party doctrine control here, not Plaintiffs' views about societal expectations of privacy in 1792.

Finally, Plaintiffs tender for the Court's consideration several principles that they maintain should guide the decision of this case instead of *Smith*. In brief, they submit that to preserve from incursion by advancing technology "that degree of privacy against government that existed when the Fourth Amendment was adopted," the Court must protect expectations of privacy that Americans would have had in their postal communications in 1792, when "law enforcement resources were neither applied nor even available to address crime or intelligence gathering." Pls.' Opp. at 7-9, 42-45. The guidance Plaintiffs offer would lead the Court far astray, however, from settled Fourth Amendment doctrine.

First, the Supreme Court has typically invoked a mandate to "preserv[e] that degree of privacy against government that existed when the Fourth Amendment was adopted," in circumstances involving the use of advanced technology to acquire information from or about constitutionally protected areas (such as the interior of the home) that could not otherwise have been obtained without a physical intrusion. *See Kyllo*, 533 U.S. at 34 (thermal imaging of a private home); *United States v Karo*, 468 U.S. 705, 714-15 (1984) (use of electronic device to determine that a traced article was located in a particular residence); *Silverman v. United States,* 365 U.S. 505, 506-07, 511-12 (1961) (use of "spike mike" attached to heating duct to overhear conversations within petitioner's house); *Goldman v. United States*, 316 U.S. 129, 138-40 (1942) (Murphy, J., dissenting) (cited in Pls.' Opp. at 8); *cf. Jones*, 132 U.S. at 949-50 & n.3 (physical intrusion on a person's "effects" to obtain information).

The Court has observed, however, that assessing the reasonableness of expectations of privacy "when the search of [other] areas such as telephone booths [or] automobiles … is at issue" is a more difficult exercise. *Kyllo*, 533 U.S. at 34. A court should not undertake that task, as Plaintiffs suggest, by attempting to gauge early Americans' expectations of what their

fledgling government had the wherewithal to accomplish using technology available in 1792. The Supreme Court's decisions make clear, instead, that *Katz'* analysis turns on the expectations of privacy in a modern society. *See, e.g., California v. Ciraolo*, 476 U.S. 203, 213-14 (1986); *Katz*, 389 U.S. at 352; *see also Maynard*, 615 F.3d at 559. Thus, individuals have no legitimate expectation that items in their back yards will not be observed from passing airplanes, *Ciraolo*, 476 U.S. at 209, 212-14; that electronic tracking devices will not be concealed in the goods they purchase, *United States v. Knotts*, 460 U.S. 276, 278-79, 282 (1983); or that invited guests will not record their conversations using microphones hidden on their persons, *United States v. White*, 401 U.S. 745, 748-54 (1971) (plurality), even though Americans in 1792 could not have begun to imagine such events. The Supreme Court "ha[s] never equated" technological enhancement of the Government's capacity to detect crime (or fight terrorism) "with unconstitutionality," *Knotts*, 460 U.S. at 284, and this Court must reject Plaintiffs' invitation to do so here.

Plaintiffs also overlook (again) the third-party doctrine. Under the third-party doctrine on which *Smith* is based, the only relevant inquiry is whether an individual has voluntarily conveyed the information in question to someone else, thereby assuming the risk that party will reveal the information to the government. *Smith*, 442 U.S. at 743-34; *see also Miller*, 425 U.S. at 443. It is that voluntary conveyance of information to a third party that extinguishes any expectation of privacy entitled to protection, no matter how tenaciously the Fourth Amendment would otherwise have guarded that interest. *See Smith*, 442 U.S. at 743-44. Thus, to preserve the same degree of privacy against government intrusion that existed in 1792, the Fourth Amendment prohibits unauthorized electronic surveillance by the Government to overhear conversations taking place in a person's home, *Alderman v. United States,* 394 U.S. 165, 176-80 (1969); *Silverman*, 365 U.S. at 511-12, but that same person has no legitimate expectation of privacy in information he conveys in conversation with an invited guest who happens to be acting as a

police informant. *White*, 401 U.S. at 248-54; *On Lee v. United States*, 343 U.S. 747, 752-54 (1952); *see Maynard*, 615 F.3d at 566 (noting that "the police may without a warrant record one's conversations by placing an undercover agent in one's midst, but may not do the same by wiretapping one's phone") (internal citations omitted); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1043 (D.C. Cir. 1978) ("To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections.").

Likewise, it has been settled since at least 1877 that "[l]etters and sealed packages … in the mail are as fully guarded from examination and inspection" by the Fourth Amendment "as if they were retained by the parties forwarding them in their own domiciles." *Ex Parte Jackson*, 96 U.S. 727, 733 (1877). Yet the courts have uniformly held, in rejecting Fourth Amendment challenges to "mail covers," that individuals who send or receive mail have no legitimate expectation of privacy in the names and addresses placed on the exterior of mailed items, because they are knowingly exposed to postal employees and others. *See Reporters Committee,* 593 F.2d at 1056-57 & n.87.[16]

Equally so, therefore, the third-party doctrine dictates that individuals, no matter how great their expectation of privacy in the contents of their communications in 1792, or 2014, "can claim no legitimate expectation" of privacy in dialed telephone numbers or other communications routing information conveyed to (or created by) third-party providers. *Smith,* 442 U.S. at 743. As the court recognized in *Smith v. Obama,* Mem. Decision at 8, that is the principle that must determine the outcome of this case.

---

[16] *See also United States v. Hinton*, 222 F.3d 664, 675 (9th Cir. 2000) (citing *United States v. Choate*, 576 F.2d 165, 174-77 (9th Cir. 1978)); *United States v. Osunegbu*, 822 F.2d 472, 480 n.23 (5th Cir. 1987); *United States v. De Poli*, 628 F.2d 779, 785-86 (2d Cir. 1980).

C. Even if Plaintiffs Had a Legitimate Expectation of Privacy in Telephony Metadata, They Have Not Alleged an Unreasonable Search of Information About Their Telephone Calls.

1. Plaintiffs have not alleged an invasion of any privacy interest they may have in metadata pertaining to their calls.

Plaintiffs provide no response to the Government's point that records of their calls are not searched, in any constitutionally meaningfully way, every time an electronic query of the metadata is performed to determine what phone numbers (or other identifiers) have been in contact with a suspected-terrorist selector. Rather, Plaintiffs simplistically claim, without citing any authority, that "[a] search is a search regardless of whether a human combs through boxes of documents or whether a computer is used to automate the process." Pls.' Opp. at 36. Plaintiffs fail to acknowledge, let alone respond to, the point that an electronic query that returns no records of their calls does not reveal the contents of those records to any sentient being, and is thus more analogous to a canine sniff of luggage or chemical field test to ascertain the presence or absence of drugs, which do not expose any noncontraband items to the government, and which therefore, as held in *Place*, 462 U.S. at 707, and *United States v. Jacobsen*, 466 U.S. 109, 123 (1984), do not infringe on any Fourth Amendment privacy interests. Defs.' Mem. at 23-24, 35-36. For this reason as well, the complaint must be dismissed.

2. Even assuming a search of metadata pertaining to Plaintiffs' calls occurs, it would be reasonable under the "special needs" doctrine.

Even if there were a reasonable expectation of privacy in telephony metadata, *contra Smith*, and an invasion of that privacy interest, *contra Place* and *Jacobsen*, Plaintiffs' Fourth Amendment claim still fails because the program is reasonable under the Supreme Court's special needs doctrine. *Id.* at 36-38. The balance of the Government's counter-terrorism interests furthered by the telephony metadata program, and the privacy interests at stake, tips in favor of the program's constitutionality, because there is no reasonable expectation of privacy in

telephony metadata under *Smith*; any privacy interest that Plaintiffs nonetheless claim exists is mitigated by the substantial restrictions on review and dissemination of metadata that are core features of the program; the governmental interest in identifying and tracking terrorist operatives to prevent terrorist attacks is overwhelmingly important; and the telephony metadata program is an effective way of accomplishing that interest. *Id.* at 36-37.

Plaintiffs raise three arguments in response. First, while Plaintiffs concede that "fighting terrorism is a critical role of government," Pls.' Opp. at 37 n.43; *see also id.* at 38 ("Plaintiffs do not dispute the importance of identifying terrorist operatives and preventing terrorist attacks"), they claim that there must be "'an imminent terrorist attack'" for the telephony metadata program to be lawful under the special needs doctrine. *Id.* at 39 (quoting *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000)). But the *Edmond* Court merely remarked that "the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack," 531 U.S. at 44, a proposition that is "neither controversial nor constraining." *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006).

The *Edmond* Court also said that its holding that a drug interdiction checkpoint was unconstitutional "does not affect the validity of . . . searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute." 531 U.S. at 47-48. Courts have recognized that such searches are justified by the ongoing, substantial, and very real threat of terrorism facing the United States, not by any imminent threat of a particular terrorist attack, and have upheld them under the special needs doctrine. *See, e.g., Elec. Privacy Info. Center v. DHS*, 653 F.3d 1, 10 (D.C. Cir. 2011) (use of scanner to search airline passengers held constitutional under special needs doctrine); *United States v. Hartwell*, 436 F.3d 174, 178-81 (3d Cir. 2006) (search of airplane passenger at airport checkpoint held constitutional under special needs doctrine). Indeed, in *MacWade*, 460 F.3d at

272, the court held that the government may employ random, suspicionless baggage searches in order to safeguard the New York City subway system from terrorist attack, specifically finding that no express threat or special imminence is required; "[a]ll that is required is that the 'risk to public safety be substantial and real' instead of merely 'symbolic.'" *Id.* (quoting *Chandler v. Miller*, 520 U.S. 305, 322-23 (1997), relied upon by Plaintiffs, *see* Pls.' Opp. at 31, 36, 39). The court went on to find the threat to the subway system "sufficiently immediate," in light of previous thwarted plots to bomb the New York City subway system, its continued desirability as a target, and recent (at the time) bombings of public transportation systems in Madrid, Moscow, and London. *MacWade*, 460 F.3d at 272.

Similarly, the telephony metadata program is predicated on the substantial and real threat posed by international terrorist organizations under investigation by the Government. The FISC, the court to which the Government presents threat information to obtain production orders under the program, has found similar bulk Internet metadata collection analogous to suspicionless searches and seizures that have been upheld under the special needs doctrine. FISC Op. & Order, Dkt. No. PR/TT, at 31, 50-54 (public version released Nov. 18, 2013) (Exh. 9, hereto). In doing so, the FISC noted that the Government's interest under the program "has even greater 'immediacy' [than other interests that have been held to justify suspicionless searches] in view of the . . . intelligence reporting and assessment regarding ongoing plans for large scale attacks within the United States." *Id.* at 52. Plaintiffs' accusations that the Government has "no evidence" to justify this program are therefore baseless and inaccurate.

Second, Plaintiffs claim that the Government can obtain any valuable intelligence information it obtains under the program through "less intrusive means," or "alternative legal authorities." Pls.' Opp. at 40. But the case law is clear that "[a]s to efficacy under the [special needs doctrine], the Government need not make a showing that it is using the least intrusive

means available. . . . Rather, the question is whether the Government has chosen 'a reasonably effective means of addressing' the need." FISC Op. & Order, Exh. 9, at 52 (citing *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 837 (2002); *United States v. Martinez-Fuerte*, 428 U.S. 543, 556-57 n.12 (1976)). *See also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995). The choice among reasonable alternatives "remains with the government officials who have a unique understanding of, and a responsibility for, limited public resources." *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 453-54 (1990); *see also Martinez-Fuerte*, 428 U.S. at 566. In addition, a low percentage of positive outcomes among the total number of searches does not render a program ineffective. FISC Op. & Order, Exh. 9, at 53 & n.38 (citing *Sitz*, 496 U.S. at 454 ("detention of the 126 vehicles that entered the checkpoint resulted in the arrest of two drunken drivers"); *Martinez-Fuerte*, 428 U.S. at 546 & n.1, 554 (out of "roughly 146,000 vehicles" temporarily seized at checkpoint near border, 171 were found to contain deportable aliens)). The Government has demonstrated that the telephony metadata program is a reasonably effective means of identifying unknown terrorist operatives. *See* Shea Decl. ¶¶ 12, 44-63; *ACLU v. Clapper*, 959 F. Supp. 2d 724, 747-48, 755-56 (S.D.N.Y. 2013).

Third, Plaintiffs claim the Government has backed away from supposed characterizations of the program as "vital" and "necessary"—words Plaintiffs seize on without context. *Id.* at 40-42. As noted above, the special needs doctrine does not, in fact, demand that the program be indispensable to be lawful. In addition, Plaintiffs' assertion that the Government "lied" about the importance of the telephony metadata program in its applications to the FISC, Pls.' Opp. at 40-41, is unsupported, and wrong. The Government's representations about the importance of the program for national security, both in seeking the FISC's authorization, and in litigation concerning the program's legality, have been consistent, and accurate. As the FISC wrote in its August 29, 2013, opinion, "the government has demonstrated through its written submissions . . .

that [bulk telephony metadata] production has been and remains *valuable* for obtaining foreign intelligence information regarding international terrorist organizations." Aug. 29, 2013, FISC Op. at 5-6 (emphasis added). *See also id.* at 20 (quoting a prior FISC decision stating that the "'finding of [the metadata's] relevance most crucially depended on the conclusion that bulk collection is necessary for NSA to employ tools that are likely to generate *useful investigative leads* to help identify and track terrorist operatives'")) (emphasis added); *id.* at 21 (explaining that bulk collection "is necessary to create a historical repository of metadata that enables NSA to find or identify" terrorist operatives, and that "the success of [NSA's] investigative tool" depends on the bulk collection). While the March 2, 2009 FISC opinion on which Plaintiffs rely (*see* Pls.' Opp. at 40-41) asked the Government to justify the continued operation of the program based on its value to the nation's security, Mar. 2, 2009 FISC Op. at 13, the Government did so in terms similar to those quoted above, *see* In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, BR 09-09, Aug. 17, 2009 Report of the United States at 6-9,[17] and the FISC permitted the program to continue on that basis. *See* Shea Decl. ¶¶ 39-40.

Thus, it has always been made clear to the FISC that the bulk telephony metadata program yields foreign intelligence information that is "useful" and "valuable" to the FBI's counter-terrorism mission, and that access to bulk metadata is "necessary" for the NSA to make this contribution to the nation's security. And that is all that would be required to uphold the program under the special-needs doctrine, even if it involved a Fourth Amendment search (or seizure) of which Plaintiffs could complain.

CONCLUSION

For the reasons stated above and in Defendants' opening memorandum of points and authorities, this case should be dismissed.

---

[17] Available at http://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

Dated: June 5, 2014

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
JULIA A. BERMAN
Trial Attorney

United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Counsel for Defendants

EXHIBIT 1

Verizon Transparency Report

National Security

The table below sets forth the number of national security demands we received in 2013. We note that while we now are able to provide more information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited.

National Security Demands

	Jan. 1, 2013 – June 30, 2013	July 1, 2013 – Dec. 31, 2013
National Security Letters	0-999	0-999
Number of customer selectors	2000-2999	2000-2999
FISA Orders (Content)	0-999	*
Number of customer selectors	4000-4999	*
FISA Orders (Non-Content)	0-999	*
Number of customer selectors	0-999	*

* The government has imposed a six month delay for reporting this data

National Security Letters

We explained in our Transparency Report that we had received between 1000 and 1999 National Security Letters in 2013. We separately provide details for the first half and second half of 2013 now; in the future, we will make semi-annual reports regarding only the immediately preceding six month period. In the first half of 2013, we received between 0 and 999 NSLs from the FBI. Similarly, we received between 0 and 999 NSLs in the second part of 2013. In the first six months of the year, those NSLs sought information regarding between 2000 and 2999 "selectors" used to identify a Verizon customer. The same is true for the second half of 2013. (The government uses the term "customer selector" to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of "customer accounts." An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.)

As we explained in our Transparency Report, the FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.

FISA orders

The government requires that we delay the report of any orders issued under the Foreign Intelligence Surveillance Act for six months. Thus, at this time, we may report FISA information only for the first half of 2013. In July, or soon thereafter, we will report FISA information regarding the second half of 2013.

Content
From January 1, 2013 through June 30, 2013, we received between 0 and 999 FISA orders for content. Those orders targeted between 4000 and 4999 "customer selectors" used to identify a Verizon customer.

Non-Content
From January 1, 2013 through June 30, 2013, we received between 0 and 999 reportable FISA orders for non-content. Some FISA orders that seek content also seek non-content; we counted those as FISA orders for content and to avoid double counting have not also counted them as FISA orders for non-content. Those orders targeted between 0 and 999 "customer selectors."

We will update our Transparency Report again in the middle of the year.

Download a PDF of this page
(/themes/site_themes/transparency/Verizon-Transparency-Report-National-Security.pdf)

© 2014 Verizon

EXHIBIT 2

(/content/csr/home.html)
People and Community (/content/csr/home/people.html)
Environment (/content/csr/home/environment.html)
Technology (/content/csr/home/technology.html)
Blog (/content/csr/home/blog.html)
FAQ, Governance, Policies (/content/csr/home/frequently-requested-info.html)
2012 Sustainability Report (/content/csr/home/2012-sustainability-report.html)



Home(/content/csr/home.html) > FAQ, Governance, Policies (/content/csr/home/frequently-requested-info.html) > Governance (/content/csr/home/frequently-requested-info/governance.html) > Transparency Report

Transparency Report

Introduction to this report

We take our responsibility to protect your information and privacy very seriously, and we pledge to continue to do so to the fullest extent possible and always in compliance with the law of the country where the relevant service is provided. Like all companies, we must provide information to government and law enforcement agencies to comply with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid and that our responses comply with the law and our own policies.

This report provides specific information for all of 2013 regarding the number and types of demands to which we responded, with the exception of certain information that the U.S. Department of Justice allows us to report only for the first six months of 2013. In the future, we'll issue reports on a semi-annual basis.

Our commitment to you

Interest in this topic has increased in the last year. As you might expect, we may make adjustments to our reporting processes and create ways to track forms of demands in the future. We're committed to providing you with as much transparency and accuracy in this reporting as is possible. This includes:

- Including new information as we are allowed by government policy changes.
- Considering ways to enhance the detail provided in this report as we begin to track these demands consistent with what can be reported publicly.

The chart below includes hyperlinks to additional information on the category of data reported.

National Security Demands(/content/csr/home/frequently-requested-info/governance/transparencyreport/national--security-demands-.html)	
National Security Letters (Jan. 1-Dec. 31, 2013)	
Total Received	2,000 - 2,999
Number of Customer Accounts	4,000 - 4,999
Foreign Intelligence Surveillance Act (Jan. 1-June 30, 2013)	
Total Content	0 - 999
Customer Accounts	35,000 - 35,999
Total Non-Content	0 - 999
Customer Accounts	0 - 999

FAQ, GOVERNANCE, POLICIES

ISSUE BRIEF LIBRARY (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/ISSUE-BRIEFS-REDIRECT.HTML)

ENVIRONMENT (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/ENVIRONMENT.HTML)

SOCIAL (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/SOCIAL.HTML)

GOVERNANCE (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/GOVERNANCE.HTML)

AT&T Political Engagement Report (/content/csr/home/frequently-requested-info/governance/ATTPoliticalEngagementRepor

Transparency Report (/content/csr/home/frequently-requested-info/governance/transparencyreport.html)

National Security Demands (/content/csr/home/frequently-requested-info/governance/transparencyreport/national--security-demands-.html)

Total U.S. Criminal and Civil Litigation Demands (/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html)

Partial or no Data Provided (/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html)

Location Demands (/content/csr/home/frequently-

Total U.S. Criminal & Civil Litigation Demands(/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html)

Total Demands (Federal, State and Local; Criminal and Civil)			301,816
Subpoenas		248,343	
Criminal	223,659		
Civil	24,684		
Court Orders		36,788	
Historic	16,478		
Real-time	20,310		
Search Warrants		16,685	
Stored Content	5,690		
All Others	10,995		

Partial or No Data Provided
(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)
(/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html)

Total		17,463
Rejected/Challenged	3,756	
Partial or No Information	13,707	

Location Demands
(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)
(/content/csr/home/frequently-requested-info/governance/transparencyreport/location-demands.html)

Total		37,839
Historical	24,229	
Real-time	12,576	
Cell Tower Searches	1,034	

Emergency Requests(/content/csr/home/frequently-requested-info/governance/transparencyreport/emergency-requests.html)

Total		94,304
911	74,688	
Exigent	19,616	

International Demands
(/content/csr/home/frequently-requested-info/governance/transparencyreport/international.html)

Total Demands		22
Law Enforcement	11	
URL/IP Blocking	11	

Share:

requested-info/governance/transparencyreport/location-demands.html)

Emergency Requests (/content/csr/home/frequently-requested-info/governance/transparencyreport/emergenc requests.html)

International Demands (/content/csr/home/frequently-requested-info/governance/transparencyreport/internatior

POLICIES (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/POLICIES.HTML)

EXTERNAL RECOGNITION (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/EXTERNAL-RECOGNITION.HTML)

MATERIALITY ASSESSMENT (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/MATERIALITY-ASSESSMENT.HTML)

MULTIMEDIA (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/MULTIMEDIA.HTML)

SUSTAINABILITY REPORT/GOALS ARCHIVE (/CONTENT/CSR/HOME/FREQUENTLY-REQUESTED-INFO/SUSTAINABILITYREPORTARCHIVE.HTML

on twitter

(https://twitter.com/attaspire)

Follow our team:



(https://twitter.com/johnfschulz)
@johnfschulz

(https://twitter.com/johnfschulz)
John Schulz, AVP of Sustainability Operations



(https://twitter.com/dutchnicole)
@DutchNicole

(https://twitter.com/dutchnicole)
Nicole Anderson, Executive Director of Philanthropy



(https://twitter.com/kathrynnisbet)
@KathrynNisbet

(https://twitter.com/kathrynnisbet)
Kathryn Nisbet, Manager, Do One Thing



ADDITIONAL RESOURCES

- Our Privacy Policy (http://www.att.com/gen/privacy-policy?pid=2506)
- Download the full Transparency Report

LATEST UPDATES

(/content/dam/csr/transpreport/ATT_Transpar
20Report.pdf)



Learn more



Learn more



Learn more



Learn more



Learn more



Learn more

Privacy Policy(http://www.att.com/privacy/) | Careers(http://www.att.jobs/) | Contact Us (http://www.att.com/ecomtactus/) | Terms of Use(http://www.wireless.att.com/legal) | Site Map(http://www.att.com/sitemap) | Accessibility(http://www.att.com/gen/general?pid=10190) | Advertising Choices(http://www.att.com/internal/adchoices) | Broadband Information(http://www.att.com/internal/broadbandinfo)

att.com Shop. Service. Support(http://www.att.com/)
att.net E-mail · News · Weather & More(http://www.att.net/)

© 2014 AT&T Intellectual Property(http://www.att.com/gen/privacy-policy?pid=2587). All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.
AT&T36USC220506

(https://www.bbb.org/online/consumer/cks.aspx?id=110020911221)

TRUSTe

(http://www.cbs.org/?page=validate&companyName=AT%26T&sealid=101)

(http://www.yellowpages.com)

Digital White & Yellow Pages
(http://www.realpageslive.com)

(http://www.att.net/teamusa)

EXHIBIT 3

Office of the Deputy Attorney General
Washington, D.C. 20530

January 27, 2014

Sent via Email

Colin Stretch, Esquire
Vice President and General Counsel
Facebook Corporate Office
1601 Willow Road
Menlo Park, CA 94025

Kent Walker, Esquire
Senior Vice President and General Counsel
Google Corporate Office Headquarters
1600 Amphitheater Parkway
Mountain View, CA 94043

Erika Rottenberg, Esquire
Vice President, General Counsel/Secretary
LinkedIn Corporation
2029 Stierlin Court
Mountain View, CA 94043

Brad Smith, Esquire
Executive Vice President and General Counsel
Microsoft Corporate Office Headquarters
One Microsoft Way
Redmond, WA 98052-7329

Ronald Bell, Esquire
General Counsel
Yahoo Inc. Corporate Office and Headquarters
701 First Avenue
Sunnyvale, CA 94089

Dear General Counsels:

Pursuant to my discussions with you over the last month, this letter memorializes the new and additional ways in which the government will permit your company to report data concerning requests for customer information. We are sending this in connection with the Notice we filed with the Foreign Intelligence Surveillance Court today.

In the summer of 2013, the government agreed that providers could report in aggregate the total number of all requests received for customer data, including all criminal process, NSLs,

and FISA orders, and the total number of accounts targeted by those requests, in bands of 1000. In the alternative, the provider could separately report precise numbers of criminal process received and number of accounts affected thereby, as well as the number of NSLs received and the number of accounts affected thereby in bands of 1000. Under this latter option, however, a provider could not include in its reporting any data about FISA process received.

The government is now providing two alternative ways in which companies may inform their customers about requests for data. Consistent with the President's direction in his speech on January 17, 2014, these new reporting methods enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

Option One.

A provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.

2. The number of NSLs received, reported in bands of 1000 starting with 0-999.

3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.

4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.

5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.

6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.[1]

7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered

[1] As the Director of National Intelligence stated on November 18, 2013, the Government several years ago discontinued a program under which it collected bulk internet metadata, and no longer issues FISA orders for such information in bulk. See http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence. With regard to the bulk collection of telephone metadata, the President has ordered a transition that will end the Section 215 bulk metadata program as it currently exists and has requested recommendations about how the program should be restructured. The result of that transition will determine the manner in which data about any continued collection of that kind is most appropriately reported.

by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.

In addition, there will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a "New Capability Order" because disclosing it would reveal that the platform, product, or service is subject to previously undisclosed collection through FISA orders. For example, a report published on July 1, 2015, will not reflect data relating to any New Capability Order received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017. After data about a New Capability Order has been published, that type of order will no longer be considered a New Capability Order, and the ordinary six-month delay will apply.

The two-year delay described above does not apply to a FISA order directed at an enhancement to or iteration of an existing, already publicly available platform, product, or service when the company has received previously disclosed FISA orders of the same type for that platform, product, or service.

A provider may include in its transparency report general qualifying language regarding the existence of this additional delay mechanism to ensure the accuracy of its reported data, to the effect that the transparency report may or may not include orders subject to such additional delay (but without specifically confirming or denying that it has received such new capability orders).

Option Two.

In the alternative, a provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.

2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.

3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

* * *

I have appreciated the opportunity to discuss these issues with you, and I am grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency. We look forward to continuing to discuss with you ways in which the

government and industry can similarly find common ground on other issues raised by the surveillance debates of recent months.

Sincerely,

James M. Cole
Deputy Attorney General

EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

ANNA J. SMITH Plaintiff, v. BARACK OBAMA, President of the United States, et al., Defendants.	Case No. 2:13-CV-257-BLW **MEMORANDUM DECISION**

INTRODUCTION

The Court has before it plaintiff Smith's motion for injunctive relief and defendants' motion to dismiss. The Court heard oral argument on May 14, 2014, and took the motions under advisement. For the reasons expressed below, the Court will grant the defendants' motion to dismiss and deny Smith's motion for injunctive relief.

BACKGROUND

The Fourth Amendment protects the right of privacy by forbidding unreasonable searches and seizures. With few exceptions, a citizen cannot be searched in violation of her reasonable expectation of privacy unless a judge has found there is probable cause to believe that she is committing a crime. This Fourth Amendment protection is violated here, Smith alleges, because the National Security Administration (NSA) is searching her telephone records without showing first that there is probable cause to believe she is engaged in criminal behavior. She asks the Court to enjoin the NSA from collecting and analyzing her telephone data.

For more than seven years, the NSA has been collecting and analyzing the telephone records of Americans to detect terrorist threats. While the agency does not listen to conversations, or identify the callers' names and addresses, it does collect the telephone numbers of all parties to a call, along with the duration and time of that call, and stores this data for five years.

The NSA's collection and analysis protocols must be periodically approved by the Foreign Intelligence Surveillance Court (FISC). The FISC prohibits the NSA from accessing the stored telephone data for any purpose other than counterterrorism or technical maintenance of the system. *See Shea Declaration (Dkt. No. 15-2)* at ¶ 31.

The NSA uses its vast trove of data to identify the telephone numbers of calls that terrorists make and receive. Before the NSA can access its telephone data, the FISC-approved protocols require the agency to first make an internal finding – authorized by one of twenty-two designated NSA officials – that a particular telephone number is associated with a terrorist organization. *Id.* at ¶ 32.

Once the NSA makes its internal determination, it may run a query through its data bank to collect (1) the telephone data of persons who made calls to – or received calls from – the suspected terrorist, and (2) the telephone data of persons who made calls to – or received calls from – the telephone numbers for any person who had direct telephone contact with the suspected terrorist. *Id.* at ¶ 23. In prior years, the scope of the query extended to a third level but "the NSA has taken immediate steps to implement restrictions [imposed by the President] limiting its review of queries to two [levels] only

and the Government is now working with the FISC to incorporate this restriction into the FISC's orders." *Id.*

Smith alleges that her own telephone data has been swept up into the NSA's broad net in violation of her Fourth Amendment rights.[1] She asks the Court to enjoin the agency from collecting and using this telephone data from her calls.[2]

ANALYSIS

The Fourth Amendment is concerned with surveillance that (1) involves a "trepassory intrusion on property" or (2) "violates a subjective expectation of privacy that society recognizes as reasonable." *See U.S. v. Jones,* 132 S.Ct. 945, 954-55 (Sotomayor, J., concurring). It is the latter interest that Smith urges here. She claims that the NSA's collection efforts violate her expectation of privacy in her telephone records.

Smith has no expectation of privacy in the telephone numbers that she dials. *See Smith v Maryland,* 442 U.S. 735 (1979). A person using the telephone "voluntarily convey[s] numerical information to the telephone company" and "assume[s] the risk that the company [will] reveal to police the numbers he dialed." *Id.* at 744.

But the data collected by the NSA goes beyond the telephone numbers that Smith dials, and reaches into her personal information. For example, the NSA's collection of

---

[1] Smith originally alleged additional claims but has conceded that they should be dismissed, leaving only the Fourth Amendment claim for resolution.

[2] The Court finds that Smith – a Verizon customer – has standing to bring this action. *See Klayman v. Obama*, 957 F.Supp.2d 1, 26-28 (D.D.C.2013) (granting standing to individual plaintiffs to challenge NSA collection of their telephone records from Verizon after finding "strong evidence" that NSA has collected Verizon metadata for the last seven years and run queries that necessarily analyzed that data).

the time and duration of phone calls is revealing: Would most citizens want to keep private the fact that they called someone at one in the morning and talked for an hour or two?

And what about location? Would most phone users expect to keep private (1) their location at any moment and (2) their travel path over time? The NSA collects "trunk identifier" data, *see Shea Declaration, supra* at ¶ 15, that shows the location where a cell-phone call enters the "trunk" system to be relayed eventually to the number being called. *See* Leslie Groll, *What Kind of Phone Data Can the NSA Collect Exactly?,* FOREIGN POLICY (June 6, 2013).[3] While this would not pinpoint a phone user's precise location, it would narrow it down considerably. *Id.*[4]; *see also State v. Earls,* 70 A.3d 630, 637 (N.J.Sup.Ct. 2013) (holding that New Jersey's constitution requires police to obtain warrant before collecting cell phone location data and noting that carriers have data that "can locate cell-phone users within buildings, and even within individual floors and rooms within buildings"). Moreover, the data also includes "comprehensive communications routing information." *See Shea Declaration, supra* at ¶ 15. While this phrase is ambiguous, it may mean that for a single call, all the trunk identifiers are collected by the NSA, allowing the agency to track "how a cell phone user moves from

---

[3] Available at http://blog.foreignpolicy.com/posts/2013/06/06/what_kind_of_phone_data_can_the_nsa_collect_exactly

[4] Trunk identifier data may be used to "locate a phone within approximately a square kilometer." Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls,* NEW YORKER (June 7, 2013), http:// www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html.

one cell phone tower to another while traveling." FOREIGN POLICY, *supra.* The speed with which the phone moves from tower to tower could indicate, for example, whether the device is being used in a car or while walking down the street.

Compare these intrusions to those faced in *Smith:* There, the Baltimore police collected the telephone numbers dialed by a suspected robber for about two days. This simple comparison reveals a looming gulf between *Smith* and this case. But the Ninth Circuit has bridged some of that chasm. In *United States v. Reed,* 575 F.3d 900 (9th Cir. 2009), the Circuit held that "there is no Fourth Amendment expectation of privacy" in data that includes the number dialed along with the length and time of the call. *Id.* at 914. The Circuit has also applied *Smith* in holding that e-mail and internet users have no expectation of privacy in the "to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account." *U.S. v. Forrester,* 512 F.3d 500, 510 (9th Cir. 2008). To the extent that an individual's telephone data collected by a cell-phone provider is no different than an individual's power consumption records collected by an electric utility, the Circuit has held that utility customers lack a reasonable expectation of privacy in such business records. *U.S. v. Golden Valley Elec. Ass'n,* 689 F.3d 1108, 1116 (9th Cir.2012).

Although the Ninth Circuit has not resolved the precise issue faced here, other courts have done so: Two of these decisions apply *Smith* to find that the NSA is not violating the Fourth Amendment. *See A.C.L.U. v Clapper,* 959 F.Supp. 2d 724 (S.D.N.Y. 2013); *U.S. v. Moalin,* 2013 WL 6079518 (S.D.Cal. 2013).

But these cases do not address a subject lurking in the shadows here: The possibility that the NSA is tracking the location of calls using the trunk identifier data discussed above. In *Jones,* five Justices wrote that the government surveillance of one's public movements for 28 days using a GPS device violated a reasonable expectation of privacy and constituted a Fourth Amendment search. *See also,* Case Comment, *Fourth Amendment – Warrantless Searches,* 127 Harv.L.Rev. 2164 (2014) (concluding that "[b]ecause the disclosure of [cell-site location information] is not necessarily voluntary, individuals still may hold an expectation of privacy in their cell-site data even under *Smith*").

The NSA denies that it is tracking location. Teresa Shea, the NSA's Director of the Signals Intelligence Directorate represents to the Court that "[t]he metadata collected by the Government pursuant to these [FISC] orders also does not include cell site locational information." *Shea Declaration, supra* at ¶ 15. A similar representation was made by the NSA's General Counsel, Robert Litt when he stated that "I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information."[5] Finally, the FISC orders submitted to the Court expressly prohibit the NSA from collecting any addresses

[5] *See Klayman,* 957 F.Supp.2d at 36 n. 57 (citing Transcript of June 25, 2013 Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction, Remarks of Robert Litt, Gen. Counsel, Office of Dir. of Nat'l Intelligence, available at http://www.dni.gov/index.php/newsroom/speeches–and–interviews/195–speeches–interviews–2013/887–transcript–newseum–special–program–nsa–surveillance–leaks–facts–and-fiction).

associated with the telephone numbers it collects, apparently precluding the collection and analysis of location data. *See Order (Dkt. No. 15-6)* at pg. 3.

Smith's briefing and argument were not extensive on this issue. While there is speculation that the NSA is tracking location, there is no evidence of that, and the agency denies it. Under these circumstances, the Court will not assume that the NSA's privacy intrusions include location tracking.

Because *Jones* does not apply, the weight of the authority favors the NSA. The Supreme Court's decision in *Smith,* supplemented by the Circuit's decisions in *Reed, Forrester,* and *Golden Valley,* and the two District Court decisions on point, *Clapper* and *Moalin,* support a finding that there is no Fourth Amendment violation here.

The contrary view is stated by *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C.2013), a thoughtful and well-written decision by Judge Richard Leon. He distinguished *Smith* by finding that the scope and duration of the NSA's collection is far beyond the individual pen register at issue in *Smith.* Of critical importance to Judge Leon was that *Smith* could never have anticipated the ubiquity of cell-phones and the fact that "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago." *Id.* at 36. As he eloquently observes, "[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life." Ultimately, he held that the plaintiffs had a likelihood of success on their Fourth Amendment claim, and he enjoined the NSA from collecting their telephone records, although he stayed his decision pending appeal.

Judge Leon's decision should serve as a template for a Supreme Court opinion. And it might yet. Justice Sotomayor is inclined to reconsider *Smith*, finding it "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *See U.S. v. Jones,* 132 U.S. 945, 957 (2012) (Sotomayor, J., concurring). The Fourth Amendment, in her view, should not "treat secrecy as a prerequisite for privacy." *Id.*

But *Smith* was not overruled, and it continues – along with the Circuit decisions discussed above – to bind this Court. This authority constrains the Court from joining *Klayman.* Accordingly, the Court will grant the defendants' motion to dismiss and deny Smith's motion for injunctive relief. The Court will issue a separate Judgment as required by Rule 58(a).

DATED: June 3, 2014

B. Lynn Winmill
Chief Judge
United States District Court

EXHIBIT 5



- **Our Company**
  - Awards and Recognition
  - Products and Services
  - Verizon Credo
  - Corporate History
  - Annual Reports
  - Corporate Governance
  - Public Policy
  - Partner Solutions
  - About Verizon Wireless
  - About Verizon Enterprise Solutions

- **Leadership Team**
  - Bios and Pictures
  - Speeches
  - Request a Speaker
  - Email Signup

- **Innovative Solutions**
  - Health Care Solutions
  - Energy Management
  - Sustainable Economy
  - Security
  - 4G LTE
  - FiOS
  - Cloud Services
  - Global IP
  - Connected Home
  - Innovation Program
  - Flex View

-
-

Search

About / Privacy Policy / Full Privacy Policy

| VZ | Disclaimer

Privacy Policy

Full Privacy Policy

- Privacy Policy Summary
- Full Privacy Policy
- Privacy Officer Message
- Recent Changes to the Policy
- Tips for Guarding Your Information
- FiOS Privacy Policy
- Browser Policy Statement
- Your California Privacy Rights
- Your Ohio Rights & Responsibilities

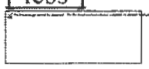
Verizon Participates in the TRUSTe Privacy Program

[more]

Verizon has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and our practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information. Verizon wants you to feel confident about your privacy when you use our Web sites (verizon.com, verizonwireless.com, mci.com, verizonbusiness.com, vzw.com, vzwshop.com, and verizon.net) so we ask TRUSTe to review these sites to ensure compliance with its guidelines. The TRUSTe program does not cover information that may be collected through downloadable software. TRUSTe's mission, as an independent third party, is to

accelerate online trust among consumers and organizations globally through its leading privacy trustmark and innovative trust solutions. If you have questions or complaints regarding our privacy policy or practices, please contact us at contact us. If you are not satisfied with our response you can contact TRUSTe here.

[less]



Verizon is accredited by the Better Business Bureau Online (BBBOnLine)

[more]

The BBBOnLine seal confirms that Verizon is an accredited business that abides by the BBB's Code of Business Practices. This Code represents sound advertising and selling practices that enhance customer trust and confidence in a business. With regard to safeguarding privacy, the BBB Code requires accredited businesses to protect any data they collect against mishandling and fraud, collect personal information only as needed, and respect the preferences of customers regarding the use of their information.

[less]

Verizon is Committed to Protecting Your Privacy

Protecting our customers' privacy is an important priority at Verizon and we are committed to maintaining strong and meaningful privacy protections. The privacy of your information is a significant responsibility and we value the trust you place in us.

Our Privacy Policy is designed to inform you about the information we collect, how we use it, and your options with regard to that collection and use. This policy also describes privacy rights you have under certain federal laws.

This policy applies to Verizon customers in the United States and to visitors to Verizon websites. For Verizon Business customers outside the United States, policies are set forth at http://www.verizonenterprise.com/terms/. Also, certain services offered to consumers as well as contracts between Verizon and its business customers (both U.S. and international) may contain additional privacy-related terms and conditions. Except as described above, this policy applies across the Verizon family of companies and the products and services they provide. The Verizon family of companies includes the companies and joint ventures controlled by Verizon, including the Verizon telephone companies, Verizon Wireless, Verizon Online and Redbox Instant by Verizon.

This policy also includes additional privacy practices that are applicable to specific Verizon offerings such as FiOS, Wireless and Redbox Instant by Verizon services.
Back to Summary

Information We Collect and How We Use It

We collect and use information about you in the following ways:

Information Collected When You Communicate with Verizon:

When you communicate with Verizon, we collect information from you that we use to deliver, provide, confirm, change, bill, monitor, maintain and repair your products and services. This information is also used to resolve issues with your order, with our products and services, or with your account. The information we collect may include your name, addresses, and other contact information; the reason for the contact; and your driver's license number and Social Security Number and payment information. We use this information to establish and maintain your customer account and billing records (including establishing credit), provide services to you, authenticate you, and contact you about products and services that we offer.

When you contact us or we contact you with calls, e-mail, in writing, or through a feature on our websites or in our applications, we may monitor or record that communication or keep a record of the transaction to help us train employees and provide high-quality customer service.

Information Collected When You Use Verizon Products and Services:

We collect information about your use of our products, services and sites. Information such as call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information, service options you choose, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, FiOS TV viewership, and other similar information may be used for billing purposes, to deliver and maintain products and services, or to help you with service-related issues or questions. In addition, this information may be used for purposes such as providing you with information about product or service enhancements, determining your eligibility for new products and services, and marketing to you based on your use of your products and services. This information may also be used to manage and protect our networks, services and users from fraudulent, abusive, or unlawful uses; and help us improve our services, research and develop new products, and offer promotions and other services.

If you subscribe to Verizon Internet access services, we may automatically measure and monitor network performance and the performance of your Internet connection to improve your, or our, service levels and products. If you contact us for service support, we also may access information about your computer, wireless device or other device settings to provide customized technical support or to install specific applications or services that you use or that are necessary to the applications or services you use.

This type of information may be aggregated or anonymized for business and marketing uses by us or by third parties. For example, aggregate or anonymous data may be used to improve our services, measure and analyze the use of services and to help make services and advertising more relevant to customers.

When you establish an online account with us, we maintain information about your user identification and password. This information is used to identify you when you sign in to your

account.

If Verizon intends to gather information from your use of our Internet access services to direct customized advertising specifically to you based on your visits over time and across different non-Verizon websites, we will provide you with notice of our plan and obtain your affirmative consent.

Please note that Verizon is not responsible for information, content, applications or services provided by others. Before you access, use, link to or download a service or application on your computer, television, wireless or other device, you should review the associated terms of service and privacy policy. Personal information you submit in those contexts may be read, collected or used by the service or application provider and others associated with these forums in a manner different from that described here.

Information Provided to Us by Third Parties:

When you purchase products or apply for service with us, we may obtain credit information about you from outside credit reporting agencies to help us with customer authentication and credit-related decisions. If you lease your residence, we may have information about how to reach your landlord and whether landlord permission is required to install our facilities.

Verizon obtains information from outside companies that collect consumer information such as demographic and interest data. Examples of this information include gender, age range, sports enthusiast, frequent diner or pet owner. We use this data and combine it with other information we have about you to help us predict customer preferences and to direct marketing offers that might be more relevant to you.

When you use social media credentials to login to or otherwise interact with a Verizon site or offer, we may collect information about your social media profile, such as your interests, "likes" and friends list. We may use this information, for example, to personalize your Verizon experiences and marketing communications, to enhance our services and to better serve you. You can control this data sharing via options in your social media accounts.

We may also obtain contact information and other marketing lead information from third parties, and may combine it with information we have to contact you or direct Verizon's marketing offers to you. Website visitors and others may provide us with your email address through "refer-a-friend" options or social networking platforms. We use these email addresses to send Verizon promotional marketing information.

Information Collected on Verizon Websites:

When you browse Verizon websites, information is collected about your device and your visit. We also collect data about your browsing, searching and buying activity as you interact with our sites. We may collect and use your IP address, mobile telephone or device number, account information, web addresses of the sites you come from and go to next and information about your connection, including your device's browser, operating system, platform type and Internet connection speed. We use this information for operational and performance measurement purposes including monitoring statistics such as how many people visit our websites; which

pages people visit on our sites; how much time is spent on each page or; which browsers are used to visit our sites.

Verizon and its vendors also use information collected on Verizon websites to help us deliver more relevant Verizon marketing messages. These messages may be delivered on our websites, on non-Verizon websites, by our representatives, via email, or via other Verizon services or devices. We use this information in order to, among other things, ensure that you see the correct products and pricing available in the geographic area in which you live, manage the frequency with which you see an advertisement, tailor advertisements to better match your interests, and to understand the effectiveness of our advertising. We also may use this information to assess the effectiveness of our sites and to help you should you request help with navigation problems on these sites.

Certain Verizon vendors may place and read cookies on our sites to help us deliver Verizon marketing messages on our sites and on non-Verizon sites. We require that these vendors provide consumers with the ability to opt-out of their use of information for these purposes. In accordance with industry self-regulatory principles, you should see this icon in or around Verizon advertisements that are delivered on other sites using information collected on our sites. Clicking on this icon will provide information about the companies and data practices that were used to deliver the ad and will also describe how you may opt-out of these advertising programs. Additional information on the choices available to you for the use of your information for advertising purposes can be found in the "How to Limit the Sharing and Use of Your Information" section below.

Additional information about "cookies" and related technologies

When you register on our sites, we may assign an anonymous, unique identifier. This may allow select advertising entities to use information they have about your web browsing on a desktop computer to deliver marketing messages to mobile devices on our network. We do not share any information that identifies you personally outside of Verizon as part of this program. You have a choice about whether to participate, and you can you can visit our relevant mobile advertising page (link to www.vzw.com/myprivacy) to learn more or advise us of your choice.

Back to Summary

Information You Provide:

When you contact us online or by other means for information about products and services or when you enter a Verizon-sponsored or affiliated contest, sweepstakes or similar promotion, we will respond to your request and may use the information you supply us to provide you with additional information about service offerings either at that time or in the future. If you enter a promotion, your information may be disclosed as part of the program's administration, such as in connection with the publication of winners, prize fulfillment, and as required by law or permitted by the promotion's official rules. Information you provide on our websites about your preferred location and other preferences may be used to provide you with more relevant product recommendations, services and special offers.

If you provide information to us in the context of an event that Verizon sponsors with another organization, such as a contest or sweepstakes, or if you visit a co-sponsored site or use a co-sponsored service, you also may be providing information to the co-sponsor. You should refer to

that co-sponsor's privacy policy for information about its practices which may differ from Verizon's practices.

We may also collect information from you when you agree to participate in surveys or provide other feedback to us regarding our products or services, when you register to receive news or public policy updates, or when you apply for a job with or a grant from Verizon. We use this information only for the purpose for which you provide it.

Verizon may send you emails that communicate information about your account or about products, services, marketing offers, or promotions that may be of interest to you. When you open a Verizon email or click on links within these emails, we may collect and retain information to provide you with future communications that may be more interesting to you. Please note that Verizon will not ask you to send us, via email, sensitive personal or account information.
Back to Summary

Additional Information for Wireless Customers

Verizon Wireless collects and uses mobile device location data for a variety of purposes, including to provide our mobile voice and data services, emergency services, and our and third-party location-based applications and services such as navigation, weather, mapping and child safety applications or tools. Where we offer our own location-based applications, we provide you with notice and choice about whether specific location-tracking features available on your device are turned on.

Many types of wireless applications and services use mobile device location data, including applications provided by other companies and wireless device operating systems. When you are considering new applications or services, you should carefully review the location-based services' or application providers' privacy policies to learn how they collect and use your information.

Verizon Wireless may use mobile usage information and consumer information for certain business and marketing reports. Mobile usage information includes the addresses of websites you visit when you use our wireless services. These data strings (or URLs) may include search terms you have used. Mobile usage information also includes the location of your device and your use of applications and features. Consumer information includes information about your use of Verizon products and services (such as data and calling features, device type, and amount of use) as well as demographic and interest categories provided to us by other companies (such as gender, age range, sports fan, frequent diner, or pet owner). We may combine this information in a manner that does not personally identify you and use it to prepare aggregated business and marketing reports that we may use ourselves or share with others for their use. We may also share location information with other companies in a way that does not personally identify you so that they may produce business and marketing reports. You have a choice about whether your information is included in these reports.

Verizon Wireless does not publish directories of our customers' wireless phone numbers, and we do not provide or make them available to third parties for listing in directories unless you request that we do so.

Back to Summary

Information About the Cable Act

To the extent that Section 631 of the Communications Act of 1934, as amended (the "Cable Act") applies to services you purchase, it entitles you to know about the personally identifiable information a cable service provider collects. This includes the nature of the use and disclosure of this information and to whom it may be disclosed, how long personally identifiable information is maintained, and how subscribers may access it. In addition, the Cable Act imposes limits on the collection and disclosure of personal information and gives subscribers the ability to enforce their privacy rights. (Personally identifiable information does not include aggregate data that does not identify a particular person).

The Cable Act allows a provider to use its cable system to collect personally identifiable information necessary to render a cable service or other services provided to subscribers and to detect and prevent unauthorized access to services. Additional personally identifiable information may be collected with the subscriber's prior consent. Personally identifiable information may be used or disclosed without the subscriber's consent where necessary to render services, and to conduct legitimate business activities related to services provided.

We may be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas, but we will not disclose records revealing your selection of video programming unless we receive a court order indicating that the governmental entity has made a specified showing of relevance and you were afforded an opportunity to contest the order. We may be required to disclose personally identifiable information (including your selection of video programming) to a non-governmental entity to comply with a court order, after you have been provided notice.

If you believe that your privacy rights have been violated, please contact us at privacyoffice@verizon.com and we will work with you to address your concerns. If you believe that you have been aggrieved as a result of a violation of the Cable Act, you may enforce the limitations imposed by the Cable Act through a civil action in a United States district court seeking damages, attorney's fees, and litigation costs. Other rights and remedies may also be available to you under federal or other applicable laws.

The Cable Act permits the disclosure of customer names and addresses as long as a subscriber has been provided with the opportunity to prohibit or limit this disclosure and the disclosure does not reveal, directly or indirectly, the subscriber's viewing or other uses of the cable or other services provided. If we intend to share data in this way, we will provide you with the opportunity to prohibit or limit this type of sharing.

Relevant TV Advertising

Verizon's Relevant TV Advertising program helps advertisers reach FiOS television customers with advertisements that may be more relevant to their interests. We do not share any information that identifies you personally outside of Verizon as part of this program. The ads may appear on a variety of platforms where FiOS television customers can access video content.

We help advertisers deliver ads to audiences based on demographic and interest information (such as gender, family size, and luxury car owner) we obtain from other companies, your address and certain information about your Verizon products and services (such as service packages purchased, video on-demand purchases, and program viewing data). You have a choice about receiving this type of advertising and you can opt out online.

Additional Information for Redbox Instant by Verizon Customers

Redbox Instant by Verizon video streaming services are offered through a joint venture between Verizon and Redbox. When you subscribe to or use Redbox Instant by Verizon services, your information is shared with both Verizon and Redbox and is covered by this privacy policy as well as Redbox's privacy policy.

Redbox Instant by Verizon services will be available to you through websites and Internet-connected device platforms operated by other companies such as gaming devices, streaming video devices, tablets and wireless phones. When you access Redbox Instant by Verizon on others' websites or platforms, you should check these providers' privacy policies to learn what information they collect and use.
Back to Summary.

Information We Share

Information Shared Within the Verizon Family of Companies:

Verizon shares customer information within our family of companies. You can limit our sharing of certain types of customer information, known as Customer Proprietary Network Information, for marketing purposes as described more fully below. Sharing this information allows us to provide you with the latest information about our products and services and to offer you our latest promotions.

Additional protections apply for certain information we collect and maintain about the telecommunications and Voice over Internet Protocol (VoIP) services you buy from us and how you use them. This information is categorized by the federal government as Customer Proprietary Network Information or CPNI. Specific laws govern our sharing and use of this type of information.

Verizon Wireless and Wireline residential customers as well as Verizon Wireline small and medium business customers receive a privacy notice regarding CPNI when they first contract for or order service and atleast every two years thereafter. For more information, please read the Verizon Wireline and Verizon Wireless CPNI notices. You may choose to opt out of the sharing of your CPNI within the Verizon family of companies for certain marketing purposes.

Our corporate and government account customers in the United States receive a CPNI consent form or service agreement requesting affirmative approval to share CPNI information. As described in the request, you may decline or withdraw CPNI consent by not signing the consent

form or by following instructions in the consent form or service agreement. Your choice on CPNI consent will remain in effect unless you change it.

If you are an Arizona resident, as required by state law, Verizon Wireless does not share your CPNI within the Verizon family of companies unless you provide consent. Customers who provide such consent are reminded annually of their current CPNI choices.

If you are a retail customer of MCI, your CPNI will not be shared within the Verizon family of companies for marketing purposes except to provide you with information about other services of the type you currently buy from us. In addition, when you are speaking with a customer service representative, we may ask your permission to review your records, including your CPNI, to provide you with information about the full array of services provided by the Verizon family of companies.

Information Shared Outside the Verizon Family of Companies:

Except as explained in this Privacy Policy, in privacy policies for specific services, or in agreements with our customers, Verizon does not sell, license or share information that individually identifies our customers, people using our networks, or website visitors with others outside the Verizon family of companies for non-Verizon purposes without the consent of the person whose information will be shared.

Verizon uses vendors and partners for a variety of business purposes such as to help us offer, provide, repair and bill for services we provide. We share information with those vendors and partners when it is necessary for them to perform work on our behalf. For example, we may provide your credit card information and billing address to our payment processing company solely for the purpose of processing payment for a transaction you have requested. We require that these vendors and partners protect the customer information we provide to them and limit their use of Verizon customer data to the purposes for which it was provided. We do not permit these types of vendors and partners to use this information for their own marketing purposes.

As described in more detail in other sections of this policy, Verizon also may share certain information with outside companies-, for example, to assist with the delivery of advertising campaigns, or preparing and sharing aggregate reports.

Verizon provides the names, addresses and telephone numbers of wireline telephone customers to directory publishers and directory assistance services unless a non-published or non-listed phone number has been requested.

We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as:

- to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law;
- in cases involving danger of death or serious physical injury to any person or other emergencies;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of or

subscription to our products and services and to protect our network, services, devices and users from such use;
- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to credit bureaus or collection agencies for reporting purposes or to obtain payment for Verizon-billed products and services;
- to a third-party that you have authorized to verify your account information;
- to outside auditors and regulators; or
- with your consent.

When you purchase services offered jointly by Verizon and one of our partners, customer information may be received by both Verizon and our partner that is providing your service. For these jointly offered services, you should also review the partner company's privacy policy which may include practices that are different from the practices described here.

If Verizon enters into a merger, acquisition or sale of all or a portion of its assets or business, customer information will also be transferred as part of or in connection with the transaction.

Information Provided to or Used by Third-Party Advertising Entities or Social Networks

You may see third-party advertisements on some Verizon websites, services, or devices. Some advertisements are chosen by companies that place advertisements on behalf of other third-party advertisers. These companies, often called ad servers, ad networks, or technology platforms, may place and access cookies on your device to collect information about your visit on our websites. The information they collect from our sites is in a form that does not identify you personally. This information may be combined with similar data obtained from other websites to help advertisers better reach their targeted audiences. Targeting may be accomplished by tailoring advertising to interests that they infer from your browsing of our sites and your interaction with other websites where these ad servers, ad networks and technology platforms also are present.

If you choose to interact with specific advertisers who advertise on our sites or services, the information you provide to them is subject to the conditions of their specific privacy policies. In addition, responding to or interacting with a particular advertisement, may result in you later receiving a targeted advertisement on our websites or on other sites as a result of an ad server or ad network concluding that you fit within a particular audience an advertiser is trying to reach.

Advertising that is customized based on predictions generated from your visits over time and across different websites is sometimes called "online behavioral" or "interest-based" advertising. In accordance with industry self-regulatory principles, we require that companies disclose when they are using online behavioral advertising programs to deliver third-party ads on our sites or collecting information about your visit to our sites for these purposes and give consumers the ability to opt-out of this use of their information. You will see an icon in or around third-party advertisements that are delivered on our sites using behavioral advertising programs. Clicking on this icon will provide additional information about the companies and data practices that were used to deliver the ad as well as information on how you may opt-out of these advertising programs. Additional information about your options regarding the use of your information for advertising purposes can be found below. Additional information about online behavioral advertising can be found here. Please note that Verizon does not have control over or access to

information contained in the cookies that are set on your computer by ad servers, ad networks or third-party advertisers.
Additional information about "cookies" and related technologies

We also may provide third-party advertisers with geographic or demographic information that allows them to tailor their ads. This information does not identify you individually.

Verizon also helps advertisers better reach our wireline and wireless Internet access customers using the postal address we have for you; certain information about your Verizon products and services-- such as device type and broadband service features; and demographic and interest information provided to us by other companies-- such as gender, age-range, sports fan, frequent diner or pet owner. This information is used to predict whether you fit within an audience an advertiser is trying to reach. In addition, using an anonymous, unique identifier we create when you register on our websites, we may allow an advertiser to use information they have about your visits to websites on a desktop computer to deliver marketing messages to mobile devices on our network. We do not share outside of Verizon any information that identifies you personally as part of these programs. You have a choice about participating in the separate Verizon and Verizon Wireless programs.

Verizon websites and services may include social network or other third-party plug-ins and widgets that may provide information to their associated social networks or third-parties about your interactions with Verizon page you visit or services you use, even if you do not click on or otherwise interact with the plug-in or widget. More information is available here.
Back to Summary

How to Limit the Sharing and Use of Your Information

You have choices about how Verizon shares and uses information.

Customer Proprietary Network Information (CPNI):

As described above, customers of Verizon telecommunication and VoIP services may choose whether to allow Verizon to share your CPNI within the Verizon family of companies for certain marketing purposes. This choice will remain in effect unless you change it. Verizon Wireline consumer and small business customers may opt-out of this sharing by calling us using the state toll-free number provided in their notice and available here. Verizon Wireless mass-market customers may call 1-800-333-9956. National and major account customers of Verizon Wireless and corporate and government customers of Verizon Wireless or Verizon Business in the United States may decline to provide or withdraw CPNI consent by following the instructions in your service agreements or CPNI consent forms.

Telemarketing:

Federal "Do Not Call" laws allow you to place your phone numbers on the National Do Not Call Registry to prevent telemarketing calls to those numbers. If you would like to add your numbers to this list, you may do so by calling 1-888-382-1222, or by visiting www.donotcall.gov.

You should be aware that even if you add your number(s) to the federal or a state Do Not Call list, most telemarketing laws allow companies to contact their own customers. If at any time you would like to be removed from Verizon's residential telemarketing list, please let us know by contacting a Verizon customer service representative at 1-800-VERIZON. Verizon Wireless also maintains a Do Not Call list. If you would like to be removed from the Verizon Wireless telemarketing list, please let us know by contacting a Verizon Wireless customer service representative at 1-800-922-0204. Please allow 30 days for your telephone number to be removed from any sales programs that are currently underway.

Marketing Email, Text Messages, Postal Mail and Door-to-Door Calls:

Marketing emails you receive from Verizon, Verizon Wireless, or Redbox Instant by Verizon include an unsubscribe instruction (usually found at the bottom of the email) that you may use to opt out of receiving future marketing-related emails. You may opt out of receiving marketing-related emails from Verizon by visiting our "Unsubscribe" site and providing the requested information. You may opt out of receiving marketing-related emails from Verizon Wireless by contacting a Verizon Wireless customer service representative at 1-800-922-0204. You may opt-out of receiving marketing-related emails from Redbox Instant by Verizon at your customer account pages online.

You may opt out of receiving marketing-related postal mailings or prevent door-to-door marketing solicitations from Verizon by calling a customer service representative at 1-800-VERIZON. You may opt out of receiving marketing-related postal mailing or prevent text message marketing by Verizon Wireless by calling a Verizon Wireless customer service representative at 1-800-922-0204. Text message solicitations from Verizon also contain an "unsubscribe" feature that you can use to prevent future marketing text messages from us. Please note that Verizon may use bulk mail service for some marketing mailings. These services deliver offers to all homes in a neighborhood or zip code. This type of mailing will continue even if you opt-out of receiving marketing-related postal mailings from Verizon.

Information Used for Online Advertising:

You have choices about whether certain information collected on websites, including Verizon's, is used to customize advertising based on predictions generated from your visits over time and across different websites. When you see this icon  in or around an advertisement you can click on the icon to see additional information on the companies and data practices that were used to deliver the ad and descriptions of how you may opt-out of these advertising programs. To learn more or to limit the collection of information by these parties, you may also visit the Aboutads.info website.

Please note that many opt-outs are cookie-based. If you buy a new computer, change web browsers or delete the cookies on your computer, you will need to opt-out again. Please also note that some wireless devices, portals and websites have limited ability to use and store cookies. As a result, advertising entities may have a limited ability to use cookies in the manner described above or to respect cookie-based opt out preferences. However, ads may still be tailored using other techniques such as publisher, device or browser-enabled targeting. You should check the privacy policies of the products, sites and services you use to learn more about any such techniques and your options. If you do not want information to be collected for marketing

purposes from services such as the Verizon Wireless Mobile Internet services, you should not use those particular services.

You also can limit the collection of certain website information by deleting or disabling cookies. Most computers' Internet browsers enable you to erase cookies from your computer hard drive, block all cookies, or receive a warning before a cookie is stored.
See information about managing cookies

Please note that disabling cookies may prevent you from using specific features on our sites and other websites, such as ordering products or services and maintaining an online account. Cookies must be enabled for you to use your Verizon e-mail account.

Relevant Advertising

Verizon broadband Internet access customers may opt-out of the relevant online advertising program described above by following the instructions here. Verizon Wireless Internet customers may opt-out of the relevant mobile advertising program by following the instructions here or by calling us at 1-866-211-0874. You may opt-out of Verizon's Relevant TV advertising program by following the instructions here. If you opt out online, you will need your account user ID and password. Also, please note that you will receive ads whether you participate in these programs or not, but under these programs, ads may be more relevant to you.

Business and Marketing Reports

Verizon Wireless customers may choose not to participate in Verizon Wireless' use of their information to create aggregated business and marketing reports that do not specifically identify any individual Verizon Wireless customers. You may opt-out by calling 1-866-211-0874 or by visiting verizonwireless.com/myprivacy. Please note that if you have a Family SharePlan® or multi-line account, you must indicate your opt-out choice for each line. If you add a line or change a telephone number, you will need to update your privacy choices.
Back to Summary

Working Together to Keep Children Safe

Verizon recognizes that online service providers must be vigilant in protecting the safety and privacy of children online. We do not knowingly market to or solicit information from children under the age of 13, without obtaining verifiable parental consent.

Verizon strongly supports educating parents and young Internet users on safe viewing practices and we offer a variety of tools to help children and parents avoid encountering objectionable content or communications while using our services.

Verizon's Parental Control Center provides many free resources that offer guidance, connect parents with experts and help give parents the technical knowledge to help keep kids safer online.

Regrettably, there are those who use the Internet to view, store and distribute child pornography

(or who engage in other types of illegal activity involving children). Child pornography is subject to severe criminal penalties and using the Verizon network to view, store or distribute it violates our service contracts. The Verizon network may not be used by customers in any manner for the storage, transmission or dissemination of images containing child pornography and we will report any instances of such activity of which we become aware to the appropriate law enforcement authorities.

If you have a complaint about child pornography, the soliciting of children for sexual activity, or any other illegal or inappropriate activity involving children on a Verizon service, report it to us by sending an email to abuse@verizon.net. Please include the words "child porn" in the subject line of your email. You can also make a report directly to the National Center for Missing and Exploited Children through its CyberTipline located at www.cybertipline.org.

Additional Internet safety resources and information are available at:

- http://www.netsmartz.org/
- http://www.wiredsafety.org/
- http://www.onguardonline.gov/
- http://www.commonsensemedia.org/
- http://www.stopbullying.gov/
- http://www.cyberbullying.us/
- http://www.connectsafely.org/

Back to Summary

Information Security and Data Retention

Verizon has technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we collect or store, including Social Security Numbers. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our practices and policies, access to sensitive personally identifiable information is authorized only for those who have a business need for such access. Personally identifiable and other sensitive records are retained only as long as reasonably necessary for business accounting, tax or legal purposes.

Although we work hard to protect personal information that we collect and store, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose personal information. Verizon maintains security and incident response plans to handle incidents involving unauthorized access to private information we collect or store.

If you become aware of a security issue, please contact Verizon's Security Control Center. We

will work with you to address any problems.

Verizon often publishes helpful information about a wide range of scams that you may encounter.

View current information about Internet and phone scams and tips on how to protect yourself

Back to Summary

Contact Information

If you have questions, concerns or suggestions related to our Privacy Policy or our privacy practices you may contact us at:

Verizon Privacy Office
1300 I Street, NW
Suite 400 West
Washington, DC 20005
Fax: 202-789-1432
Email: privacyoffice@verizon.com

Accessing and Updating Your Information

We strive to keep our customer records as accurate as possible. You may correct or update your Verizon customer information by calling a Verizon customer service representative at 1-800-VERIZON or by accessing your account online and providing the updated information there. Similarly, updates can be made to your Verizon Wireless account by calling a Verizon Wireless customer service representative at 1-800-922-0204 or online. Verizon Business customers may update their information by contacting their account manager. Updates can be made to your Redbox Instant by Verizon account information by visiting the "My Account" pages online.

If you are a FiOS or other customer served over our fiber-to-the-premises network and you would like to see your personally identifiable information, please contact us at privacyoffice@verizon.com so we may arrange a time and convenient location for you to do so during business hours. You will need to provide proper identification and you may examine records that contain personally identifiable information about you and no one else. If you believe any of your personally identifiable information is inaccurate, we will work with you to ensure that corrections are made. Verizon reserves the right to charge you for the cost of photocopying any documents you request.

Links to and from non-Verizon Websites and Content

Verizon websites and Redbox Instant by Verizon platforms may contain links to non-Verizon sites. Verizon applications or other content may be included on web pages and web sites that are not associated with Verizon and over which we have no control. We are not responsible for the content on these sites or platforms or the privacy policies and practices employed by these sites

and platforms. We recommend that you review the policies and practices of the sites you visit.

Information Sharing: Blogs and Social Networking

Some Verizon websites, applications, and services may allow you to participate in web log ("blog") discussions, message boards, chat rooms, and other forms of social networking and to post reviews. Please be aware that these forums are accessible to others. We urge you to not submit any personally identifiable information to these forums because any information you post can be read, collected, shared, or otherwise used by anyone who accesses the forum. Verizon is not responsible for the information you choose to submit in these forums. If you post content to information sharing forums, including any information about the movies you rent or view, you are doing so by choice and you are providing consent to the disclosure of this information.

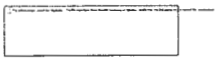
Changes to This Policy

We reserve the right to make changes to this Privacy Policy, so please check back periodically for changes. You will be able to see that changes have been made by checking to see the effective date posted at the end of the policy.

If Verizon elects to use or disclose information that identifies you as an individual in a manner that is materially different from that stated in our policy at the time we collected that information from you, we will give you a choice regarding such use or disclosure by appropriate means, which may include use of an opt-out mechanism.

Updated January 2014

© 2009, 2011-2014 Verizon. All Rights Reserved.









- Home
- Our Company
- Innovative Solutions
- Corporate Responsibility
- News Center
- Investors
- Careers

- Privacy Policy
- Terms & Conditions

© 2013 Verizon

EXHIBIT 6

AT&T Privacy Policy

About Our Privacy Policy

Whenever you do something like buy one of our products, stream a movie or download an app, information is created. Because we know your privacy is important, we have a Privacy Policy to explain how we collect, use and protect that information. There's a quick summary below, and the entire policy is written in an easy FAQ format. We want to simplify this, so you can make informed choices about your privacy, and then spend the rest of your time enjoying our products and services.

Effective September 16, 2013

A Quick Summary of Our Privacy Policy

Our privacy policy applies to your use of our products and services. We will always provide you with notice of material changes to this Policy. In order to do things like constantly improve our services, products and relationship with you, we may collect different types of information that help us learn more about how you use our offerings.

Here's some of the information we collect:

- ***Account Information*** includes your name, address, telephone number, e-mail address, service-related details such as payment data, security codes, service history and other information like that;
- ***Network Performance & Usage Information*** tells us how you use our network, our products and our services, and how well our equipment and network is performing;
- ***Web Browsing & Wireless Application Information*** tells us about the websites you visit and the mobile applications you use on our network;
- ***Location Information*** tells us where your wireless device is located, as well as your ZIP-code and street address;
- ***U-verse Information*** tells us about which programs you watch and record, the games you play, the applications you use and similar information about how you use our U-verse services and applications.

Here are the three basic ways we collect it:

- We get information from you when you do things like make a purchase from us;
- We collect it from how you use our products and services;
- Other sources, like credit agencies and marketing companies, provide it to us.

Here are just some of the ways we use it. To:

- Provide services and improve your customer experience;
- Send you bills for your services;
- Respond to your questions;
- Address network integrity and security issues;
- Do research and analysis to maintain, protect, develop and improve our network;
- Let you know about service updates, offers and promotions;
- Improve entertainment options;

- Deliver Relevant Advertising;
- Create External Marketing & Analytics Reports;
- Assist in the prevention and investigation of illegal activities and violations of our Terms of Service or Acceptable Use Policies.

Some examples of who we share your Personal Information with:

- **Across AT&T companies** to give you the best customer experience and to help you get everything we have to offer.
- **With other companies that perform services on our behalf** only as needed for them to perform those services. We require them to protect your information consistent with our Policy.
- **With other companies and entities, to**:
  - Respond to 911 requests and other emergencies or exigencies;
  - Comply with court orders and other legal process;
  - Assist with identity verification, and preventing fraud and identity theft;
  - Enforce our agreements and property rights; and
  - Obtain payment for products and services including the transfer or sale of delinquent accounts to third parties for collection

Details on Personal and Anonymous & Aggregate Information

- What is Personal Information? Information that identifies or reasonably can be used to identify you.
- What is Anonymous? This is information that doesn't identify you and can't reasonably be used to identify you specifically.
- What is Aggregate? We take a whole bunch of people's data and combine it into anonymous groups or categories.
- How we use this information? We use and share this information in many ways including research, media analysis and retail marketing and Relevant Advertising. This data is also included in External Marketing &Analytics Reports
- Want to learn more? Go here.

Our privacy commitments

- We don't sell your Personal Information to anyone for any purpose. Period.
- We keep your Personal Information in our business records while you are a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.

Our Online Privacy Policy for Children

- We want you to know that we don't knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.
- For information about safety and controls, view our AT&T Smart Controls parental tools.

Your Choices & Controls

- You have choices about which types of advertising you get from us;
- You can control whether your anonymous information is used in our External Marketing & Analytics Reports;
- You can choose whether to receive marketing calls, e-mails or text messages from us;
- You have a choice about how we use your Customer Proprietary Network Information;

Visit our Privacy Policy for more information.

- Definitions
- Scope of this Policy
- The Information We Collect, How We Collect It, And How We Use It
- Information Sharing
- Online Activity Tracking and Advertising
- Location Information
- Aggregate and Anonymous Information
- External Marketing & Analytics Reports
- Online Privacy Policy for Children
- Data Protection & Security
- Changes
- Choices & Controls
- How to Contact Us

Your California Privacy Rights

California Civil Code Section 1798.83 entitles California customers to request information concerning whether a business has disclosed Personal Information to any third parties for their direct marketing purposes. As stated in this Privacy Policy, we will not sell your Personal Information to other companies and we will not share it with other companies for them to use for their own marketing purposes without your consent.

California Web Site Data Collection & "Do Not Track" Notices

Web Site Data Collection: We do not knowingly allow other parties to collect personally identifiable information about your online activities over time and across third-party web sites when you use our websites and services. AT&T provides information about the opt-out choices it makes available, and the opt-outs choices provided by certain third-party website and mobile application analytics companies we use here.

"Do Not Track" Notice: Because the providers of "do not track" and similar signals do not yet operate according to common, industry-accepted standards, AT&T currently does not respond to those signals. For more information on Do Not Track, please visit www.allaboutdnt.com.

California customers who wish to request further information about our compliance with these requirements, or have questions or concerns about our privacy practices and policies may contact us at privacypolicy@att.com, or write to us at AT&T Privacy Policy, 1120 20th Street, N.W., 10th Floor, Washington, DC 20036.

AT&T Privacy Policy FAQ

Our AT&T Privacy Policy in easy, FAQ format.

We understand that everyone thinks that privacy policies are long, complicated and difficult to understand. So we're going to try to make this as simple as possible.

DEFINITIONS

Let's start with what we mean when we say:

Aggregate Information: Information that we combine into anonymous groups of customers or users. One way to think of it is in terms of a survey or opinion poll. Aggregate information would tell you that 80 percent of the people voted for a candidate, but not who actually voted. These groups are large enough to reasonably prevent individuals from being identified.

Anonymous Information: Information that doesn't directly identify and can't reasonably be used to identify an individual customer or user.

Customer: Anyone who purchases or uses our products or services. When a customer purchases retail products or services for use by others, like a family account, those family members also are customers.

Mobile Application: A software application that runs on smartphones, tablet computers or other mobile devices and that allows users to access a variety of services and information.

Personal Information: Information that directly identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address. Personal Information does not include published listing information.

Relevant Advertising: Uses aggregate information about groups of people (like age, ethnicity, income range, where those groups live and work, and their interests) to develop advertising that is more likely to be useful to that group. It does not use individual data about what a specific person might like. "Online behavioral advertising" is one type of relevant advertising. It uses interest categories based on the websites visited by groups of people to deliver advertising online.

User: Anyone who visits our websites or uses our mobile applications.

Website: And other terms like "Internet site," "site" and "web page" all mean the same thing, namely any page or location on the Internet, no matter what device (cell phone, tablet, laptop, PC, etc.) or protocol (http, WAP, ftp or other) is used to access the page or location.

QUESTIONS ABOUT THE SCOPE OF THIS POLICY

1. What does this Policy cover?

This Privacy Policy covers our practices regarding the information we collect about our customers and users (how we collect it and how we use it). Use of our products and services, as well as visits to our websites, are subject to this Privacy Policy.

2. Do you have any Privacy Policies other than this one?

   Yes. The Joint AT&T EchoStar Privacy Policy for AT&T|DISH Network Customer Account Information remains in effect for AT&T|DISH subscribers.

   AT&T companies that do not operate under our brand may have separate privacy policies.

   Some areas outside the United States require us to work a little differently. In that case, AT&T may adopt separate privacy policies as necessary to reflect the requirements of applicable local laws.

3. What about my family members and other users of my AT&T account? Does this Policy apply to them?

   Yes. You're responsible for making sure all family members or other users under your account understand and agree to this Policy. Get everyone together and talk about it. Or, send it by e-mail to make sure they're on board. Hang it on the fridge. Up to you, just share it!

4. When is information not covered by this Policy?

   Any time you give information to companies other than AT&T. Some examples are:

   - When you use a non-AT&T Wi-Fi service;
   - When you download applications or make purchases from other companies while using our Internet or wireless services;
   - When you go to a non-AT&T website from one of our websites or applications (by clicking on a link or an advertisement, for example);
   - If you use public forums - such as social networking services, Internet bulletin boards, chat rooms, or blogs - the information is publicly available, and we cannot prevent distribution and use of that information by other parties;
   - Information about your location, usage and the numbers you dial when you're out and about and roaming on the network of another company;
   - When you purchase or use non-AT&T products (such as wireless devices, internet browsers and mobile applications) in combination with AT&T services;
   - When we license our brand to other companies for their use in marketing and selling certain non-AT&T products and services, information you give those companies is not covered by this Policy.

5. Can my information be covered by this policy and other privacy policies at the same time?

   Yes, that can happen. For example:

   Sometimes we will provide a service with other companies. In that case your information may be subject to this Policy and that of the other companies. For example, if you use AT&T High Speed Internet services "powered by" Yahoo! Inc., your information may be covered by both this Policy and the Yahoo! Privacy Policy.

   If you purchase one of our products or services from a retailer like Best Buy or Amazon.com, for example, any information you provide to them may be subject to both their policy and ours.

   If you connect to our Wi-Fi service through another network, such as one provided in a hotel, airport or other venue, any information collected from your use of that network could be subject to either the AT&T policy or the venue policy, and sometimes both. The same thing applies if you connect to our network through your employer's corporate network, or any network operated by a non-AT&T company.

   We think it's a great idea to take a look at the privacy policies of any companies you do business with to learn how they use your information.

6. What about business customers?

   We have written product or service agreements with our business customers that contain specific provisions about confidentiality, security or handling of information. When one of these agreements differs from or conflicts with this Policy, the terms of those agreements will apply. In all other instances, the terms of this Policy apply.

QUESTIONS ABOUT THE INFORMATION WE COLLECT, HOW WE COLLECT IT AND HOW WE USE IT

1. What information do we collect?

   We may collect different types of information based on your use of our products and services and on our business relationship with you.

   - **Account Information:**

     - **Contact Information** that allows us to communicate with you. We get this information when you order or register for our services. This would include information like your name, address, telephone number and e-mail address.

     - **Billing Information** related to your financial relationship with us, such as the services we provide to you, the telephone numbers you call and text, your payment history, your credit history, your credit card numbers, Social Security number, security codes and your service history.

- **Technical & Usage Information** related to the services we provide to you, including information about how you use our network, services, products or websites. Some examples include:
    - **Equipment Information** that identifies your equipment on our network, such as equipment type, device IDs, device status, serial numbers, settings, configuration and software.
    - **Network Performance & Usage Information** about the operation of the equipment, services and applications you use on our network. Examples of this might include wireless device location, the number of text messages sent and received, voice minutes used, bandwidth used, and resources you use when uploading, downloading or streaming data to and from the Internet. We also collect information like transmission rates and delays, data associated with remote monitoring services and security characteristics.
        - Some Network Performance & Usage Information and some Billing Information is **Customer Proprietary Network Information or "CPNI."** Unique rules apply to CPNI. Go here to learn more about what it is, how we use it and the choice you can make about that use.
    - **Web Browsing & Mobile Application Information** such as IP addresses, URLs, data transmission rates and delays. We also learn about the pages you visit, the time you spend, the links or advertisements you see and follow, the search terms you enter, how often you open an application, how long you spend using the app and other similar information.
- **Location Information** includes your ZIP-code and street address, as well as the whereabouts of your wireless device. Location information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System.
- **U-verse Information** is generated when you use our U-verse suite of services including TV, On Demand, Total Home DVR®, High Speed Internet Service, Online, U-verse App for tablet or smartphone and similar AT&T services and products, including the programs and channels you and those in your household watch and record, the times you watch and how long you watch. It also includes information like the games you play and the applications you use. We also collect information related to your use and interaction with the U-verse equipment in your home, including the U-verse TV remote and Set Top Box.

2. How Do You Collect Information?

In three basic ways:

- **You Give It To Us** when you make a purchase or set up an account with us;
- **We Automatically Collect Information** when you use our network, products and services. For example, we use network tools to collect your call records; we collect wireless device location from our network and from your device; and we also use cookies, web server logs and other technologies.
- **We Obtain Information from Outside Sources** like credit reports, marketing mailing lists, and commercially available geographic and demographic information.

3. How Do You Use My Information?

   We use your information to improve your experience and to make our business stronger. Some examples include:

   - Providing and managing your services, responding to your questions and addressing problems;
   - Delivering customized content, Relevant Advertising and personalized offers for products and services that may be of interest to you;
   - Communicating service updates, offers and promotions;
   - Protecting network integrity and security, ensuring quality control, optimizing capacity and preventing misuse;
   - Network enhancement planning, engineering and technical support;
   - Conducting research and analysis for maintaining, protecting and developing our network and our services;
   - Preventing illegal activities, suspected fraud, and potential threats to our network and our customers' networks;
   - Investigating violations of our Terms of Service, Acceptable Use Policies, or other service conditions or restrictions; and
   - Protecting the safety of any person.

4. Do you use the information I store using one of your cloud services?

   We only use it to provide you with that service, unless we first get your permission to use it for something different.

QUESTIONS ABOUT INFORMATION SHARING

1. Do you provide information for phone books and Caller ID?

   Yes and No.

Yes, we share the names, addresses and telephone numbers of our wireline telephone and U-verse Voice customers with businesses that publish directories and provide directory assistance services. We are required by law to do that. We honor your request for non-published or non-listed phone numbers. Once we provide published listing information to those businesses, they may use, sort, package, repackage and make it available again in different formats to anyone. We also provide calling name and number information for Caller ID.

No, we do not give listing information for wireless numbers to phone book publishers or directory assistance services without your permission.

2. Do you share my Personal Information internally?

   Yes. Our products and services are developed, managed, marketed and sold by a variety of AT&T companies. Sharing this information helps us offer you the high quality, seamless and innovative range of products you have come to expect from us. Some of these include:

   - Wireless voice, data, Internet, home security, automation and remote monitoring services provided by AT&T Mobility and AT&T Digital Life; and
   - The U-verse suite of TV, Voice and High Speed Internet Access services offered by the AT&T telephone companies.

   If one of our subsidiaries does not operate under the AT&T brand, information sharing with that subsidiary is handled as though it is a non-AT&T company.

3. Do you share my Personal Information with other companies for them to market to me?

   We will only share your Personal Information with other companies for them to use for the marketing of their own products and services when we have your consent.

4. Are there any other times when you might provide my Personal Information to other companies or entities?

   Yes. We share your Personal Information with companies that perform services for us, like processing your bill. Because we take our responsibility to safeguard your Personal Information seriously, we do not allow those companies to use it for any purpose other than to perform those services, and we require them to protect it in a way consistent with this Policy.

   Companies that perform these services may be located outside the United States. If your Personal Information is shared with these companies, it could be accessible to government authorities according to the laws that govern those countries.

   There are also occasions when we provide Personal Information to other companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to:

- Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims;
- Obtain payment or make refunds for products and services that appear on your AT&T billing statements, including the transfer or sale of delinquent accounts or refund obligations to third parties for collection or payment;
- Enforce our agreements and protect our rights or property,
- Assist with identity verification and e-mail address validation;
- Notify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury; and
- Notify the National Center for Missing and Exploited Children of information concerning child pornography of which we become aware through the provision of our services.

5. Do you share my personally identifiable U-verse TV viewing information with other companies?

   We don't share your personally identifiable U-verse TV information with other companies for them to use for the marketing of their own products and services without your consent. We are required to notify you about the special requirements we must follow when it comes to sharing your personally identifiable U-verse TV information in response to a Court Order:

   Notice Regarding Disclosure of Personally Identifiable Information of AT&T U-verse TV Subscribers in Response to Court Order

   - In the case of a court order obtained by a non-governmental entity, AT&T is authorized to disclose personally identifiable information collected from AT&T U-verse TV subscribers as a result of the subscriber's use of AT&T's U-verse TV service only after providing prior notice to the subscriber.
   - In the case of a court order obtained by a governmental entity, AT&T is authorized to disclose personally identifiable information collected from AT&T U-verse TV subscribers as a result of the subscriber's use of AT&T's U-verse TV service only if, in the court proceeding relevant to the order:
     - The governmental entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
     - The subject of the information has an opportunity to appear and contest the governmental entity's claim; and

- We have provided notice to the subscriber as required by applicable state law.

QUESTIONS ABOUT MY INFORMATION & ADVERTISING

1. Do you use my information to send me advertising?

   Yes. We may use information like the preferences you have expressed and interests you have demonstrated on our websites, in our stores and through use of our products and services, to provide you with marketing information and advertisements for AT&T products and services. Those ads may be delivered on our websites and mobile applications. This is called "first party" advertising. It is part of our service relationship and you are not able to opt-out from this type of advertising.

   Our advertising affiliate, AT&T AdWorks, and our advertising partners may also use anonymous information gathered through cookies and similar technologies, as well as other anonymous and aggregate information that either of us may have to help us tailor the ads you see on non-AT&T sites. For example, if you see an ad from us on a non-AT&T sports-related website, you may later receive an ad for sporting equipment delivered by us on a different website. This is called "online behavioral advertising," which is a type of Relevant Advertising.

2. Do you use my information for other types of Relevant Advertising?

   Yes. AT&T AdWorks also uses information we get through your use of our products and services, from our advertising partners, and information like your age and gender to deliver Relevant Advertising that is not online behavioral advertising. We combine your anonymous information with that of other users into aggregate "audience segments." These segments are based on particular interests and/or factual characteristics that everyone in that audience segment is likely to share. We might use that information to send you advertisements that are relevant to those interests or characteristics.

   We are careful to create Relevant Advertising with aggregate audience segments that are large enough that you can't be identified individually.

3. Do you use the location of my device for advertising purposes?

   Yes. AT&T AdWorks uses information about the locations you visit in order to create combined wireless location interest characteristics that can be used to provide Relevant Advertising to you and others like you.

   Location characteristics are types of locations - like "movie theaters." People who live in a particular geographic area (a city, ZIP-code or ZIP+ 4 code, for example) might appear to have a high interest in movies, thanks to collective information that shows wireless devices from that area are often located in the vicinity of movie theaters. We might create a "movies characteristic" for that area, and deliver movie ads to the people who live there.

   We may associate your wireless device with a particular geographic area, such as a city, ZIP-code, or ZIP + 4 code, based on your billing address or the cell towers you

connect with most frequently. AT&T AdWorks does not keep a record of the places you have visited.

In addition to other privacy protections, the process we use to create our audience segment includes a requirement that the ZIP + 4 or other geographic area to which a wireless location is assigned must contain a minimum of 25 households. ZIP + 4 codes with less than 25 households are combined with other ZIP + 4 codes to satisfy this requirement.

4. What's in it for me?

   Just like the name says, you get advertising that's more relevant to your interests. For example, if a particular audience segment, like adults between the ages of 21 and 25 with a certain income range, has demonstrated a greater interest in movies than other segments, we might send them a movie ad for a movie geared toward young adults.This is just one way we deliver content that's more relevant.

5. How do you use information about the programs I watch on U-verse TV to advertise to me?

   We combine information about the shows that our customers are watching with their common interests to help us figure out what types of advertising they might be interested in seeing.

   It sometimes works like this: We look at the group of people watching a particular show. We identify common characteristics within that group. We use those characteristics to identify and deliver advertising that might be most relevant to watchers of that TV show. We might also deliver that same advertising during shows that appear to have similar audiences.

6. Do I ever have a chance to tell you what I'm personally interested in?

   Yes. With AT&T Alerts you can sign up to receive text-message offers from businesses that are near your current location and match the interests you've selected. Check it out at http://alerts.att.com/join. You can change your mind at any time and stop receiving alerts.

   When we add new offers like AT&T Alerts we'll let you know, so you can decide if you'd like to participate. For example, we may offer you free or discounted services in exchange for the use of your Personal Information for advertising and other similar purposes. We promise, before we use any of your Personal Information (including information we gather as an Internet service provider) for such purposes, we will always give you the opportunity to make an informed choice about whether to participate

7. What information do you provide to advertisers?

   AT&T may provide reports to advertisers and other business customers about the success of its advertising campaigns. Those reports contain aggregate information about the number of times a particular ad was viewed, when it was viewed, whether it was viewed on a TV, a mobile device or a computer, demographics associated with

the viewing audience and other similar information. Your anonymous information will not be included in aggregate reports about the success of Relevant Advertising campaigns if you have opted-out of Relevant Advertising delivered by AT&T AdWorks.

QUESTIONS ABOUT LOCATION INFORMATION

1. What is location information?

   Exactly what it sounds like! It includes your ZIP-code and street address, as well as the whereabouts of your wireless device.

2. How is it used?

   We use it in all kinds of ways, here are some examples:

   - **We Provide Wireless Voice and Data Services**: We monitor, collect and use wireless location information, together with other information we get from our network and your wireless device, to maintain and improve our network. We also might use location information with your consent to provide you with a customized experience. For example, when you dial 411 Directory Assistance for a business telephone number, we might use your wireless location information to return the number of the business location closest to you.

   - **Location Based Services (LBS):** Your device can be used to access a ton of services based on location. We offer these services via applications that have been pre-loaded or downloaded by you on your device. LBS also may be provided via text message or other functionality. We'll give you prior notice and ask for your consent when your location is used or shared. The form of consent may vary, but will be appropriate for the type of AT&T LBS you use.

   - **LBS from other providers**: With your consent (to us or the other company) we also may enable LBS from other companies by providing location information to their developers or location service providers.

   - We use it for **Advertising**.

3. How accurate is wireless location information?

   It depends on the technology we're using. For example, we can locate your device based on the cell tower that's serving you. The range could be up to 1,000 meters in any direction from the tower in urban areas, and up to 10,000 meters in rural areas. Wi-Fi networks provide more accurate location information, associating you with the place where the network is located - like a coffee shop - or to an area within or around that place.

   Services such as 411, 911, a "friend locator" application or a navigation/mapping application, require more precise information. So for those we develop a more precise estimate of location by associating the serving cell tower ID with other information, like the latitude and longitude of the tower, radio frequency parameters, GPS information and timing differences in radio signals. Depending on a variety of

factors, those methods may estimate the location of your device to within 30 to 1000 meters.

4. Are you the only ones who can locate my wireless device?

   Other companies may also be able to locate your device. For example, your handset manufacturer and your operating system provider may be able to locate your device. If you download mobile applications, those apps may be able to obtain your location directly from your handset or the operating system. Mobile applications that give you access to your employer's network may also give your employer the ability to locate your device.

   We urge you to review Policies of all providers.

QUESTIONS ABOUT AGGREGATE AND ANONYMOUS INFORMATION

1. Where do you get anonymous information?

   Sometimes we'll collect information about how you use our products using cookies and other similar technologies. This information doesn't include your Personal Information and is considered anonymous.

   When we collect information that identifies you personally, we may anonymize it for certain purposes. We remove data fields (such as name, address and telephone number) that can reasonably be used to identify you. We also use a variety of statistical techniques and operational controls to anonymize data. Anonymizing information is one of the tools we use to protect your privacy.

2. Tell me more about aggregate information.

   Aggregate information is a form of anonymous information. We combine data that meet certain criteria into anonymous groups. For example, we might want to compare how customers in Beverly Hills, CA (or any city, county or ZIP-code) use their cell phones to how customers in Boulder, CO use their cell phones. In order to do that, we would combine customer data in each of the geographies into anonymous groups and look at all that aggregate data to understand how the two groups are different or similar.

3. Do you share anonymous or aggregate information?

   Yes, we may share this information with other companies and entities for specific uses, which may include:

   - Universities, laboratories, think tanks and other entities that conduct networking, social, behavioral, environmental and other types of scientific research, for the purpose of creating fundamental new knowledge;
   - Municipalities, government or other entities that may use this data for purposes such as municipal and transportation planning, and emergency and disaster response coordination.

We share this information in external reports like our External Marketing & Analytics Reports and Metric Reports.

QUESTIONS ABOUT EXTERNAL MARKETING AND ANALYTICS REPORTS

1. Tell me more about the External Marketing & Analytics Program.

   We use aggregate information to create External Marketing & Analytics Reports that we may sell to other companies for their own marketing, advertising or other similar uses.

   These reports may be a combination of information from wireless and Wi-Fi locations, U-verse, website browsing and mobile application usage and other information we have about you and other customers. You have a choice about whether your anonymous information is included in these reports.

   Some examples of External Marketing & Analytics Reports include:

   - Reports for retail businesses that show the number of wireless devices in or near their store locations by time of day and day of the week, together with demographic characteristics of the users (such as age and gender) in those groups.
   - Reports that combine anonymous U-verse TV viewing behaviors with other aggregate information we may have about our subscribers to create reports that would help a TV network better understand the audiences that are viewing their programs, those that are not, how frequently they watch, when they watch and other similar information; and
   - Reports for device manufacturers that combine information such as device type, make and model with demographic and regional location information to reflect the popularity of particular device types with various customer segments.

2. Do you provide companies with individual anonymous data as part of your External Marketing & Analytics Program?

   Yes. For example, we might share anonymous U-verse TV viewing information with media research companies that combine this data with other information to provide audience analysis services about what shows certain audience segments are watching. When we provide individual anonymous information to businesses, we require that they only use it to provide aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information, and that they will handle it in a secure manner, consistent with this Policy.

3. Do you use my anonymous information in other types of external reports?

   Yes, we may use your anonymous information to provide Metrics Reports to our business customers and service suppliers. These reports are considered part of the underlying service and we do not sell them to other customers or suppliers.

For example, if you connect to our Wi-Fi service in a hotel, airport or other venue you should know the operator of that venue is our business customer, and that we will provide that operator with Metrics Reports about usage of and communications with the Wi-Fi network in their location. Those reports contain statistical information like:

- The number of devices connecting to the Wi-Fi network, duration of Wi-Fi sessions and the amount of bandwidth used during those sessions; and
- Foot-traffic data, including the numbers of devices inside and outside the store at a given time; the number of new and frequent visitors; where visitors are located within the store (e.g., specific departments or other locations within the venue) and frequency of visits and time spent within the store.
- **NOTE:** When your wireless device is turned on, it regularly sends out signals that enable it to connect to cell towers, Wi-Fi access points or other technologies so that we (and others) are able to provide you with services. These signals can be used to determine your device location. You can turn Wi-Fi to the "off" position on the "settings" feature of your device to prevent the collection of these signals by Wi-Fi equipment in retail stores and other public places.

Another example, we also license U-verse video programming from content providers. As part of our agreement, we provide them with Metrics Reports. These reports contain combined measurements and statistical information related to the number of U-verse TV subscribers who watched or accessed a particular program at a particular time and other similar measurements.

QUESTIONS ABOUT OUR ONLINE PRIVACY POLICY FOR CHILDREN

1. Do you collect information about my children's use?

   We do not knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.

2. What happens when my child is using an account not registered to them?

   Internet and wireless devices and services purchased for family use may be used by children without our knowledge. When that happens, information collected may appear to us to be associated with the adult customer who subscribes to our services and will be treated as the adult's information under this Policy.

3. What can I do to help better protect my child's information?

   We encourage you to spend time online with your children, and to participate in and monitor their online activity. We have developed a website that offers safety and control tools, expert resources and tips designed to help you manage technology choices and address safety concerns. Please visit AT&T Smart Controls for more information.

4. What if my child has an AT&T e-mail sub-account?

If you create an AT&T e-mail sub-account for a child under the age of 13:

- With your permission we collect your child's name, nicknames and aliases, alternative e-mail address, birth date, gender and ZIP-code.
- We use the information collected on sub-accounts to create and maintain those accounts, for research, to customize the advertising and content seen on our pages and for other marketing purposes. Your child can use their AT&T e-mail address and password to log onto websites and online services provided by us, like uverse.com. We and our advertising partners may collect and use information about customers who log onto those sites as described in the "Questions about the Information We Collect, How we Collect It and How We Use It" section of this Privacy Policy. A list of the advertising partners who collect information on our sites and the ability to opt-out of advertising provided by those partners is available here
- We will not contact a child under the age of 13 about special offers or for marketing purposes without parental consent.
- You or your child can review, edit, update, and delete information relating to your child's sub-account and, if you no longer wish your child to have such an account, you can revoke your consent at any time, by logging on to manage your account here.

You may e-mail us at privacypolicy@att.com, call us at 800.495.1547 or write to us at AT&T Privacy Policy, 1120 20th Street, N.W., 10th Floor, Washington, DC 20036 with any questions or concerns you may have about our Children's Online Privacy Policy.

QUESTIONS ABOUT DATA PROTECTION AND SECURITY

1. Do we sell your Personal Information?

   No. We do not sell your Personal Information to anyone, for any purpose. Period.

2. How long do we keep your Personal Information?

   We keep your Personal Information as long as we need for business, tax or legal purposes. After that, we destroy it by making it unreadable or undecipherable.

3. What safeguards does AT&T have in place?

   We've worked hard to protect your information. And we've established electronic and administrative safeguards designed to make the information we collect secure. Some examples of those safeguards include:

   - All of our employees are subject to the AT&T Code of Business Conduct (COBC) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business - including, specifically, the legal requirements and company policies surrounding the privacy of

communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.

- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information. Some examples are:
    - Maintaining and protecting the security of computer storage and network equipment, and our security procedures require employee user names and passwords to access sensitive data;
    - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
    - Limiting access to Personal Information to only those with jobs requiring such access; and
    - Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change the information.
    - Although we strive to keep your Personal Information secure, no security measures are perfect, and we cannot guarantee that your Personal Information will never be disclosed in a manner inconsistent with this Policy (for example, as the result of unauthorized acts by third parties that violate the law or this Policy).

4. Will you notify me in case of a security breach?

   Yes. We will make reasonable attempts to notify you if we determine that we have experienced a security breach and there is a reasonably likely risk of identity theft, or where otherwise required by law.

5. Can I review and correct my Personal Information?

   Yes. We are happy to help you review and correct the Personal Information we have associated with your account and billing records. Please contact us.

6. Have your privacy practices been certified?

   Yes, and we're very proud of it! TRUSTe has awarded us the TRUSTe Privacy Seal. As an independent third party, TRUSTe's mission is to accelerate online trust among consumers and organizations globally through its leading privacy Trustmark and innovative trust solutions.

   Our TRUSTe Privacy Seal signifies that TRUSTe has reviewed our Privacy Policy and practices for compliance with TRUSTe's program requirements. These include transparency, accountability and choice regarding the collection and use of your Personal Information. The TRUSTe program covers only information that is collected through our certified web sites.

QUESTIONS ABOUT FUTURE CHANGES

1. What happens if there is a change in corporate ownership?

   Information about our customers and users, including Personal Information, may be shared and transferred as part of any merger, acquisition, sale of company assets or transition of service to another provider. This also applies in the unlikely event of an insolvency, bankruptcy or receivership in which customer and user records would be transferred to another entity as a result of such a proceeding.

2. Will I be notified if there are changes to this policy?

   We may update this Privacy Policy as necessary to reflect changes we make and to satisfy legal requirements. We will post a prominent notice of the change on our websites. We will provide you with other appropriate notice of important changes at least 30 days before the effective date.

YOUR CHOICES & CONTROLS

1. You can choose not to receive some types of advertising online or on your wireless device.

   - Opt-out of all Relevant Advertising delivered by AT&T AdWorks online here, and on your mobile device here. You'll need to opt-out on each computer browser and mobile device you want to exclude.
   - Opt-out of online behavioral advertising provided by AT&T and other advertisers by clicking the "Advertising Choices" link at the bottom of our web pages.
   - Opt-out of interest-based advertising on att.net powered by Yahoo! here.
   - Opt-out of online behavioral advertising from many other ad networks at the Network Advertising Initiative (NAI) site..
   - When you see online ads for AT&T products and services that display this icon  , click and you will get information on how to opt-out.
   - To limit collection of data on web sites that may be used for advertising, go here for information on how to manage cookies and other similar technologies on your computer.

2. Do I have choices about receiving first party advertisements from AT&T?

   Because first party advertising is part of the service you receive when you visit our websites and use our mobile applications, we don't offer an opt-out for first party advertising.

3. You can also choose not to receive other types of marketing from AT&T.

We realize that unwanted marketing contacts can be a hassle and we've worked hard to meet the expectations of customers and potential customers who have expressed a desire to limit certain types of solicitation communications from us.

E-Mail: Every marketing e-mail we send contains instructions and a link that will allow you to stop additional marketing e-mails for that product or service type. You also can unsubscribe from AT&T marketing e-mails here.

Text Messages: Opt-out of AT&T marketing text message contacts by replying "stop" to any message.

AT&T Consumer Telemarketing: Ask to be removed from our consumer telemarketing lists by contacting us at one of the numbers listed here. You also can ask the AT&T representative to remove you from our telemarketing lists when you receive a marketing or promotional call from us.

AT&T Business Telemarketing: Where required by state laws and/or regulations, we honor requests to be removed from our telemarketing lists from business customers.

Federal Do Not Call: The FTC maintains a National Do Not Call Registry at donotcall.gov, and your state may maintain its own Do Not Call Registry. Putting your number on these Registries also may limit our AT&T telemarketing calls to that number.

Postal Mail: To review our Residential Do Not Mail Policy Statement and to limit postal mail solicitations, click here. You will still receive billing statements, legal notices, product updates and other similar correspondence, and you may still receive some promotional mailings.

All of our practices are designed to satisfy state and federal legal requirements limiting marketing contacts. Those laws and regulations - such as the requirements governing the state and federal "Do Not Call" lists - generally permit companies to contact their own current and, in some cases, former customers, even when those customers are listed on the federal and state "Do Not Call" lists.

Restricting our use of your CPNI will not eliminate all types of our marketing contacts.

4. Can I choose to exclude my anonymous information from your External Marketing & Analytics and other similar reports?

   Yes. Click here to opt-out. This opt-out also applies to the sharing of your anonymous information with other companies for their use in creating marketing and analytics reports. Although this opt out does not apply to Metrics Reports, it will apply if we combine Metrics Report information with other customer information (like demographics) to create reports that we provide to our business customers or service suppliers.

5. Are there any other opt-out choices I should know about?

We may use services provided by analytics companies to obtain information about website performance and how you use our mobile applications and other products and services. Go here for more information about the opt-outs made available by some of those vendors, and to make choices about participation.

6. These Choices and Controls also are available at www.att.com/yourchoices.

HOW TO CONTACT US ABOUT THIS POLICY

- We encourage you to contact us directly at either of these addresses below for any questions about this Privacy Policy.
    - E-mail us at privacypolicy@att.com
    - Write to us at AT&T Privacy Policy, 1120 20th Street, N.W., 10th Floor, Washington, DC 20036.
- For questions not related to privacy click on the "Contact Us" link at the upper right hand corner of this page. You also can access your online account from the upper right hand corner of our home page at att.com for additional service options.
- If you do not receive acknowledgment of your privacy inquiry or your inquiry is not addressed to your satisfaction, you may contact TRUSTe through the TRUSTe Watchdog Dispute Resolution Process. TRUSTe will serve as a liaison to resolve your concerns.
- You also have the option of filing a complaint with the FTC Bureau of Consumer Protection, using an online form, or by calling toll-free 877.FTC.HELP (877.328.4357; TTY: 866.653.4261). Other rights and remedies also may be available to you under federal or other applicable laws.

Customer Proprietary Network Information (CPNI)

What is CPNI?

Customer Proprietary Network Information (CPNI) is information that AT&T and other telecommunications carriers obtain when providing your telecommunications services to you. CPNI includes the types of telecommunications services you currently purchase, how you use them, and the billing information related to those services, including items such as the types of local, long distance and wireless telecommunications services that you have purchased and your calling details. Your telephone number, name and address are not considered CPNI.

Use and Disclosure of CPNI

We use your CPNI to offer you additional services of the type you already purchase from AT&T. We also may use your CPNI to offer you products and services, packages, discounts and promotions from the AT&T companies, such as High Speed DSL Internet

access, wireless service and U-verse TV services, which may be different from the types of services you already purchase.

AT&T uses technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use. AT&T does not disclose CPNI outside of the AT&T companies or their agents without customer consent except as required or allowed by law. When AT&T uses third parties to perform services on its behalf that require the use of CPNI, AT&T requires that they protect CPNI consistent with this privacy policy. *AT&T does not sell CPNI to unaffiliated third parties.*

Restricting our use of your CPNI

If you wish to restrict our use of your CPNI for marketing purposes, you may contact a customer service representative at the customer service phone number located on your AT&T telephone bill or one of the following numbers:

Wireless - 1-800-331-0500

Business - 1-888-944-0447

Residential - 1-800-288-2020

Spanish Language - 1-800-870-5855

For assistance in other languages, please visit world.att.com.

Legacy AT&T Consumer - 1-800-222-0300

Restricting our use of your CPNI for marketing purposes will not affect the provision of any AT&T products or services to which you subscribe, nor will it eliminate all types of AT&T marketing contacts.

Customer Service Contact Numbers

Wireless — 1-800-331-0500

Business — 1-888-944-0447

Residential — 1-800-288-2020

Spanish Language — 1-800-870-5855

For assistance in other languages, please visit world.att.com.

Legacy AT&T Consumer — 1-800-222-0300

Customers of the following AT&T family of companies may contact us directly using the following:

YELLOWPAGES — Please contact YELLOWPAGES by sending an email to ypcsupport@yellowpages.com.

AnyWho — Please follow the opt-out instructions to remove your **residential** phone number from the AnyWho Web site.

Ether — Please contact Ether using the Customer Support request.

Keen — Please contact Keen using the Customer Support form.

AT&T Internet Services — Customers can manage newsletter subscriptions or other e-mail communications from Yahoo! by modifying their AT&T Yahoo! Marketing Preferences.

EXHIBIT 7

Customer Agreement

Contact A Sales Associate Chat Now

MY VERIZON WIRELESS CUSTOMER AGREEMENT

(Para una copia de este documento en espanol, visite nuestro website: **vzw.com/espanol.**)

Thanks for choosing Verizon Wireless. In this Customer Agreement, you'll find important information about your Service, including our ability to make changes to your Service or this agreement's terms, our liability if things don't work as planned and how any disputes between us must be resolved in arbitration or small claims court . If you're signing up for Service for a minimum contract term, you'll also find information about that contract term and what happens if you cancel a line of Service early or don't pay on time, including the possibility of an early termination fee you may owe Verizon Wireless.

MY SERVICE

Your Service terms and conditions are part of this agreement. Your Plan includes your monthly allowances and features, where you can use them (your "Coverage Area"), and their monthly and pay –per–use charges. You can also subscribe to several Optional Services, like text messaging packages. Together, your Plan and any Optional Services you select are your Service. The terms and conditions for your Service can be found in the brochures that are available when you activate, or online at **verizonwireless.com**

HOW DO I ACCEPT THIS AGREEMENT?

You accept this agreement by:

- Agreeing in writing, by email, over the phone, or in person;
- Opening a package that says you are accepting by opening it; or
- Activating your Service.

When you accept, you're representing that you are at least 18 years old and are legally able to accept an agreement. If you're accepting for an organization, you're representing that you are authorized to bind that organization, and where the context requires, "you" means the organization. By accepting you are agreeing to every provision of this Agreement whether or not you have to read it.

If you do accept, you can cancel a line of Service within 14 days of accepting this Agreement without having to pay an early termination fee as long as you return, within the applicable return period, any equipment you purchased from us or one of our authorized agents at a discount in connection with your acceptance of this Agreement, but you'll still have to pay for your Service through that date. If you signed up for Prepaid Service, no refunds will be granted after 14 days or if your account has been activated. Your activation fee will not be refunded unless you cancel within three days of accepting.

If you change your device or receive a Service promotion, you may be required to change your Plan to one that we are currently offering at that time.

MY PRIVACY

We collect personal information about you. We gather some information through our relationship with you, such as information about the quantity, technical configuration, type, destination and amount of your use of our telecommunications services. You can find out how we use, share and protect the information we collect about you in the Verizon Privacy Policy, available at **verizon.com/privacy.** By entering this Agreement, you consent to our data collection, use and sharing practices described in our Privacy Policy. We provide you with choices to limit, in certain circumstances, our use of the data we have about you. You can review these choices at **verizon.com/privacy#limits.** If there are additional specific advertising and marketing practices for which your consent is necessary, we will seek your consent (such as through the privacy–related notices you receive when you purchase or use products and services) before engaging in those practices. If you subscribe to Service for which usage charges are billed at the end of the billing period ("Postpay Service"), we may investigate your credit history at any time and share credit information about you with credit reporting agencies and other Verizon companies. If you'd like the name and address of any credit agency that gives us a credit report about you, just ask.

Many services and applications offered through your device may be provided by third parties. Some of these services and applications, which you may block or restrict at no cost, may involve charges for which you will be billed. The amount and frequency of the charges will be disclosed when you agree to the charges. Before you use, link to or download a service or application provided by a third party, you should review the terms of such service or application and applicable privacy policy. Personal information you submit may be read, collected or used by the service or application provider and/or other users of those forums. Verizon Wireless is not responsible for any third–party information, content, applications or services you access, download or use on your device. You are responsible for maintaining virus and other Internet security protections when accessing these third–party products or services. For edditional information, visit the Verizon Content Policy at **http://responsibility.verizon.com/contentpolicy**

You consent to allow Verizon Wireless and anyone who collects on our behalf to contact you about your account status, including past due or current charges, using prerecorded calls, email and calls or messages delivered by an automatic telephone dialing system to any wireless phone number or email address you provide. Verizon Wireless will treat any email address you provide as your private email that is not accessible by unauthorized third parties. Unless you notify us that your wireless service is based in a different time zone, calls will be made to your cellular device during permitted calling hours based upon the time zone affiliated with the mobile telephone number you provide.

WHAT HAPPENS IF MY POSTPAY SERVICE IS CANCELED BEFORE THE END OF MY CONTRACT TERM?

If you're signing up for Postpay Service, you're agreeing to subscribe to a line of Service either on a month–to–month basis or for a minimum contract term, as shown on your receipt or order confirmation. (If your Service is suspended without billing, that time doesn't count toward completing your contract term.) Once you've completed your contract term, you'll automatically become a customer on a month–to–month basis for that line of Service. **If you cancel a line of Service, or if we cancel it for good cause, during its contract term, you'll have to pay an early termination fee. If your contract term results from your purchase of an advanced device, your early termination fee will be $350 minus $10 for each full month of your contract term that you complete. Otherwise, your early termination fee will be $175 minus $5 for each full month of your contract term that you complete. Cancellations will become effective on the last day of that month's billing cycle,** and you are responsible for all charges incurred until then. Also, if you bought your wireless device from an authorized agent or third–party vendor, you should check whether they charge a separate termination fee.

CAN I TAKE MY WIRELESS PHONE NUMBER TO ANOTHER CARRIER?

You may be able to take, or "port", your wireless phone number to another carrier. If you port a number from us, we'll treat it as though you asked us to cancel your Service for that number. After the porting is completed, you won't be able to use our service for that number, but you'll remain responsible for all fees and charges through the end of that billing cycle, just like any other cancellation. If you're a Prepaid customer, you won't be entitled to a refund of any balance on your account. If you port a number to us, please be aware that we may not be able to provide some services right away, such as 911 location services. You don't have any rights to your wireless phone number, except for any right you may have to port it.

DIRECTORY INFORMATION

We will not publish your wireless phone number in any available directory or give it to anyone for that purpose, unless you ask us to.

CAN I HAVE SOMEONE ELSE MANAGE MY POSTPAY ACCOUNT?

No problem – just tell us by phone, in person, or in writing. You can appoint someone to manage your Postpay account for a single transaction, or until you tell us otherwise. The person you appoint will be able to make changes to your account, including adding new lines of Service, buying new wireless devices, and extending your contract term. Any changes that person makes will be treated as modifications to this agreement.

CAN VERIZON WIRELESS CHANGE THIS AGREEMENT OR MY SERVICE?

We may change prices or any other term of your Service or this agreement at any time,but we'll provide notice first, including written notice if you have Postpay Service. If you use your Service after the change takes effect, that means you're accepting the change. If you're a Postpay customer and a change to your Plan or this agreement has a material adverse effect on you, you can cancel the line of Service that has been affected within 60 days of receiving the notice with no early termination fee if we fail to negate the change after you notify us of your objection to it.

MY WIRELESS DEVICE

Your wireless device must comply with Federal Communications Commission regulations, be certified for use on our network, and be compatible with your Service. Please be aware that we may change your wireless device's software, applications or programming remotely, without notice. This could affect your stored data, or how you've programmed or use your wireless device. By activating Service that uses a SIM (Subscriber Identity Module) card, you agree we own the intellectual property and software in the SIM card, that we may change the software or other data in the SIM card remotely and without notice, and we may utilize any capacity in the SIM card for administrative, network, business and/or commercial purposes. If you bought a wireless device for Postpay Service from Verizon Wireless that doesn't use a SIM card, and you want to reprogram it for use with another wireless network, the default programming code is set to "000000" or "123456." But please note that your wireless device may not work with another wireless network, or the other wireless carrier may not accept your wireless device on its network. If you activate a wireless device for Prepaid Service, during the first six (6) months after activation, it can only be used for Prepaid Service. The iPhone 4 is configured to work only with the wireless services of Verizon Wireless and may not work on another carrier's network, even after completion of your contract term.

WHERE AND HOW DOES VERIZON WIRELESS SERVICE WORK?

Wireless devices use radio transmissions, so unfortunately you can't get Service if your device isn't in range of a transmission signal. And please be aware that even within your Coverage Area, many things can affect the availability and quality of your Service, including network capacity, your device, terrain, buildings, foliage and weather.

WHAT CHARGES ARE SET BY VERIZON WIRELESS?

You agree to pay all access, usage and other charges that you or the user of your wireless device incurred. For Postpay Service, our charges also include Federal Universal Service, Regulatory and Administrative Charges, and we may also include other charges related to our governmental costs. We set these charges; they aren't taxes, they aren't required by law, they are not necessarily related to anything the government does, they are kept by us in whole or in part, and the amounts and what they pay for may change.

GOVERNMENT TAXES, FEES AND SURCHARGES

You must pay all taxes, fees and surcharges set by federal, state and local governments. Please note that we may not always be able to notify you in advance of changes to these charges.

WHAT ARE ROAMING CHARGES?

You're "roaming" whenever your wireless device uses a transmission site outside your Coverage Area or uses another company's transmission site. Sometimes roaming happens even when you're within your Coverage Area. There may be higher rates and extra charges (including charges for long distance, tolls or calls that don't connect) for roaming calls, depending on your Plan.

HOW DOES VERIZON WIRELESS CALCULATE MY CHARGES?

For charges based on the amount of time used or data sent or received, we'll round up any fraction to the next full minute or, depending on how you're billed for data usage, the next full megabyte or gigabyte. For outgoing calls, usage time starts when you first press **Send** or the call connects to a network, and for incoming calls, it starts when the call connects to a network (which may be before it rings). Usage time may end several seconds after you press **End** or after the call disconnects. For calls made on our network, we charge only for calls that are answered, including by machines. For Postpay Service, usage cannot always be processed right away and may be included in a later bill, but the usage will still count towards your allowance for the month when the Service was used.

HOW AND WHEN CAN I DISPUTE CHARGES?

If you're a Postpay customer, you can dispute your bill within 180 days of receiving it, but unless otherwise provided by law or unless you're disputing charges because your wireless device was lost or stolen, you still have to pay all charges until the dispute is resolved. If you're a Prepaid customer, you can dispute a charge within 180 days of the date the disputed charge was incurred. **YOU MAY CALL US TO DISPUTE CHARGES ON YOUR BILL OR ANY SERVICE(S) FOR WHICH YOU WERE BILLED, BUT IF YOU WISH TO PRESERVE YOUR RIGHT TO BRING AN ARBITRATION OR SMALL CLAIMS CASE REGARDING SUCH DISPUTE, YOU MUST WRITE TO US AT THE CUSTOMER SERVICE ADDRESS ON YOUR BILL, OR SEND US A COMPLETED NOTICE OF DISPUTE FORM (AVAILABLE AT VERIZONWIRELESS.COM), WITHIN THE 180–DAY PERIOD MENTIONED ABOVE. IF YOU DO NOT NOTIFY US IN WRITING OF SUCH DISPUTE WITHIN THE 180-DAY PERIOD, YOU WILL HAVE WAIVED YOUR RIGHT TO DISPUTE THE BILL OR SUCH SERVICE(S) AND TO BRING AN ARBITRATION OR SMALL CLAIMS CASE REGARDING ANY SUCH DISPUTE.**

WHAT ARE MY RIGHTS FOR DROPPED CALLS OR INTERRUPTED SERVICE?

If you drop a call in your Coverage Area, redial. If it's answered within 5 minutes, call us within 90 days if you're a Postpay customer, or within 45 days if you're a Prepaid customer, and we'll give you a 1–minute airtime credit. If you're a Postpay customer and you lose Service in your Coverage Area for more than 24 hours in a row and we're at fault, call us within 180 days and we'll give you a credit for the time lost. Please be aware that these are your only rights for dropped calls or interrupted Service.

ABOUT MY PAYMENTS

If you're a Postpay customer and we don't get your payment on time, we will charge you a late fee of up to 1.5 percent per month (18 percent per year) on the unpaid balance, or a flat $5 per month, whichever is greater, if allowed by law in the state of your billing address. (If you choose another company to bill you for our Service [such as another Verizon company], late fees are set by that company or by its tariffs and may be higher than our late fees.) Late fees are part of the rates and charges you agree to pay us. If you fail to pay on time and Verizon Wireless refers your account(s) to a third party for collection, a collection fee will be assessed and will be due at the time of the referral to the third party. The fee will be calculated at the maximum percentage permitted by applicable law, not to exceed 18 percent. We may require a deposit at the time of activation or afterward, or an increased deposit. We'll pay simple interest on any deposit at the rate the law requires. We may apply deposits or payments in any order to any amounts you owe us on any account. If your final credit balance is less than $1, we will refund it only if you ask. You may have to pay a $35 fee to re–activate Service if your Service is terminated , or a $15 fee to reconnect Service if it is interrupted for non–payment or suspended for any reason.

If you're a Prepaid customer, you may replenish your balance at any time before the expiration date by providing us with another payment. Your balance may not exceed $1,000 and you may be prevented from replenishing if your balance reaches $1,000. We will suspend service when your account reaches the expiration date and any unused balance will be forfeited.

We may charge you up to $25 for any returned check.

WHAT IF MY WIRELESS DEVICE GETS LOST OR STOLEN?

We're here to help. It's important that you notify us right away, so we can suspend your Service to keep someone else from using it. If you're a Postpay customer and your wireless device is used after the loss or theft but before you report it, and you want a credit for any charges for that usage, we're happy to review your account activity and any other information you'd like us to consider. Keep in mind that you may be held responsible for the charges if you delayed reporting the loss or theft without good reason, but you don't have to pay any charges you dispute while they are being investigated. If we haven't given you a courtesy suspension of recurring monthly charges during the past year, we'll give you one for 30 days or until you replace or recover your wireless device, whichever comes first.

WHAT ARE VERIZON WIRELESS' RIGHTS TO LIMIT OR END SERVICE OR END THIS AGREEMENT?

We can, without notice, limit, suspend or end your Service or any agreement with you for any good cause, including, but not limited to: (1) if you: (a) breach this agreement; (b) resell your Service; (c) use your Service for any illegal purpose, including use that violates trade and economic sanctions and prohibitions promulgated by any US governmental agency; (d) install, deploy or use any regeneration equipment or similar mechanism (for example, a repeater) to originate, amplify, enhance, retransmit or regenerate an RF signal without our permission; (e) steal from or lie to us; or, if you're a Postpay customer; (f) do not pay your bill on time; (g) incur charges larger than a required deposit or billing limit, or materially in excess of your monthly access charges (even if we haven't yet billed the charges); (h) provide credit information we can't verify; or (i) are unable to pay us or go bankrupt; or (2) if you, any user of your device or any line of service on your account, or any account manager on your account: (a) threaten, harass, or use vulgar and/or inappropriate language toward our representatives; (b) interfere with our operations; (c) "spam," or engage in other abusive messaging or calling; (d) modify your device from its manufacturer's specifications; or (e) use your Service in a way that negatively affects our network or other customers. We can also temporarily limit your Service for any operational or governmental reason.

AM I ELIGIBLE FOR SPECIAL DISCOUNTS?

If you're a Postpay customer, you may be eligible for a discount if you are and remain affiliated with an organization that has an agreement with us. Unless your discount is through a government employee discount program, we may share certain information about your Service (including your name, your wireless telephone number and your total monthly charges) with your organization from time to time to make sure you're still eligible. We may adjust or remove your discount according to your organization's agreement with us, and remove your discount if your eligibility ends or your contract term expires. In any case, this won't be considered to have a material adverse effect on you.

DISCLAIMER OF WARRANTIES

We make no representations or warranties, express or implied, including, to the extent permitted by applicable law, any implied warranty of merchantability or fitness for a particular purpose, about your Service, your wireless device, or any applications you access through your wireless device. We do not warrant that your wireless device will work perfectly or will not need occasional upgrades or modifications, or that it will not be negatively affected by network-related modifications, upgrades or similar activity. If you download or use applications, services or software provided by third parties (including voice applications), 911 or E911, or other calling functionality, may work differently than services offered by us, or may not work at all. Please review all terms and conditions of such third-party products.

Please be aware that if you activated your wireless device through our Open Development program, we can't vouch for the device's call quality or overall functionality.

WAIVERS AND LIMITATIONS OF LIABILITY

You and Verizon Wireless both agree to limit claims against each other for damages or other monetary relief to direct damages. This limitation and waiver will apply regardless of the theory of liability. That means neither of us will try to get any indirect, special, consequential, treble or punitive damages from the other. This limitation and waiver also applies if you bring a claim against one of our suppliers, to the extent we would be required to indemnify the supplier for the claim. You agree we aren't responsible for problems caused by you or others, or by any act of God. You also agree we aren't liable for missed or deleted voice mails or other messages, or for any information (like pictures) that gets lost or deleted if we work on your device. If another wireless carrier is involved in any problem (for example, while you're roaming), you also agree to any limitations of liability that it imposes.

HOW DO I RESOLVE DISPUTES WITH VERIZON WIRELESS?

WE HOPE TO MAKE YOU A HAPPY CUSTOMER, BUT IF THERE'S AN ISSUE THAT NEEDS TO BE RESOLVED, THIS SECTION OUTLINES WHAT'S EXPECTED OF BOTH OF US.

YOU AND VERIZON WIRELESS BOTH AGREE TO RESOLVE DISPUTES ONLY BY ARBITRATION OR IN SMALL CLAIMS COURT. THERE'S NO JUDGE OR JURY IN ARBITRATION, AND THE PROCEDURES MAY BE DIFFERENT, BUT AN ARBITRATOR CAN AWARD YOU THE SAME DAMAGES AND RELIEF, AND MUST HONOR THE SAME TERMS IN THIS AGREEMENT, AS A COURT WOULD. IF THE LAW ALLOWS FOR AN AWARD OF ATTORNEYS' FEES, AN ARBITRATOR CAN AWARD THEM TOO. WE ALSO BOTH AGREE THAT:

(1) THE FEDERAL ARBITRATION ACT APPLIES TO THIS AGREEMENT. EXCEPT FOR SMALL CLAIMS COURT CASES THAT QUALIFY, ANY DISPUTE THAT IN ANY WAY RELATES TO OR ARISES OUT OF THIS AGREEMENT OR FROM ANY EQUIPMENT, PRODUCTS AND SERVICES YOU RECEIVE FROM US (OR FROM ANY ADVERTISING FOR ANY SUCH PRODUCTS OR SERVICES) WILL BE RESOLVED BY ONE OR MORE NEUTRAL ARBITRATORS BEFORE THE AMERICAN ARBITRATION ASSOCIATION ("AAA") OR BETTER BUSINESS BUREAU ("BBB"). YOU CAN ALSO BRING ANY ISSUES YOU MAY HAVE TO THE ATTENTION OF FEDERAL, STATE, OR LOCAL GOVERNMENT AGENCIES, AND IF THE LAW ALLOWS, THEY CAN SEEK RELIEF AGAINST US FOR YOU.

(2) UNLESS YOU AND VERIZON WIRELESS AGREE OTHERWISE, THE ARBITRATION WILL TAKE PLACE IN THE COUNTY OF YOUR BILLING ADDRESS. FOR CLAIMS OVER $10,000, THE AAA'S WIRELESS INDUSTRY ARBITRATION ("WIA") RULES WILL APPLY, IN SUCH CASES, THE LOSER CAN ASK FOR A PANEL OF THREE NEW ARBITRATORS TO REVIEW THE AWARD. FOR CLAIMS OF $10,000 OR LESS, THE PARTY BRINGING THE CLAIM CAN CHOOSE EITHER THE AAA'S WIA RULES OR THE BBB'S RULES FOR BINDING ARBITRATION OR, ALTERNATIVELY, CAN BRING AN INDIVIDUAL ACTION IN SMALL CLAIMS COURT. YOU CAN GET PROCEDURES, RULES AND FEE INFORMATION FROM THE AAA (WWW.ADR.ORG), THE BBB (WWW.BBB.ORG) OR FROM US. FOR CLAIMS OF $10,000 OR LESS, YOU CAN CHOOSE WHETHER YOU'D LIKE THE ARBITRATION CARRIED OUT BASED ONLY ON DOCUMENTS SUBMITTED TO THE ARBITRATOR, OR BY A HEARING IN–PERSON OR BY PHONE.

(3) THIS AGREEMENT DOESN'T ALLOW CLASS OR COLLECTIVE ARBITRATIONS EVEN IF THE AAA OR BBB PROCEDURES OR RULES WOULD. NOT WITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, THE ARBITRATOR MAY AWARD MONEY OR INJUNCTIVE RELIEF ONLY IN FAVOR OF THE INDIVIDUAL PARTY SEEKING RELIEF AND ONLY TO THE EXTENT NECESSARY TO PROVIDE RELIEF WARRANTED BY THAT PARTY'S INDIVIDUAL CLAIM. NO CLASS OR REPRESENTATIVE OR PRIVATE ATTORNEY GENERAL THEORIES OF LIABILITY OR PRAYERS FOR RELIEF MAY BE MAINTAINED IN ANY ARBITRATION HELD UNDER THIS AGREEMENT.

(4) IF EITHER OF US INTENDS TO SEEK ARBITRATION UNDER THIS AGREEMENT, THE PARTY SEEKING ARBITRATION MUST FIRST NOTIFY THE OTHER PARTY OF THE DISPUTE IN WRITING AT LEAST 30 DAYS IN ADVANCE OF INITIATING THE ARBITRATION. NOTICE TO VERIZON WIRELESS SHOULD BE SENT TO VERIZON WIRELESS DISPUTE RESOLUTION MANAGER, ONE VERIZON WAY, VC52N061, BASKING RIDGE, NJ 07920. THE NOTICE MUST DESCRIBE THE NATURE OF THE CLAIM AND THE RELIEF BEING SOUGHT. IF WE ARE UNABLE TO RESOLVE OUR DISPUTE WITHIN 30 DAYS, EITHER PARTY MAY THEN PROCEED TO FILE A CLAIM FOR ARBITRATION. WE'LL PAY ANY FILING FEE THAT THE AAA OR BBB CHARGES YOU FOR ARBITRATION OF THE DISPUTE. IF YOU PROVIDE US WITH SIGNED WRITTEN NOTICE THAT YOU CANNOT PAY THE FILING FEE, VERIZON WIRELESS WILL PAY THE FEE DIRECTLY TO THE AAA OR BBB. IF THAT ARBITRATION PROCEEDS, WE'LL ALSO PAY ANY ADMINISTRATIVE AND ARBITRATOR FEES CHARGED LATER, AS WELL AS FOR ANY APPEAL TO A PANEL OF THREE NEW ARBITRATORS (IF THE ARBITRATION AWARD IS APPEALABLE UNDER THIS AGREEMENT).

(5) WE ALSO OFFER CUSTOMERS THE OPTION OF PARTICIPATING IN A FREE INTERNAL MEDIATION PROGRAM. THIS PROGRAM IS ENTIRELY VOLUNTARY AND DOES NOT AFFECT EITHER PARTY'S RIGHTS IN ANY OTHER ASPECT OF THESE DISPUTE RESOLUTION PROCEDURES. IN OUR VOLUNTARY MEDIATION PROGRAM, WE WILL ASSIGN AN EMPLOYEE WHO'S NOT DIRECTLY INVOLVED IN THE DISPUTE TO HELP BOTH SIDES REACH AN AGREEMENT. THAT PERSON HAS ALL THE RIGHTS AND PROTECTIONS OF A MEDIATOR AND THE PROCESS HAS ALL OF THE PROTECTIONS ASSOCIATED WITH MEDIATION. FOR EXAMPLE, NOTHING SAID IN THE MEDIATION CAN BE USED LATER IN AN ARBITRATION OR LAWSUIT. IF YOU'D LIKE TO KNOW MORE, PLEASE CONTACT US AT **VERIZONWIRELESS.COM** OR THROUGH CUSTOMER SERVICE. IF YOU'D LIKE TO START THE MEDIATION PROCESS, PLEASE GO TO **VERIZONWIRELESS.COM** OR CALL CUSTOMER SERVICE FOR A NOTICE OF DISPUTE FORM TO FILL OUT, AND MAIL, FAX OR EMAIL IT TO US ACCORDING TO THE DIRECTIONS ON THE FORM.

(6) WE MAY, BUT ARE NOT OBLIGATED TO, MAKE A WRITTEN SETTLEMENT OFFER ANYTIME BEFORE ARBITRATION BEGINS. THE AMOUNT OR TERMS OF ANY SETTLEMENT OFFER MAY NOT BE DISCLOSED TO THE ARBITRATOR UNTIL AFTER THE ARBITRATOR ISSUES AN AWARD ON THE CLAIM. IF YOU DON'T ACCEPT THE OFFER AND THE ARBITRATOR AWARDS YOU AN AMOUNT OF MONEY THAT'S MORE THAN OUR OFFER BUT LESS THAN $5,000, OR IF

WE DON'T MAKE YOU AN OFFER, AND THE ARBITRATOR AWARDS YOU ANY AMOUNT OF MONEY BUT LESS THAN $5,000, THEN WE AGREE TO PAY YOU $5,000 INSTEAD OF THE AMOUNT AWARDED. IN THAT CASE WE ALSO AGREE TO PAY ANY REASONABLE ATTORNEYS' FEES AND EXPENSES, REGARDLESS OF WHETHER THE LAW REQUIRES IT FOR YOUR CASE. IF THE ARBITRATOR AWARDS YOU MORE THAN $5,000, THEN WE WILL PAY YOU THAT AMOUNT.

(7) AN ARBITRATION AWARD AND ANY JUDGMENT CONFIRMING IT APPLY ONLY TO THAT SPECIFIC CASE; IT CAN'T BE USED IN ANY OTHER CASE EXCEPT TO ENFORCE THE AWARD ITSELF.

(8) IF FOR SOME REASON THE PROHIBITION ON CLASS ARBITRATIONS SET FORTH IN SUBSECTION (3) CANNOT BE ENFORCED, THEN THE AGREEMENT TO ARBITRATE WILL NOT APPLY.

(9) IF FOR ANY REASON A CLAIM PROCEEDS IN COURT RATHER THAN THROUGH ARBITRATION, YOU AND VERIZON WIRELESS AGREE THAT THERE WILL NOT BE A JURY TRIAL. YOU AND VERIZON WIRELESS UNCONDITIONALLY WAIVE ANY RIGHT TO TRIAL BY JURY IN ANY ACTION, PROCEEDING OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT IN ANY WAY. IN THE EVENT OF LITIGATION, THIS PARAGRAPH MAY BE FILED TO SHOW A WRITTEN CONSENT TO A TRIAL BY THE COURT.

ABOUT THIS AGREEMENT

If we don't enforce our rights under this agreement in one instance, that doesn't mean we won't or can't enforce those rights in any other instance. You cannot assign this agreement or any of your rights or duties under it without our permission. However, we may assign this agreement or any debt you owe us without notifying you. **If you're a Postpay customer, please note that many notices we send to you will show up as messages on your monthly bill. If you have online billing, those notices will be deemed received by you when your online bill is available for viewing. If you get a paper bill, those notices will be deemed received by you three days after we mail the bill to you. If we send other notices to you, they will be considered received immediately if we send them to your wireless device, or to any email or fax number you've given us, or after three days if we mail them to your billing address. If you need to send notices to us, please send them to the customer service address on your latest bill.**

If you're a Prepaid customer and we send notices to you, they will be considered received immediately if we send them to your wireless device or to any email or fax number you've given us, or if we post them as a precall notification on your Service, or after three days if we mail them to the most current address we have for you. If you need to send notices to us, please send them to the Customer Service Prepaid address atverizonwireless.com/contactus

If any part of this agreement, including anything regarding the arbitration process (except for the prohibition on class arbitrations as explained in part 8 of the dispute resolution section above), is ruled invalid, that part may be removed from this agreement.

This agreement and the documents it incorporates form the entire agreement between us. You can't rely on any other documents, or on what's said by any Sales or Customer Service Representatives, and you have no other rights regarding Service or this agreement. This agreement isn't for the benefit of any third party except our parent companies, affiliates, subsidiaries, agents, and predecessors and successors in interest. Except where we've agreed otherwise elsewhere in this agreement, this agreement and any disputes covered by it are governed by federal law and the laws of the state encompassing the area code of your wireless phone number when you accepted this agreement, without regard to the conflicts of laws and rules of that state.

Last Updated: 03/24/14

EXHIBIT 8

Print

WIRELESS CUSTOMER AGREEMENT ("Agreement")

"AT&T" or "we," "us," or "our" refers to AT&T Mobility LLC, acting on behalf of its FCC-licensed affiliates doing business as AT&T. "You" or "your" refers to the person or entity that is the customer of record.

PLEASE READ THIS AGREEMENT CAREFULLY TO ENSURE THAT YOU UNDERSTAND EACH PROVISION, INCLUDING OUR USE OF YOUR LOCATION INFORMATION (SEE SECTION 3.6). THIS AGREEMENT REQUIRES THE USE OF ARBITRATION ON AN INDIVIDUAL BASIS TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS OR CLASS ACTIONS, AND ALSO LIMITS THE REMEDIES AVAILABLE TO YOU IN THE EVENT OF A DISPUTE.

This Agreement, including the AT&T Privacy Policy Located at **att.com/privacy (http://www.att.com/privacy)**, Customer Service Summary, and terms of service for wireless products, features, applications, and services ("Services") not otherwise described herein that are posted on applicable AT&T websites or devices, and any documents expressly referred to herein or therein, make up the complete agreement between you and AT&T and supersede any and all prior agreements and understandings relating to the subject matter of this Agreement.

1.0 TERM COMMITMENT, CHARGES, BILLING AND PAYMENT

1.1 What Is The Term Of My Service? How Can I Fulfill My Service Commitment? What are My Rights to Cancel Service and Terminate My Agreement?

AT&T Wireless Service(s) may be used with: (a) a mobile device that contains a SIM that is assigned to your account ("Device") and/or, (b) a device that is designed and purchased for use exclusively on AT&T's network ("Equipment").

Term of Service. Your Agreement begins on the day we activate your Service(s) and continues through the Term of Service, typically a 12 month or 24 month period ("Service Commitment"), specified on your Customer Service Summary. At the end of your service commitment, this Agreement will automatically continue on a month-to-month basis. If your Agreement has no Service Commitment, it is a month-to-month Agreement.

Fulfillment of Service Commitment. You have received certain benefits from us in exchange for your Service Commitment, which may include, but are not limited to, a subsidized wireless device. There are two alternative ways to fulfill your Service Commitment. You can pay for the Services described in your Customer Service Summary for the term of your Service Commitment, or you can terminate your Agreement prior to the end of your Service Commitment and pay an Early Termination Fee ("ETF"). The Early Termination Fee is not a penalty, but rather is an alternative means for you to perform your obligations under the Agreement that partially compensates us for the fact that the Service Commitment on which your rate plan is based was not completed.

Your Termination Rights. Within the first 14 days after service activation, you may terminate your Agreement for any reason and not be required to pay an ETF. If you terminate within three (3) days of accepting the Agreement, AT&T will refund your activation fee, if any. However, you agree to pay AT&T for all fees, charges, and other amounts incurred and owed under your Agreement, and you agree to return to AT&T any Equipment you purchased from AT&T in connection with your Service Commitment. If you fail to return this Equipment, you will be charged the difference between the amount you paid AT&T for the Equipment and the amount you would have been charged for the Equipment had you not agreed to a Service Commitment. AT&T also may charge you a restocking fee for any returned Equipment. Some dealers may impose additional fees.

After the first 14 days, you may terminate your Agreement for any reason. However, you agree to pay AT&T for all fees, charges, and other amounts incurred and owed under your Agreement along with the applicable ETF. The Early Termination Fee is either: (a) $325 minus $10 for each full month of your Service Commitment that you complete; or (b) $150 minus $4 for each full month of your Service Commitment that you complete. To determine whether your Equipment has a $325 Early Termination Fee or a $150 Early Termination Fee, check **att.com/equipmentETF (http://www.att.com/equipmentETF)**.

After your Service Commitment ends and you are on a month-to-month Agreement, you may terminate your Agreement at any time with 30 days notice without incurring an ETF. If you sign a new Agreement before the end of the term of your existing Agreement and terminate that new Agreement within 14 days as allowed above, you agree that you will be bound by the terms and conditions of your existing Agreement including fulfillment of any remaining Service Commitment thereunder.

1.2 What are AT&T's Rights to Cancel My Service(s) and Terminate My Agreement?

AT&T may interrupt, suspend or cancel your Services and terminate your Agreement without advance notice for any reason including, but not limited to, the following:

- Any conduct that we believe violates this Agreement or AT&T's Acceptable Use Policy;
- Any conduct that involves the use of abusive, derogatory, insulting, threatening, vulgar or similarly unreasonable language or behavior directed at any of our employees or representatives whether it be in person, over the phone, or in writing;
- You use your Device/Equipment and/or our Services for an unlawful purpose;
- You use your Device/Equipment and/or our Services in any way that: (a) is harmful to, interferes with, or negatively affects our network, other customers, or the network of any other provider, (b) is harmful to, interferes with, or negatively affects our Services or operations, (c) infringes intellectual property rights of AT&T or others, (d) results in the publication of threatening, offensive or illegal material, or (e) generates spam or other abusive messaging or calling, a security risk, or a violation of privacy;
- You fail to make all required payments when due;
- Your credit has deteriorated and/or we believe that there is a risk of non-payment;
- You refuse to pay any required advance payment or deposit;
- We discover that you are underage;
- You provide inaccurate or misleading credit information; or
- You modify your device from its manufacturer's specifications.

AT&T's rights under this Section 1.2 are in addition to any specific rights that we reserve in other provisions of this Agreement to interrupt, suspend, modify, or cancel your Services and terminate your Agreement.

After your Service Commitment ends and you are on a month-to-month Agreement, AT&T may terminate your Agreement at any time with 30 days notice.

1.3 Can AT&T Change My Terms And Rates?

We may change any terms, conditions, rates, fees, expenses, or charges regarding your Services at any time. We will provide you with notice of material changes (other than changes to governmental fees, proportional charges for governmental mandates, roaming rates or administrative charges) either in your monthly bill or separately. You understand and agree that State and Federal Universal Service Fees and other governmentally imposed fees, whether or not assessed directly upon you, may be increased based upon the government's or our calculations.

IF WE INCREASE THE PRICE OF ANY OF THE SERVICES TO WHICH YOU SUBSCRIBE, BEYOND THE LIMITS SET FORTH IN YOUR CUSTOMER SERVICE SUMMARY, OR IF WE MATERIALLY DECREASE THE GEOGRAPHICAL AREA IN WHICH YOUR AIRTIME RATE APPLIES (OTHER THAN A TEMPORARY DECREASE FOR REPAIRS OR MAINTENANCE), WE'LL DISCLOSE THE CHANGE AT LEAST ONE BILLING CYCLE IN ADVANCE (EITHER THROUGH A NOTICE WITH YOUR BILL, A TEXT MESSAGE TO YOUR DEVICE, OR OTHERWISE), AND YOU MAY TERMINATE THIS AGREEMENT WITHOUT PAYING AN EARLY TERMINATION FEE OR RETURNING OR PAYING FOR ANY PROMOTIONAL ITEMS, PROVIDED YOUR NOTICE OF TERMINATION IS DELIVERED TO US WITHIN THIRTY (30) DAYS AFTER THE FIRST BILL REFLECTING THE CHANGE.

If you lose your eligibility for a particular rate plan, we may change your rate plan to one for which you qualify.

1.4 How Will I Receive My Bill? What Charges Am I Responsible For? How Much Time Do I Have To Dispute My Bill?

You will receive an electronic (paperless) bill at AT&T's online account management site unless you tell us you want a paper bill. You will be given the option to choose electronic billing or paper billing when you purchase service. Each month we will send you an email notice when your electronic bill is available online. This will be sent to your official email address on file with AT&T. You are required to keep your email address current and to notify us immediately of any change in your email address. You always have the option of switching back to a paper bill by changing your billing preferences at AT&T's online account management site. You will not receive a paper bill in the mail unless you expressly request one.

You are responsible for paying all charges for or resulting from Services provided under this Agreement, including any activation fee that may apply to each voice or data line. You will receive monthly bills that are due in full.

IF YOU DISPUTE ANY CHARGES ON YOUR BILL, YOU MUST NOTIFY US IN WRITING AT AT&T BILL DISPUTE, 1025 LENOX PARK, ATLANTA, GA 30319 WITHIN 100 DAYS OF THE DATE OF THE BILL OR YOU'LL HAVE WAIVED YOUR RIGHT TO DISPUTE THE BILL AND TO PARTICIPATE IN ANY LEGAL ACTION RAISING SUCH DISPUTE.

Charges include, without limitation, airtime, roaming, recurring monthly service, activation, administrative, and late payment charges; regulatory cost recovery and other surcharges; optional feature charges; toll, collect call and directory assistance charges; restoral and reactivation charges; any other charges or calls billed to your phone number; and applicable taxes and governmental fees, whether assessed directly upon you or upon AT&T.

To determine your primary place of use ("PPU") and which jurisdiction's taxes and assessments to collect, you're required to provide us with your residential or business street address. If you don't provide us with such address, or if it falls outside our licensed Services area, we may reasonably designate a PPU within the licensed Services area for you. You must live and have a mailing address within AT&T's owned network coverage area.

1.5 How Does AT&T Calculate My Bill?

Usage and monthly fees will be billed as specified in your customer service summary or rate plan information online. If the Equipment you order is shipped to you, your Services may be activated before you take delivery of the Equipment so that you can use it promptly upon receipt. Thus, you may be charged for Services while your Equipment is still in transit. If, upon receiving your first bill, you have been charged for Services while your Equipment was in transit, you may contact Customer Care 1-800-331-0500 to request a credit. Except as provided below, monthly Services and certain other charges are billed one month in advance, and there is no proration of such charges if Service is terminated on other than the last day of your billing cycle. Monthly Service and certain other charges are billed in arrears if you're a former customer of AT&T Wireless and maintain uninterrupted Service on select AT&T rate plans, however, if you elect to receive your bills for your Services combined with your wireline phone bill (where available) you will be billed in advance as provided above. You agree to pay for all services used with your Device.

AIRTIME AND OTHER MEASURED USAGE ("CHARGEABLE TIME") IS BILLED IN FULL-MINUTE INCREMENTS, AND ACTUAL AIRTIME AND USAGE ARE ROUNDED UP TO THE NEXT FULL-MINUTE INCREMENT AT THE END OF EACH CALL FOR BILLING PURPOSES. AT&T CHARGES A FULL MINUTE OF AIRTIME USAGE FOR EVERY FRACTION OF THE LAST MINUTE OF AIRTIME USED ON EACH WIRELESS CALL. UNLESS OTHERWISE PROVIDED IN YOUR PLAN, MINUTES WILL BE DEPLETED ACCORDING TO USAGE IN THE FOLLOWING ORDER: NIGHT AND WEEKEND MINUTES, MOBILE TO MOBILE MINUTES, ANYTIME MINUTES AND ROLLOVER, EXCEPT THAT MINUTES THAT ARE PART OF BOTH A LIMITED PACKAGE AND AN UNLIMITED PACKAGE WILL NOT BE DEPLETED FROM THE LIMITED PACKAGE. Chargeable Time begins for outgoing calls when you press SEND (or similar key) and for incoming calls when a signal connection from the caller is established with our facilities. Chargeable Time ends after you press END (or similar key), but not until your wireless telephone's signal of call disconnect is received by our facilities and the call disconnect signal has been confirmed.

All outgoing calls for which we receive answer supervision or which have at least 30 seconds of Chargeable Time, including ring time, shall incur a minimum of one minute airtime charge. Answer supervision is generally received when a call is answered; however, answer supervision may also be generated by voicemail systems, private branch exchanges, and interexchange switching equipment. Chargeable Time may include time for us to recognize that only one party has disconnected from the call, time to clear the channels in use, and ring time. Chargeable Time may also occur from other uses of our facilities, including by way of example, voicemail deposits and retrievals, and call transfers. Calls that begin in one rate period and end in another rate period may be billed in their entirety at the rates for the period in which the call began.

DATA TRANSPORT OR USAGE IS CALCULATED IN FULL-KILOBYTE INCREMENTS, AND ACTUAL TRANSPORT OR USAGE IS ROUNDED UP TO THE NEXT FULL-KILOBYTE INCREMENT AT THE END OF EACH DATA SESSION FOR BILLING PURPOSES. AT&T CALCULATES A FULL KILOBYTE OF DATA TRANSPORT/USAGE FOR EVERY FRACTION OF THE LAST KILOBYTE OF DATA TRANSPORT/USAGE USED ON EACH DATA SESSION. TRANSPORT OR USAGE IS BILLED EITHER BY THE KILOBYTE ("KB") OR MEGABYTE ("MB"). IF BILLED BY MB, THE FULL KBs CALCULATED FOR EACH DATA SESSION DURING THE BILLING PERIOD ARE TOTALED AND ROUNDED UP TO NEXT FULL MB INCREMENT TO DETERMINE BILLING. IF BILLED BY KB, THE FULL KBs CALCULATED FOR EACH DATA SESSION DURING THE BILLING PERIOD ARE TOTALED TO DETERMINE BILLING. NETWORK OVERHEAD, SOFTWARE UPDATE REQUESTS, EMAIL NOTIFICATIONS, AND RESEND REQUESTS CAUSED BY NETWORK ERRORS CAN INCREASE MEASURED KILOBYTES. DATA TRANSPORT/USAGE OCCURS WHENEVER YOUR DEVICE IS CONNECTED TO OUR NETWORK AND IS ENGAGED IN ANY DATA TRANSMISSION, AS DISCUSSED IN MORE DETAIL IN SECTION 6.4.

If you select a rate plan that includes a predetermined allotment of Services (for example, a predetermined amount of airtime, megabytes or messages), unless otherwise specifically provided as a part of such rate plan, any unused allotment of Services from one billing cycle will not carry over to any other billing cycle. We may bill you in a format as we determine from time to time. Additional charges may apply for additional copies of your bill, or for detailed information about your usage of Services.

Delayed Billing: Billing of usage for calls, messages, data or other Services (such as usage when roaming on other carriers' networks, including internationally) may occasionally be delayed. Such usage charges may appear in a later billing cycle, will be deducted from Anytime monthly minutes or other Services allotments for the month when the usage is actually billed, and may result in additional charges for that month. Those minutes will be applied against your Anytime monthly minutes in the month in which the calls appear on your bill. You also remain responsible for paying your monthly Service fee if your Service is suspended for nonpayment. We may require payment by money order, cashier's check, or a similarly secure form of payment at our discretion.

1.6 Are Advance Payments And/Or Deposits Required?

We may require you to make deposits or advance payments for Services, which we may offset against any unpaid balance on your account. Interest won't be paid on advance payments or deposits unless required by law. We may require additional advance payments or deposits if we determine that the initial payment was inadequate. Based on your creditworthiness as we determine it, we may establish a credit limit and restrict Services or features. If your account balance goes beyond the limit we set for you, we may immediately interrupt or suspend Services until your balance is brought below the limit. Any charges you incur in excess of your limit become immediately due. If you have more than one account with us, you must keep all accounts in good standing to maintain Services. If one account is past due or over its limit, all accounts in your name are subject to interruption or termination and all other available collection remedies.

1.7 What if I fail to pay my AT&T Bill when it is due?

You agree that for each bill not paid in full by the due date, AT&T may charge and you will pay a late payment fee of $5.

You expressly authorize, and specifically consent to allowing, AT&T and/or its outside collection agencies, outside counsel, or other agents to contact you in connection with any and all matters relating to unpaid past due

charges billed by AT&T to you. You agree that, for attempts to collect unpaid past due charges, such contact may be made to any mailing address, telephone number, cellular phone number, e-mail address, or any other electronic address that you have provided, or may in the future provide, to AT&T. You agree and acknowledge that any e-mail address or any other electronic address that you provide to AT&T is your private address and is not accessible to unauthorized third parties. For attempts to collect unpaid charges, you agree that in addition to individual persons attempting to communicate directly with you, any type of contact described above may be made using, among other methods, pre-recorded or artificial voice messages delivered by an automatic telephone dialing system, pre-set e-mail messages delivered by an automatic e-mailing system, or any other pre-set electronic messages delivered by any other automatic electronic messaging system.

1.8 What Happens If My Check Bounces?

We'll charge you up to $30 (depending on applicable law) for any check or other instrument (including credit card charge backs) returned unpaid for any reason.

1.9 Are There Business or Government Benefits?

You may receive or be eligible for certain rate plans, discounts, features, promotions, and other benefits ("Benefits") through a business or government customer's agreement with us ("Business Agreement"). All such Benefits are provided to you solely as a result of the corresponding Business Agreement, and may be modified or terminated without notice. You may also be eligible for certain additional Services. Please see **http://www.wireless.att.com/businesscenter (http://www.wireless.att.com/businesscenter)** for such Services and the associated additional terms, which are hereby incorporated by reference.

If a business or government entity pays your charges or is otherwise liable for the charges, you authorize us to share your account information with it or its authorized agents. If you use Service(s) and/or receive certain Benefits tied to a Business Agreement with us, but you're liable for your own charges, then you authorize us to share enough account information with it or its authorized agents to verify your continuing eligibility for those Services or Benefits.

You may receive Benefits because of your agreement to have the charges for your Services, billed ("Joint Billing") by a wireline company affiliated with AT&T ("Affiliate") or because you subscribe to certain services provided by an Affiliate. If you cancel Joint Billing or the Affiliate service your rates will be adjusted without notice to a rate plan for which you qualify.

1.10 Who Can Access My Account and for What Purpose?

You authorize us to provide information about and to make changes to your account, including new or extended Service Commitments and the purchase of Products and/or Services, upon the direction of any person able to provide information we deem sufficient to identify you. In addition, you may designate individuals who are authorized to make certain changes to your account ("Authorized Users"). You are responsible for all changes made by such Authorized Users, including new or extended Service Commitments and the purchase of Products or Services. You consent to the use by us or our authorized agents of regular mail, predictive or autodialing equipment, email, text messaging, facsimile or other reasonable means to contact you to advise you about our Services or other matters we believe may be of interest to you. In any event, we reserve the right to contact you by any means regarding customer service-related notifications, or other such information.

2.0 HOW DO I RESOLVE DISPUTES WITH AT&T?

2.1 Dispute Resolution By Binding Arbitration

PLEASE READ THIS CAREFULLY. IT AFFECTS YOUR RIGHTS.

Summary:

Most customer concerns can be resolved quickly and to the customer's satisfaction by calling our customer service department at 1-800-331-0500. **In the unlikely event that AT&T's customer service department is unable to resolve a complaint you may have to your satisfaction (or if AT&T has not been able to resolve**

a dispute it has with you after attempting to do so informally), we each agree to resolve those disputes through binding arbitration or small claims court instead of in courts of general jurisdiction. Arbitration is more informal than a lawsuit in court. Arbitration uses a neutral arbitrator instead of a judge or jury, allows for more limited discovery than in court, and is subject to very limited review by courts. Arbitrators can award the same damages and relief that a court can award. **Any arbitration under this Agreement will take place on an individual basis; class arbitrations and class actions are not permitted.** For any non-frivolous claim that does not exceed $75,000, AT&T will pay all costs of the arbitration. Moreover, in arbitration you are entitled to recover attorneys' fees from AT&T to at least the same extent as you would be in court.

In addition, under certain circumstances (as explained below), AT&T will pay you more than the amount of the arbitrator's award and will pay your attorney (if any) twice his or her reasonable attorneys' fees if the arbitrator awards you an amount that is greater than what AT&T has offered you to settle the dispute.

2.2 Arbitration Agreement

(1) AT&T and you agree to arbitrate **all disputes and claims** between us. This agreement to arbitrate is intended to be broadly interpreted. It includes, but is not limited to:

- claims arising out of or relating to any aspect of the relationship between us, whether based in contract, tort, statute, fraud, misrepresentation or any other legal theory;
- claims that arose before this or any prior Agreement (including, but not limited to, claims relating to advertising);
- claims that are currently the subject of purported class action litigation in which you are not a member of a certified class; and
- claims that may arise after the termination of this Agreement.

References to "AT&T," "you," and "us" include our respective subsidiaries, affiliates, agents, employees, predecessors in interest, successors, and assigns, as well as all authorized or unauthorized users or beneficiaries of services or Devices under this or prior Agreements between us. Notwithstanding the foregoing, either party may bring an individual action in small claims court. This arbitration agreement does not preclude you from bringing issues to the attention of federal, state, or local agencies, including, for example, the Federal Communications Commission. Such agencies can, if the law allows, seek relief against us on your behalf. **You agree that, by entering into this Agreement, you and AT&T are each waiving the right to a trial by jury or to participate in a class action.** This Agreement evidences a transaction in interstate commerce, and thus the Federal Arbitration Act governs the interpretation and enforcement of this provision. This arbitration provision shall survive termination of this Agreement.

(2) A party who intends to seek arbitration must first send to the other, by certified mail, a written Notice of Dispute ("Notice"). The Notice to AT&T should be addressed to: Office for Dispute Resolution, AT&T, 1025 Lenox Park Blvd., Atlanta, GA 30319 ("Notice Address"). The Notice must (a) describe the nature and basis of the claim or dispute; and (b) set forth the specific relief sought ("Demand"). If AT&T and you do not reach an agreement to resolve the claim within 30 days after the Notice is received, you or AT&T may commence an arbitration proceeding. During the arbitration, the amount of any settlement offer made by AT&T or you shall not be disclosed to the arbitrator until after the arbitrator determines the amount, if any, to which you or AT&T is entitled. You may download or copy a form Notice and a form to initiate arbitration at **att.com/arbitration-forms (http://www.att.com/arbitration-forms)**.

(3) After AT&T receives notice at the Notice Address that you have commenced arbitration, it will promptly reimburse you for your payment of the filing fee, unless your claim is for greater than $75,000. (The filing fee currently is $200 for claims under $10,000 but is subject to change by the arbitration provider. If you are unable to pay this fee, AT&T will pay it directly upon receiving a written request at the Notice Address.) The arbitration will be governed by the Commercial Arbitration Rules and the Supplementary Procedures for Consumer Related Disputes (collectively, "AAA Rules") of the American Arbitration Association ("AAA"), as modified by this Agreement, and will be administered by the AAA. The AAA Rules are available online at **adr.org (http://www.adr.org)**, by calling the AAA at 1-800-778-7879, or by writing to the Notice Address. (You may obtain information that is designed for non-lawyers about the arbitration process at **att.com/arbitration-**

information (http://www.att.com/arbitration-information).) The arbitrator is bound by the terms of this Agreement. All issues are for the arbitrator to decide, except that issues relating to the scope and enforceability of the arbitration provision are for the court to decide. Unless AT&T and you agree otherwise, any arbitration hearings will take place in the county (or parish) of your billing address. If your claim is for $10,000 or less, we agree that you may choose whether the arbitration will be conducted solely on the basis of documents submitted to the arbitrator, through a telephonic hearing, or by an in-person hearing as established by the AAA Rules. If your claim exceeds $10,000, the right to a hearing will be determined by the AAA Rules. Regardless of the manner in which the arbitration is conducted, the arbitrator shall issue a reasoned written decision sufficient to explain the essential findings and conclusions on which the award is based. Except as otherwise provided for herein, AT&T will pay all AAA filing, administration, and arbitrator fees for any arbitration initiated in accordance with the notice requirements above. If, however, the arbitrator finds that either the substance of your claim or the relief sought in the Demand is frivolous or brought for an improper purpose (as measured by the standards set forth in Federal Rule of Civil Procedure 11(b)), then the payment of all such fees will be governed by the AAA Rules. In such case, you agree to reimburse AT&T for all monies previously disbursed by it that are otherwise your obligation to pay under the AAA Rules. In addition, if you initiate an arbitration in which you seek more than $75,000 in damages, the payment of these fees will be governed by the AAA rules.

(4) If, after finding in your favor in any respect on the merits of your claim, the arbitrator issues you an award that is greater than the value of AT&T's last written settlement offer made before an arbitrator was selected, then AT&T will:

- pay you the amount of the award or $10,000 ("the alternative payment"), whichever is greater; and
- pay your attorney, if any, twice the amount of attorneys' fees, and reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration ("the attorney premium").

If AT&T did not make a written offer to settle the dispute before an arbitrator was selected, you and your attorney will be entitled to receive the alternative payment and the attorney premium, respectively, if the arbitrator awards you any relief on the merits. The arbitrator may make rulings and resolve disputes as to the payment and reimbursement of fees, expenses, and the alternative payment and the attorney premium at any time during the proceeding and upon request from either party made within 14 days of the arbitrator's ruling on the merits.

(5) The right to attorneys' fees and expenses discussed in paragraph (4) supplements any right to attorneys' fees and expenses you may have under applicable law. Thus, if you would be entitled to a larger amount under the applicable law, this provision does not preclude the arbitrator from awarding you that amount. However, you may not recover duplicative awards of attorneys' fees or costs. Although under some laws AT&T may have a right to an award of attorneys' fees and expenses if it prevails in an arbitration, AT&T agrees that it will not seek such an award.

(6) The arbitrator may award declaratory or injunctive relief only in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by that party's individual claim. **YOU AND AT&T AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING.** Further, unless both you and AT&T agree otherwise, the arbitrator may not consolidate more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding. If this specific provision is found to be unenforceable, then the entirety of this arbitration provision shall be null and void.

(7) Notwithstanding any provision in this Agreement to the contrary, we agree that if AT&T makes any future change to this arbitration provision (other than a change to the Notice Address) during your Service Commitment, you may reject any such change by sending us written notice within 30 days of the change to the Arbitration Notice Address provided above. By rejecting any future change, you are agreeing that you will arbitrate any dispute between us in accordance with the language of this provision.

2.3 Puerto Rico Customers

For Puerto Rico customers, references to "small claims court" in sections 2.1 and 2.2 should be understood to mean the Puerto Rico Telecommunications Regulatory Board.

3.0 TERMS RELATING TO YOUR DEVICE AND CONTENT

3.1 Your Device

Your Device must be compatible with, and not interfere with, our Services and must comply with all applicable laws, rules, and regulations. We may periodically program your Device remotely with system settings for roaming service, to direct your Device to use network services most appropriate for your typical usage, and other features that cannot be changed manually.

You agree that you won't make any modifications to your Equipment or its programming to enable the Equipment to operate on any other system. AT&T may, at its sole and absolute discretion, modify the programming to enable the operation of the Equipment on other systems.

If you bought a Device from AT&T, it may have been programmed with a SIM lock which will prevent it from operating with other compatible wireless telephone carriers' services. If you wish to use this Device with the service of another wireless telephone carrier, you must enter a numeric Unlock Code to unlock the phone. AT&T will provide the Unlock Code upon request, provided that you meet certain criteria including, but not limited to the following: (a) you have paid for your Device in full; (b) your account has been active for at least sixty days and is in good standing (i.e. it has no past due amount or unpaid balance owed AT&T); (c) you have fulfilled your Service Commitment by expiration of any contractual term, upgrading to a new Device under AT&T's standard or early upgrade policies, or payment of any applicable ETF; (d) your Device has not been reported lost or stolen; and (e) AT&T has the Unlock Code or can reasonably obtain it from the manufacturer. AT&T will unlock a maximum of five phones per account, per year. For Devices sold with a Prepaid Plan, AT&T will provide you with the Unlock Code upon request if you provide a detailed receipt or other proof of purchase of the phone and AT&T has the Unlock Code or can reasonably obtain it from the manufacturer. For further details on eligibility requirements and for assistance on obtaining the Unlock Code for your handset, please call 1-800-331-0500 or visit an AT&T company store.

You are solely responsible for complying with U.S. Export Control laws and regulations and the import laws and regulations of foreign countries when traveling internationally with your Device.

3.2 Where and How Does AT&T Service Work?

AT&T does not guarantee availability of wireless network. Services may be subject to certain Device and compatibility/limitations including memory, storage, network availability, coverage, accessibility and data conversion limitations. Services (including without limitation, eligibility requirements, plans, pricing, features and/or service areas) are subject to change without notice.

When outside AT&T's coverage area, access will be limited to information and applications previously downloaded to or resident on your device. Coverage areas vary between AT&T network technologies. See coverage map(s), available at store or from your sales representative, for details or the coverage map at www.att.com/coverageviewer (http://www.att.com/coverageviewer).

Actual network speeds depend upon device characteristics, network, network availability and coverage levels, tasks, file characteristics, applications and other factors. Performance may be impacted by transmission limitations, terrain, in-building/in-vehicle use and capacity constraints.

3.3 What Information, Content, And Applications Are Provided By Third Parties?

Certain information, applications, or other content is provided by independently owned and operated content providers or service providers who are subject to change at any time without notice.

AT&T IS NOT A PUBLISHER OF THIRD-PARTY INFORMATION, APPLICATIONS, OR OTHER CONTENT AND IS NOT RESPONSIBLE FOR ANY OPINIONS, ADVICE, STATEMENTS, OR OTHER INFORMATION, SERVICES OR GOODS PROVIDED BY THIRD PARTIES.

Third-party content or service providers may impose additional charges. Policies regarding intellectual property, privacy and other policies or terms of use may differ among AT&T's content or service providers and you are bound by such policies or terms when you visit their respective sites or use their services. It is your responsibility to read the rules or service agreements of each content provider or service provider.

Any information you involuntarily or voluntarily provide to third parties is governed by their policies or terms. The accuracy, appropriateness, content, completeness, timeliness, usefulness, security, safety, merchantability, fitness for a particular purpose, transmission or correct sequencing of any application, information or downloaded data is not guaranteed or warranted by AT&T or any content providers or other third party. Delays or omissions may occur. Neither AT&T nor its content providers, service providers or other third parties shall be liable to you for any loss or injury arising out of or caused, in whole or in part, by your use of any information, application or content, or any information, application, or other content acquired through the Service.

You acknowledge that every business or personal decision, to some degree or another, represents an assumption of risk, and that neither AT&T nor its content and service providers or suppliers, in providing information, applications or other content or services, or access to information, applications, or other content underwrites, can underwrite, or assumes your risk in any manner whatsoever.

3.4 How Can I Get Mobile Content?

You understand that Devices can be used to acquire or purchase goods, content, and services (including subscription plans) like ring tones, graphics, games, applications and news alerts from AT&T or other companies ("Content"). You understand that you are responsible for all authorized charges associated with such Content from any Device assigned to your account, that these charges will appear on your bill (including charges on behalf of other companies), and that such purchases can be restricted by using parental controls available from an AT&T salesperson, or by calling AT&T.

You have full-time access to your Content purchase transaction history on our website. You may contest charges and seek refunds for purchases with which you are not satisfied. AT&T reserves the right to restrict Content purchases or terminate the account of anyone who seeks refunds on improper grounds or otherwise abuses this Service.

Actual Content may vary based on the Device capabilities. Content may be delivered in multiple messages. Content charges are incurred at the stated one-time download rate or subscription rate, plus a per kilobyte or per megabyte default pay per use charge for the Content transport when delivered, unless you have a data plan and such charges appear separately on your bill. You will be charged each time you download Content. Data Service charges apply.

3.5 Am I Responsible If Someone Makes A Purchase With My Device?

Except as otherwise provided in this Agreement, if your Device is used by others to make Content purchases, you are responsible for all such purchases. If this occurs, you are giving those other users your authority to:

1) make Content purchases from those Devices, and to incur charges for those Content purchases that will appear on your bill;

2) give consent required for that Content, including the consent to use that user's location information to deliver customized information to that user's Device; or

3) make any representation required for that content, including a representation of the user's age, if requested.

Usage by others can be restricted by use of parental controls or similar features. Visit **att.com/smartlimits (http://www.att.com/smartlimits)** to learn more.

3.6 Does AT&T Collect Location-Based Network Performance Information From My Device? Can I Use Location-Based Services With My Device?

AT&T collects information about the approximate location of your Device in relation to our cell towers and the Global Positioning System (GPS). We use that information, as well as other usage and performance information also obtained from our network and your Device, to provide you with wireless voice and data services, and to maintain and improve our network and the quality of your wireless experience. We may also use location information to create aggregate data from which your personally identifiable information has been removed or obscured. Such aggregate data may be used for a variety of purposes such as scientific and marketing research and services such as vehicle traffic volume monitoring. It is your responsibility to notify users on your account that we may collect and use location information from Devices.

Your Device is also capable of using optional Content at your request or the request of a user on your account, offered by AT&T or third parties that make use of a Device's location information ("Location-Based Services"). Please review the terms and conditions and the associated privacy policy for each Location-Based Service to learn how the location information will be used and protected. For more information on Location-Based Services, please visit **att.com/privacy (http://www.att.com/privacy)** .

Our directory assistance service (411) may use the location of a Device to deliver relevant customized 411 information based upon the user's request for a listing or other 411 service. By using this directory assistance service, the user is consenting to our use of that user's location information for such purpose. This location information may be disclosed to a third party to perform the directory assistance service and for no other purpose. Such location information will be retained only as long as is necessary to provide the relevant customized 411 information and will be discarded after such use. Please see our privacy policy at **att.com/privacy (http://www.att.com/privacy)** for additional details.

3.7 What If My Device Is Lost Or Stolen?

If your wireless Device is lost or stolen, you must contact us immediately to report the Device lost or stolen. You're not liable for charges you did not authorize, but the fact that a call was placed from your Device is evidence that the call was authorized. Once you report to us that the Device is lost or stolen, you will not be responsible for subsequent charges incurred by that Device.

You can report your Device as lost or stolen and suspend Services without a charge by contacting us at the phone number listed on your bill or at **wireless.att.com (http://www.wireless.att.com)** . If there are charges on your bill for calls made after the Device was lost or stolen, but before you reported it to us, notify us of the disputed charges and we will investigate. You may submit documents, statements and other information to show any charges were not authorized. You may be asked to provide information and you may submit information to support your claim. We will advise you of the result of our investigation within 30 days. While your phone is suspended you will remain responsible for complying with all other obligations under this Agreement, including, but not limited to, your monthly fee. We both have a duty to act in good faith in a reasonable and responsible manner including in connection with the loss or theft of your Device. (California Customers see Section 11.1 "California: What if there are Unauthorized Charges Billed to My Device?" below.)

4.0 TERMS RELATING TO THE USE AND LIMITATIONS OF SERVICE

4.1 What Are The Limitations On Service And Liability?

Unless prohibited by law, the following limitations of liability apply. Service may be interrupted, delayed, or otherwise limited for a variety of reasons, including environmental conditions, unavailability of radio frequency channels, system capacity, priority access by National Security and Emergency Preparedness personnel in the event of a disaster or emergency, coordination with other systems, equipment modifications and repairs, and problems with the facilities of interconnecting carriers. We may block access to certain categories of numbers (e.g., 976, 900, and international destinations) at our sole discretion.

Additional hardware, software, subscription, credit or debit card, Internet access from your compatible PC and/or special network connection may be required and you are solely responsible for arranging for or obtaining all such requirements. Some solutions may require third party products and/or services, which are subject to any applicable third party terms and conditions and may require separate purchase from and/or agreement with the

third party provider. AT&T is not responsible for any consequential damages caused in any way by the preceding hardware, software or other items/requirements for which you are responsible.

Not all plans or Services are available for purchase or use in all sales channels, in all areas or with all devices. AT&T is not responsible for loss or disclosure of any sensitive information you transmit. AT&T's wireless services are not equivalent to wireline Internet. AT&T is not responsible for nonproprietary services or their effects on devices.

We may, but do not have the obligation to, refuse to transmit any information through the Services and may screen and delete information prior to delivery of that information to you. There are gaps in service within the Services areas shown on coverage maps, which, by their nature, are only approximations of actual coverage.

WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE OR COVERAGE. WE CANNOT ASSURE YOU THAT IF YOU PLACE A 911 CALL YOU WILL BE FOUND. AIRTIME AND OTHER SERVICE CHARGES APPLY TO ALL CALLS, INCLUDING INVOLUNTARILY TERMINATED CALLS. AT&T MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY, SECURITY, OR PERFORMANCE REGARDING ANY SERVICES, SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE, for any:

(a) act or omission of a third party;
(b) mistakes, omissions, interruptions, errors, failures to transmit, delays, or defects in the Services or Software provided by or through us;
(c) damage or injury caused by the use of Services, Software, or Device, including use in a vehicle;
(d) claims against you by third parties;
(e) damage or injury caused by a suspension or termination of Services or Software by AT&T; or
(f) damage or injury caused by failure or delay in connecting a call to 911 or any other emergency service.

Notwithstanding the foregoing, if your Service is interrupted for 24 or more continuous hours by a cause within our control, we will issue you, upon request, a credit equal to a pro-rata adjustment of the monthly Service fee for the time period your Service was unavailable, not to exceed the monthly Service fee. Our liability to you for Service failures is limited solely to the credit set forth above.

Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software, or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries.

To the full extent allowed by law, you hereby release, indemnify, and hold AT&T and its officers, directors, employees and agents harmless from and against any and all claims of any person or entity for damages of any nature arising in any way from or relating to, directly or indirectly, service provided by AT&T or any person's use thereof (including, but not limited to, vehicular damage and personal injury), INCLUDING CLAIMS ARISING IN WHOLE OR IN PART FROM THE ALLEGED NEGLIGENCE OF AT&T, or any violation by you of this Agreement. This obligation shall survive termination of your Service with AT&T. AT&T is not liable to you for changes in operation, equipment, or technology that cause your Device or Software to be rendered obsolete or require modification.

SOME STATES, INCLUDING THE STATE OF KANSAS, DON'T ALLOW DISCLAIMERS OF IMPLIED WARRANTIES OR LIMITS ON REMEDIES FOR BREACH. THEREFORE, THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS AGREEMENT GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

4.2 How Can I Use My AT&T Service?

All use of AT&T's wireless network and Services is governed by AT&T's Acceptable Use Policy, which can be found at **att.com/AcceptableUsePolicy (http://www.att.com/AcceptableUsePolicy)**, as determined solely by AT&T. AT&T can revise its Acceptable Use Policy at any time without notice by updating this posting.

4.3 Who Is Responsible For Security?

AT&T DOES NOT GUARANTEE SECURITY. Data encryption is available with some, but not all, Services sold by AT&T. If you use your Device to access company email or information, it is your responsibility to ensure your use complies with your company's internal IT and security procedures.

4.4 How Can I Use the Software?

The software, interfaces, documentation, data, and content provided for your Equipment as may be updated, downloaded, or replaced by feature enhancements, software updates, system restore software or data generated or provided subsequently by AT&T (hereinafter "Software") is licensed, not sold, to you by AT&T and/or its licensors/suppliers for use only on your Equipment. Your use of the Software shall comply with its intended purposes as determined by us, all applicable laws, and AT&T's Acceptable Use Policy at **att.com/AcceptableUsePolicy (http://www.att.com/AcceptableUsePolicy)** .

You are not permitted to use the Software in any manner not authorized by this License. You may not (and you agree not to enable others to) copy, decompile, reverse engineer, disassemble, reproduce, attempt to derive the source code of, decrypt, modify, defeat protective mechanisms, combine with other software, or create derivative works of the Software or any portion thereof. You may not rent, lease, lend, sell, redistribute, transfer or sublicense the Software or any portion thereof. You agree the Software contains proprietary content and information owned by AT&T and/or its licensors/suppliers.

AT&T and its licensors/suppliers reserve the right to change, suspend, terminate, remove, impose limits on the use or access to, or disable access to, the Software at any time without notice and will have no liability for doing so. You acknowledge AT&T's Software licensors/suppliers are intended third party beneficiaries of this license, including the indemnification, limitation of liability, disclaimer of warranty provisions found in this Agreement.

4.5 How Can I Use Another Carrier's Network (Off-Net Usage)?

4.5.1 Voice

If your use of minutes (including unlimited Services) on other carrier networks ("off-net voice usage") during any two consecutive months exceed your off-net voice usage allowance, AT&T may, at its option, terminate your Services, deny your continued use of other carriers' coverage or change your plan to one imposing usage charges for off-net voice usage. Your off-net voice usage allowance is equal to the lesser of 750 minutes or 40% of the Anytime Minutes included with your plan.

4.5.2 Data

If your use of the Data Services on other carriers' wireless networks ("offnet data usage") during any month exceeds your offnet data usage allowance, AT&T may at its option terminate your access to Data Services, deny your continued use of other carriers' coverage, or change your plan to one imposing usage charges for offnet data usage. Your offnet data usage allowance is equal to the lesser of 24 megabytes or 20% of the kilobytes included with your plan. You may be required to use a Device programmed with AT&T's preferred roaming database.

4.5.3 Messaging

If you use messaging services (including unlimited Services) on other carrier networks ("off-net messaging usage") during any two consecutive months exceed your off-net messaging usage allowance, AT&T may, at its option, terminate your messaging service, deny your continued use of other carriers' coverage or change your plan to one imposing usage charges for off-net messaging usage. Your off-net messaging usage allowance is equal to the lesser of 3,000 messages or 50% of the messages included with your plan.

4.5.4 Notice

AT&T will provide notice that it intends to take any of the above actions, and you may terminate this Agreement.

4.6 How Do I Get Service Outside AT&T's Wireless Network (Roaming)?

Services originated or received while outside your plan's included coverage area are subject to roaming charges. Domestic roaming charges for wireless data or voice Services may be charged with some plans when outside AT&T's wireless network. International roaming rates apply for any voice, messaging or data usage incurred outside the U.S., Puerto Rico and U.S. Virgin Islands. Use of Services when roaming is dependent upon roaming carrier's support of applicable network technology and functionality. Display on your device may not indicate whether you will incur roaming charges. Check with roaming carriers individually for support and coverage details.

4.6.1 International Services

Certain eligibility restrictions apply which may be based on service tenure, payment history and/or credit. Rates are subject to change. For countries, rates and additional details, see **att.com/global (http://www.att.com/global)**.

4.6.1.1 **International Long Distance:**

International rates apply for calls made and messages sent from the U.S., Puerto Rico and U.S.V.I. to another country. Calling or messaging to some countries may not be available. Calls to wireless numbers and numbers for special services, such as Premium Rated Services, may cost more than calls to wireline numbers. If a customer calls an overseas wireline number and the call is forwarded to a wireless number, the customer will be charged for a call terminated to a wireless number. International Long Distance calling rates are charged per minute and apply throughout the same footprint in which the customer's airtime package minutes apply.

4.6.1.2 **International Long Distance Text, Picture & Video Messaging:**

Additional charges apply for premium messages and content. Messages over 300 KBs are billed an additional 50¢/message. For a complete list of countries, please visit **att.com/text2world (http://www.att.com/text2world)**.

4.6.1.3 **International Roaming:**

Compatible Device required. Your plan may include the capability to make and receive calls while roaming internationally. AT&T, in its sole discretion, may block your ability to use your Device while roaming internationally until eligibility criteria are met. International roaming rates, which vary by country, apply for all calls placed or received while outside the United States, Puerto Rico and U.S.V.I. Please consult **att.com/global (http://www.att.com/global)** or call 611 from your mobile device or 800-331-0500 for a list of currently available countries and carriers. All countries may not be available for roaming. All carriers within available countries may not be available on certain plans or packages. Availability, quality of coverage and services while roaming are not guaranteed. When roaming internationally, you will be charged international roaming airtime rates including when incoming calls are routed to voicemail, even if no message is left. Substantial charges may be incurred if Device is taken out of the U.S. even if no services are intentionally used. Billing for international roaming usage may be delayed up to three billing cycles due to reporting between carriers. Taxes are additional. If you want to block the ability to make and receive calls or use data functions while roaming internationally, you may request that by calling 1-916-843-4685 (at no charge from your wireless phone). For AT&T Canada and Mexico Travel Minutes, package and overage rates apply only in Canada or Mexico, and if you remove the package before your monthly bill cycle ends, the included monthly minutes allotment will be reduced proportionately.

4.6.1.4 **International Data:**

International data rates apply to all data usage outside the U.S., Puerto Rico and U.S.V.I., including accessing cloud-based services to upload/download/stream content. Many Devices, including iPhone, transmit and receive data messages without user intervention and can generate unexpected charges when powered "on" outside the United States, Puerto Rico and U.S.V.I. AT&T may send "alerts" via SMS or email, to notify you of data usage. These are courtesy alerts. There is no guarantee you will receive them. They are not a guarantee of a particular bill limit. Receipt of Visual Voicemail messages are charged at international data pay-per-use rates unless customer has an international data

plan/package, in which case receipt of Visual Voicemail messages decrement Kilobytes included in such plan/package.

4.6.1.5 **Data Global Add-Ons and Global Messaging Plans/Packages:**

Require that domestic data or messaging capability be in place. Rates apply only for usage within "roam zone" comprised of select carriers. Within the roam zone, overage rate applies if you exceed the MBs allotted for any Data Global Add-On or the messages allotted for any Global Messaging Plan/Package. International roaming pay-per-use rates apply in countries outside the roam zone. See **att.com/globalcountries (http://www.att.com/dataconnectglobal)** for current roam zone list.

4.6.1.6 **Data Connect Global/North America Plans:**

Do not include capability to place a voice call and require a 1 year agreement. For specific terms regarding international data plans, see Section 6.10.2 of the Wireless Customer Agreement.

4.6.1.7 **Cruise Ship Roaming:**

Cruise ship roaming rates apply for calls placed or data used while on the ship.

4.6.1.8 **International Miscellaneous**

Export Restrictions: You are solely responsible for complying with U.S. Export Control laws and regulations, and the import laws and regulations of foreign countries when traveling internationally with your Device.

5.0 WHAT VOICE SERVICES DOES AT&T OFFER?

5.1 What Are The General Terms That Apply To All AT&T Voice Rate Plans?

You may obtain usage information by calling customer service or using one of our automated systems. **Pricing/Taxes/No Proration:** Prices do not include taxes, directory assistance, roaming, Universal Service Fees, and other surcharges. Final month's charges are not prorated. **Activation Fees:** Activation Fee may apply for each new line. **Nights and Weekends:** Nights are 9:00 p.m. to 6:00 a.m. Weekends are 9:00 p.m. Friday to 6:00 a.m. Monday (based on time of day at the cell site or switch providing your Service). Included long distance calls can be made from the 50 United States, Puerto Rico and U.S. Virgin Islands to the 50 United States, Puerto Rico, U.S. Virgin Islands, Guam and Northern Mariana Islands. Roaming charges do not apply when roaming within the Services area of land-based networks of the 50 United States, Puerto Rico and U.S. Virgin Islands. Additional charges apply to Services used outside the land borders of the U.S., Puerto Rico and U.S. Virgin Islands.

5.2 Voicemail

Unless you subscribe to an Unlimited Voice Plan or are an upstate New York customer subscribing to Enhanced Voicemail, airtime charges apply to calls to your voicemail service, including calls where the caller does not leave a message, because the call has been completed, calls to listen to, send, reply to, or forward messages, or to perform other activities with your voicemail service, including calls forwarded from other phones to your voicemail service. You are solely responsible for establishing and maintaining security passwords to protect against unauthorized use of your voicemail service. For information as to the number of voicemail messages you can store, when voicemail messages will be deleted, and other voicemail features, see **att.com/wirelessvoicemail (http://www.att.com/wirelessvoicemail)**. We reserve the right to change the number of voicemails you can store, the length you can store voicemail messages, when we delete voicemail messages, and other voicemail features without notice. We may deactivate your voicemail service if you do not initialize it within a reasonable period after activation. We will reactivate the service upon your request. See **att.com/global (http://www.att.com/global)** for information about using voicemail internationally.

5.3 Voicemail-To-Text (VMTT)

AT&T is not responsible, nor liable for: 1) errors in the conversion of or its inability to transcribe voicemail messages to text/email; 2) lost or misdirected messages; or, 3) content that is unlawful, harmful, threatening, abusive, obscene, tortious, or otherwise objectionable.

We do not filter, edit or control voice, text, or email messages, or guarantee the security of messages. We can interrupt, restrict or terminate VMTT without notice, if your use of VMTT adversely impacts AT&T's network, for example that could occur from abnormal calling patterns or an unusually large number of repeated calls and messages; or if your use is otherwise abusive, fraudulent, or does not comply with the law.

You are solely responsible for and will comply with all applicable laws as to the content of any text messages or emails you receive from VMTT that you forward or include in a reply to any other person. You authorize AT&T or a third party working on AT&T's behalf to listen to, and transcribe all or part of a voicemail message and to convert such voicemail message into text/email, and to use voicemail messages and transcriptions to enhance, train and improve AT&T's speech recognition and transcription services, software and equipment.

Charges for VMTT include the conversion of the voicemail message and the text message sent to your wireless device. Additional charges, however, may apply to receiving email on your wireless device from VMTT, as well as, replying to or forwarding VMTT messages via SMS (text) or email, depending on your plan.

SMS (text messaging) blocking is incompatible with VMTT. (If you do not have a texting plan on your handset, we add a texting pay per use feature when you add VMTT with text delivery.) If you are traveling outside the U.S. coverage area, you will incur international data charges for emails received from VMTT, as well as, charges for emails you respond to or forward from VMTT, unless you have an international data plan and the usage falls within the plan's usage limits.

Transcription times cannot be guaranteed. Customers purchasing email delivery are responsible for providing a correct email address and updating the email address when changes to the email account are made.

If you choose SMS (text) delivery, VMTT only converts the first 480 characters of a voicemail message into text and you will receive up to three text messages of a transcribed message. The transcription, therefore, may not include the entire voicemail message with SMS delivery. Adding VMTT will create a new voicemail box and all messages and greetings will be deleted from your current voicemail box.

5.4 Unlimited Voice Services

Unlimited voice Services are provided primarily for live dialog between two individuals. If your use of unlimited voice Services for conference calling or call forwarding exceeds 750 minutes per month, AT&T may, at its option, terminate your Service or change your plan to one with no unlimited usage components.

Unlimited voice Services may not be used for monitoring services, data transmissions, transmission of broadcasts, transmission of recorded material, or other connections which don't consist of uninterrupted live dialog between two individuals. If AT&T finds that you're using an unlimited voice Service offering for other than live dialog between two individuals, AT&T may, at its option terminate your Service or change your plan to one with no unlimited usage components. AT&T will provide notice that it intends to take any of the above actions, and you may terminate the agreement.

5.5 Caller ID

Your caller identification information (such as your name and phone number) may be displayed on the Device or bill of the person receiving your call; technical limitations may, in some circumstances, prevent you from blocking the transmission of caller identification information. Contact customer service for information on blocking the display of your name and number. Caller ID blocking is not available when using Data Services, and your wireless number is transmitted to Internet sites you visit.

5.6 Rollover® Minutes

If applicable to your plan, Rollover Minutes accumulate and expire through 12 rolling bill periods. Bill Period 1 (activation) unused Anytime Minutes will not carry over. Bill Period 2 unused Anytime Minutes will begin to carry

over. Rollover Minutes accumulated starting with Bill Period 2 will expire each bill period as they reach a 12-bill-period age. Rollover Minutes will also expire immediately upon default or if customer changes to a non-Rollover plan. If you change plans (including the formation of a FamilyTalk plan), or if an existing subscriber joins your existing FamilyTalk plan, any accumulated Rollover Minutes in excess of your new plan or the primary FamilyTalk line's included Anytime Minutes will expire. Rollover Minutes are not redeemable for cash or credit and are not transferable. If you change to non-AT&T Unity plans with Rollover Minutes (including the formation of a FamilyTalk plan) any accumulated Rollover Minutes in excess of your new non-AT&T Unity plan or the primary non-AT&T Unity FamilyTalk line's included Anytime Minutes will expire.

5.7 Mobile To Mobile Minutes

If applicable to your plan, Mobile to Mobile Minutes may be used when directly dialing or receiving calls from any other AT&T wireless phone number from within your calling area. Mobile to Mobile Minutes may not be used for interconnection to other networks. Calls to AT&T voicemail and return calls from voicemail are not included.

5.8 Family Talk® Plan

If applicable to your plan, FamilyTalk may require up to a two-year Service Commitment for each line. FamilyTalk plans include only package minutes included with the primary number, and minutes are shared by the additional lines. The rate shown for additional minutes applies to all minutes in excess of the Anytime Minutes. FamilyTalk requires two lines. If the rate plan for the primary number is changed to an ineligible plan or the primary number is disconnected, one of the existing additional lines shall become the primary number on the rate plan previously subscribed to by the former primary number; if only one line remains, it shall be converted to the closest single line rate.

5.9 A-List®

A-List is available only with select Nation, FamilyTalk and Unity plans. Nation Plan and Individual Subscribers can place/receive calls to/from up to 5 (and FamilyTalk subscribers can place/receive calls to/from up to 10) wireline or wireless telephone numbers without being charged for airtime minutes. All qualifying lines on a FamilyTalk account share the same 10 A-List numbers. Only standard domestic wireline or wireless numbers may be added and A-List is only for domestic calls. Directory assistance, 900 numbers, chat lines, pay per call numbers, customer's own wireless or Voice Mail access numbers, numbers for call routing services and call forwarding services from multiple phones, and machine to machine numbers are not eligible. Depending on the PBX system, a private telephone system often serving businesses, AT&T may not be able to determine if your selected PBX A-List number is calling/receiving calls from your wireless number and airtime charges could apply. Forwarded calls will be billed based on the originating number, not the call forwarding number, and airtime charges may apply. Only voice calling is eligible. A-List number selections may only be managed online via MyWireless Account. Selected telephone numbers do not become active until 24 hours after added. AT&T reserves the right to block any A-List number and to reduce the amount of telephone numbers that can be used for A-List without notice. A-List is not eligible on Save/Promotional Plans.

5.10 AT&T Viva Mexico℠ ("Mexico Plan") & AT&T Nation®/FamilyTalk® With Canada ("Canada Plan")

Certain eligibility requirements apply. Anytime Minutes and Night and Weekend Minutes between Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, or Canada and your U.S. wireless coverage area if you subscribe to the Canada Plan, will be treated for billing purposes as calls to and from your U.S. wireless coverage area.

Calls made from or received in Mexico and Canada cannot exceed your monthly off-net usage allowance (the lesser of 750 min./mo. or 40% of your Anytime Minutes/mo.) in any two consecutive months. Calls made from or received in Mexico and Canada will not qualify as Mobile to Mobile Minutes. Special rates apply for data usage in Mexico and Canada. International long distance text, instant, picture and video messaging rates apply to messaging from the U.S. to Mexico and Canada and international roaming rates apply when such messages are sent from Mexico and Canada.

International Roaming charges apply when using voice and data Services outside Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, and Canada and your U.S. wireless coverage area, if you subscribe to the Canada Plan. International long distance charges apply when calling to areas outside Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, and Canada and your U.S. wireless coverage area if you subscribe to the Canada Plan.

Anytime Minutes are primarily for live dialog between two people. You may not use your Services other than as intended by AT&T and applicable law. Plans are for individual, non-commercial use only and are not for resale. Unlimited Microcell Calling feature cannot be used on accounts with Viva Mexico and Nation Canada calling plans.

5.11 AT&T Unity℠ And AT&T Unity℠-FamilyTalk® Plans Requirements

5.11.1 Eligibility Requirements:

AT&T local and wireless combined bill required. For residential customers, qualifying AT&T local plan from AT&T required. For business customers, qualifying AT&T local service plan required. Specific AT&T Services that qualify vary by location; see **att.com (http://www.att.com)** or call 1-800-288-2020. Certain business accounts are not eligible for Unity plans. Discounts on any other combined-bill wireless plans will be lost if an AT&T Unity plan is added to your combined bill. If an existing wireless plan is upgraded to an AT&T Unity plan, all discounts and promotions will be lost when subscribing to that plan.

5.11.2 AT&T Unity℠ Minutes:

AT&T Unity Calling Minutes may be used when directly dialing or receiving calls from any other eligible AT&T wireline or wireless phone number from within your calling area. Calls to AT&T voicemail and return calls from voicemail not included. AT&T Unity Minutes are not included when checking usage for the current billing period.

5.12 VoiceDial Services

Regular airtime charges apply. Mobile to Mobile Minutes do not apply. Calls to 911, 411, 611, 711 and international dialing cannot be completed with VoiceDial Services. Caller ID cannot be blocked. Caller ID will be delivered on calls, even if you have permanently blocked your name and number. For complete terms and conditions, see **att.com/voicedial (http://www.att.com/voicedial)**.

5.13 AT&T Messaging Unlimited with Mobile to Any Mobile Calling Feature

Available only with select Nation, FamilyTalk, and BusinessTalk plans and can be discontinued at anytime. Messaging Unlimited Plan required. Mobile to Any Mobile minutes only apply when you directly dial another U.S. mobile number or directly receive a call from another U.S. mobile phone number from within your calling area in the U.S., Puerto Rico, or U.S.V.I. Mobile to Any Mobile is not available with the AT&T Viva Mexico or AT&T Nation/FamilyTalk with Canada plans. Calls made through Voice Connect, calls to directory assistance, and calls to voicemail and return calls from voicemail are not included. Only numbers included in the wireless number database that AT&T uses will be treated as a call to a mobile number or a call received from a mobile number. So for example, Type 1 numbers belonging to other carriers and not included in the industry wireless LNP database, and numbers for which ports to wireless service have not yet completed, will not be treated as a call to a mobile number or a call received from a mobile number. Also calls made to and calls received from mobile toll-free numbers, mobile chat lines, mobile directory assistance, calling applications, numbers for call routing and call forwarding services, and machine to machine numbers are not included.

6.0 WHAT DATA AND MESSAGING SERVICES DOES AT&T OFFER?

6.1 What Are The General Terms That Apply To All Data And Messaging Plans?

AT&T provides wireless data and messaging Services, including but not limited to, features that may be used with Data Services and wireless content and applications ("Data Services"). The absolute capacity of the wireless

data network is limited; consequently, Data Services may only be used for permitted activities. Pricing and data allowances for Data Services are device dependent and based on the capabilities and capacity of each Device.

For Data Services with a monthly megabyte (MB) or gigabyte (GB) data allowance, once you exceed your monthly data allowance you will be automatically charged for overage as specified in the applicable rate plan. All data allowances, including overages, must be used in the billing period in which the allowance is provided. Unused data allowances will not roll over to subsequent billing periods.

AT&T data plans are designed for use with only one of the following distinct Device types: (1) Smartphones, (2) basic and Quick Messaging phones, (3) tablets, (4) LaptopConnect cards, (5) stand-alone Mobile Hotspot devices, and (6) Home Bases. A data plan designated for one type of device may not be used with another type of device. For example, a data plan designated for use with a basic phone or a Smartphone may not be used with a LaptopConnect card, tablet, or stand-alone Mobile Hotspot device, by tethering devices together, by SIM card transfer, or any other means. A data tethering plan, however, may be purchased for an additional fee to enable tethering on a compatible device. An Activation Fee may apply for each data line.

Consumer data plans do not allow access to corporate email, company intranet sites, and other business applications. Access to corporate email, company intranet sites, and/or other business applications requires an applicable Enterprise Data plan. Enterprise Email requires an eligible data plan and Device. Terms may vary depending on selected Enterprise Email solution.

AT&T RESERVES THE RIGHT TO TERMINATE YOUR DATA SERVICES WITH OR WITHOUT CAUSE, INCLUDING WITHOUT LIMITATION, UPON EXPIRATION OR TERMINATION OF YOUR WIRELESS CUSTOMER AGREEMENT.

6.2 What Are The Intended Uses Of AT&T's Wireless Data Service?

AT&T's wireless data network is a shared resource, which AT&T manages for the benefit of all of its customers so that they can enjoy a consistent, high-quality mobile broadband experience and a broad range of mobile Internet services, applications and content. However, certain activities and uses of the network by an individual customer or small group of customers can negatively impact the use and enjoyment of the network by others. Therefore, certain activities and uses of AT&T's wireless data service are permitted and others are prohibited. The terms and conditions of your use of AT&T's wireless data service are set forth below.

Permitted Activities. AT&T's wireless data services are intended to be used for the following permitted activities: (i) web browsing; (ii) email; and (iii) intranet access if permitted by your rate plan (for example, access to corporate intranets, email, and individual productivity applications like customer relationship management, sales force, and field service automation); (d) uploading and downloading applications and content to and from the Internet or third-party application stores, and (e) using applications and content without excessively contributing to network congestion.

You agree to use AT&T's wireless data services only for these permitted activities.

Prohibited Activities: AT&T's wireless data services are not intended to be used in any manner which has any of the following effects and such use is prohibited if it: (a) conflicts with applicable law, (b) hinders other customers' access to the wireless network, (c) compromises network security or capacity, (d) excessively and disproportionately contributes to network congestion, (e) adversely impacts network service levels or legitimate data flows, (f) degrades network performance, (g) causes harm to the network or other customers, (h) is resold either alone or as part of any other good or service, (i) tethers a wireless device to a computing device (such as a computer, Smartphone, eBook or eReader, media player, laptop, or other devices with similar functions) through use of connection kits, applications, devices or accessories (using wired or wireless technology) and you have not subscribed to a specific data plan designed for this purpose, or (j) there is a specific data plan required for a particular use and you have not subscribed to that plan.

The following specific uses of AT&T's wireless data service are prohibited:

- AT&T's wireless data services may not be used in any manner that defeats, obstructs or penetrates, or attempts to defeat, obstruct or penetrate the security measures of AT&T's wireless network or systems, or another entity's network or systems; that accesses, or attempts to access without authority, the accounts of

others; or that adversely affects the ability of other people or systems to use either AT&T's wireless services or other parties' Internet-based resources. For example, this includes, but is not limited to, malicious software or "malware" that is designed, intentionally or unintentionally, to infiltrate a network or computer system such as spyware, worms, Trojan horses, rootkits, and/or crimeware; "denial of service" attacks against a network host or individual user; and "spam" or unsolicited commercial or bulk email (or activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk e-mail).

- AT&T's wireless data services may not be used in any manner that has the effect of excessively contributing to network congestion, hindering other customers' access to the network, or degrading network performance by maintaining a sustained and continuous wireless data service connection or active wireless Internet connection. For example, this includes, but is not limited to, server devices or host computer applications such as continuous Web camera posts or broadcasts, automatic data feeds, or automated machine-to-machine connections; "auto-responders," "cancel-bots," or similar automated or manual routines that generate excessive amounts of traffic or that disrupt user groups or email use by others; use of the service as a substitute or backup for private lines or full-time or dedicated data connections; peer-to-peer (P2P) file sharing services; and software or other devices that maintain continuous active Internet connections when a connection would otherwise be idle or any "keep alive" functions, unless they adhere to AT&T data retry requirements (as may be modified from time to time).
- AT&T's wireless data services also may not be used with high bandwidth applications, services and content that are not optimized to work with AT&T's wireless data services and, therefore disproportionately and excessively contribute to network congestion. This includes, but is not limited to, redirecting television signals for viewing on computing devices, web broadcasting, and/or the operation of servers, telemetry devices, or supervisory control and data acquisition devices, unless they meet AT&T's wireless data services optimization requirements.

You agree not to use AT&T's wireless data services for any of these prohibited activities.

AT&T's Rights to Ensure Compliance. You agree that AT&T has the right to take any and all actions necessary to enforce this Section 6.2 if you use AT&T's wireless data services in any manner that is prohibited, including, but not limited to, the following actions:

- AT&T may modify, without advance notice, the permitted and prohibited activities, and the optimization requirements for your wireless data services;
- AT&T may engage in any reasonable network management practice to enhance customer service, to reduce network congestion, to adapt to advances and changes in technology, and/or to respond to the availability of wireless bandwidth and spectrum;
- AT&T may reduce your data throughput speeds at any time or place if your data usage exceeds an applicable, identified usage threshold during any billing cycle. AT&T will provide you with advance notice of the usage threshold applicable to your data plan, or any changes to the applicable usage threshold either by a bill insert, email, text message or other appropriate means;
- AT&T may use reasonable methods to monitor and collect customer usage information to better optimize the operation of the network. Details concerning the information that AT&T collects about its customers, and how it uses and protects that information are addressed in the AT&T Privacy Policy (see **att.com/privacy) (http://www.att.com/privacy)**;
- If you are an AT&T unlimited data plan customer, AT&T may migrate you from the unlimited data plan to a tiered data plan and bill you the appropriate monthly fees. We will provide you with notice of this change at least one billing cycle in advance either by a bill insert, email, text message, or other appropriate means;
- AT&T may interrupt, suspend, cancel or terminate your wireless data services without advance notice.

Unlimited Data Customers. If you are a grandfathered AT&T unlimited plan data service customer, you agree that "unlimited" means you pay a fixed monthly charge for wireless data service regardless of how much data you use. You further agree that "unlimited" does not mean that you can use AT&T's wireless data service in any way that you choose or for any prohibited activities, and that if you use your unlimited data plan in any manner that is prohibited, AT&T can limit, restrict, suspend or terminate your data service or switch you to a tiered data plan.

6.3 What Are The Voice And Data Plan Requirements?

A voice plan is required on all voice-capable Devices, unless specifically noted otherwise in the terms governing your plan.

An eligible tiered pricing data plan is required for certain Devices, including iPhones and other designated Smartphones. Eligible voice and tiered pricing data plans cover voice and data usage in the U.S. and do not cover International voice and data usage and charges. If it is determined that you are using a voice-capable Device without a voice plan, or that you are using an iPhone or designated Smartphone without an eligible voice and tiered data plan, AT&T reserves the right to switch you to the required plan or plans and bill you the appropriate monthly fees. In the case of the tiered data plan, you will be placed on the data plan which provides you with the greatest monthly data usage allowance. If you determine that you do not require that much data usage in a month, you may request a lower data tier at a lower monthly recurring fee.

6.4 How Does AT&T Calculate My Data Usage/Billing?

DATA TRANSPORT/USAGE OCCURS WHENEVER YOUR DEVICE IS CONNECTED TO OUR NETWORK AND IS ENGAGED IN ANY DATA TRANSMISSION, INCLUDING BUT NOT LIMITED TO: (i) SENDING OR RECEIVING EMAIL, DOCUMENTS, OR OTHER CONTENT, (ii) ACCESSING WEBSITES, OR (iii) DOWNLOADING AND USING APPLICATIONS. SOME APPLICATIONS, CONTENT, PROGRAMS, AND SOFTWARE THAT YOU DOWNLOAD OR THAT COMES PRE-LOADED ON YOUR DEVICE AUTOMATICALLY AND REGULARLY SEND AND RECEIVE DATA TRANSMISSIONS IN ORDER TO FUNCTION PROPERLY, WITHOUT YOU AFFIRMATIVELY INITIATING THE REQUEST AND WITHOUT YOUR KNOWLEDGE. FOR EXAMPLE, APPLICATIONS THAT PROVIDE REAL-TIME INFORMATION AND LOCATION-BASED APPLICATIONS CONNECT TO OUR NETWORK, AND SEND AND RECEIVE UPDATED INFORMATION SO THAT IT IS AVAILABLE TO YOU WHEN YOU WANT TO ACCESS IT. IN ADDITION, ANY ADVERTISEMENTS OR ADVERTISER-RELATED MESSAGES OR DATA DELIVERED TO YOUR DEVICE, EVEN IF DELIVERED TO AN APPLICATION, AS WELL AS ANY MESSAGES OR CONTENT THAT INITIATE IN RESPONSE TO AN ADVERTISEMENT, WILL COUNT TOWARD YOUR DATA USAGE. YOU WILL BE BILLED FOR ALL DATA TRANSPORT AND USAGE WHEN YOUR DEVICE IS CONNECTED TO OUR NETWORK, INCLUDING THAT WHICH YOU AFFIRMATIVELY INITIATE OR THAT WHICH RUNS AUTOMATICALLY IN THE BACKGROUND WITHOUT YOUR KNOWLEDGE, AND WHETHER SUCCESSFUL OR NOT. A DATA SESSION INITIATED ON THE AT&T NETWORK WILL CONTINUE ITS CONNECTION OVER THE AT&T NETWORK UNTIL THE DATA TRANSMISSION IS CONCLUDED, EVEN WHEN YOU CONNECT TO A WI-FI NETWORK DURING THE TRANSMISSION.

Unless designated for International or Canada use, prices and included use apply to access and use on AT&T's wireless network and the wireless networks of other companies with which AT&T has a contractual relationship within the United States and its territories (Puerto Rico and the U.S. Virgin Islands), excluding areas within the Gulf of Mexico.

Usage on networks not owned by AT&T is limited as provided in your data plan. Charges will be based on the location of the site receiving and transmitting service and not the location of the subscriber. Mobile Broadband and 4G access requires a compatible device.

Data Service charges paid in advance for monthly or annual Data Services are nonrefundable. Some Data Services may require an additional monthly subscription fee and/or be subject to additional charges and restrictions. Prices do not include taxes, directory assistance, roaming, universal services fees or other surcharges.

In order to assess your usage during an applicable billing period, you may obtain approximate usage information by calling customer service or using one of our automated systems.

6.5 Text Messaging And Picture/Video Messaging

If you do not enroll in a monthly recurring plan for messaging, data, or Video Share, you may have access to messaging, data, and video share services and be charged on a pay-per-use basis if you use those services.

Messages are limited to 160 characters per message. Premium text and picture/video messages are charged at their stated rates. Standard rates apply to all incoming messages when in the U.S. Different, non-standard per message charges apply to international messages sent from the U.S.

Text, Picture, and Video messages are charged when sent or received, whether read or unread, solicited or unsolicited. AT&T does not guarantee delivery of messages. Text, Picture, and Video messages, including downloaded content, not delivered within 3 days will be deleted. AT&T reserves the right to change this delivery period as needed without notification.

You are charged for each part of messages that are delivered to you in multiple parts. Picture/Video Messaging, data plan, and Text Messaging may need to be provisioned on an account in order to use Picture/Video Messaging. Some elements of Picture/Video messages may not be accessible, viewable, or heard due to limitations on certain wireless phones, PCs, or e-mail.

AT&T reserves the right to change the Picture/Video message size limit at any time without notification. Picture/Video Messaging pricing is for domestic messages only. When a single message is sent to multiple recipients, the sender is charged for one message for each recipient and each recipient is charged for the message received.

Text message notifications may be sent to non-Picture/Video Messaging subscribers if they subscribe to Text Messaging. You may receive unsolicited messages from third parties as a result of visiting Internet sites, and a per-message charge may apply whether the message is read or unread, solicited or unsolicited.

You agree you will not use our messaging services to send messages that contain advertising or a commercial solicitation to any person or entity without their consent. You will have the burden of proving consent with clear and convincing evidence if a person or entity complains you did not obtain their consent. Consent cannot be evidenced by third party lists you purchased or obtained. You further agree you will not use our messaging service to send messages that: (a) are bulk messages (b) are automatically generated; (c) can disrupt AT&T's network; (d) harass or threaten another person (e) interfere with another customer's use or enjoyment of AT&T's Services; (f) generate significant or serious customer complaints, (g) that falsify or mask the sender/originator of the message; or (h) violate any law or regulation. AT&T reserves the right, but is not obligated, to deny, disconnect, suspend, modify and/or terminate your messaging service or messaging services with any associated account(s), or to deny, disconnect, suspend, modify and/or terminate the account(s), without notice, as to anyone using messaging services in any manner that is prohibited. Our failure to take any action in the event of a violation shall not be construed as a waiver of the right to enforce such terms, conditions, or policies. Advertising and commercial solicitations do not include messaging that: (a) facilitates, completes, or confirms a commercial transaction where the recipient of such message has previously agreed to enter into with the sender of such message; or (b) provides account information, service or product information, warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient of such message.

6.6 AT&T My Media CLUB

Your enrollment gives you the option to receive text messages each week on music trivia, news and more. Every 30 days your subscription will be automatically renewed and new credits added to your account which can be used to buy ringtones and graphics through the MEdia Mall. Music, Voice, Sound Effect Tones, polyphonic ringtones & graphics are 1 credit. Unused credits expire at the end of each 30 day period. The 30 day period is not necessarily equivalent to a calendar month end or the billing cycle. You may terminate your subscription at any time by texting the word "STOP" to 7225. Any remaining credits will be available for the remainder of your subscription billing cycle. Savings claim based on price of Music Tones. Ringtone and graphics provided by independent providers.

6.7 Mobile Email

Requires e-mail account with compatible internet service provider and a downloaded or preloaded e-mail application for the wireless device. Access and use of Mobile Email is billed by total volume of data sent and received (in kilobytes) in accordance with your data plan. E-mail attachments cannot be sent, downloaded, read,

or forwarded on the mobile device. Only a paper clip icon appears indicating an attachment. You must view attachments from your PC. Upgrades to the application may be required in order to continue to use the Service. Wireless data usage charges will apply for downloading the application and any upgrades.

6.8 Mobile Video

Compatible Phone and eligible data plan required. Service not available outside AT&T's Mobile Broadband and 4G coverage areas. Premium content is charged at stated monthly subscription rates or at stated pay per view rates. Content rotates and is subject to withdrawal. Mobile Video is for individual use, not for resale, commercial purposes or public broadcast. Content can only be displayed on the device screen. No content may be captured, downloaded, forwarded, duplicated, stored, or transmitted. The content owner reserves and owns all content rights. All trademarks, service marks, logos, and copyrights not owned by AT&T are the property of their owners. Some Mobile Video content is intended for mature audiences and may be inappropriate for younger viewers. Parental guidance suggested. Use Parental Controls to restrict access to mature content. Content may be provided by independent providers, and AT&T is not responsible for their content. Providers may collect certain information from yor use for tracking and managing content usage.

6.9 AT&T Wi-Fi Services

AT&T Wi-Fi service use with a Wi-Fi capable wireless device is subject to the Terms of Services & Acceptable Use Policy ("Terms") found at att.com/attwifitosaup (http://www.att.com/attwifitosaup). Your use represents your agreement to those Terms, incorporated herein by reference. AT&T Wi-Fi Basic service is available at no additional charge to wireless customers with select Wi-Fi capable devices and a qualified data rate plan. Other restrictions may apply.

6.10 DataConnect Plans

6.10.1 What Are the General Terms that Apply to All DataConnect Plans?

A voice plan is not required with DataConnect plans.

We may, at our discretion, suspend your account if we believe your data usage is excessive, unusual or is better suited to another rate plan. If you are on a data plan that does not include a monthly MB/GB allowance and additional data usage rates, you agree that AT&T has the right to impose additional charges if you use more than 5 GB in a month; provided that, prior to the imposition of any additional charges, AT&T shall provide you with notice and you shall have the right to terminate your Data Service.

6.10.2 Data Global Add-On/DataConnect Global Plans/DataConnect North America Plans

Available countries, coverage and participating international carriers included in the "Select International Roam Zone" and "Select Canada/Mexico Roam Zone" vary from our generally available Canada/international wireless data roam zones and may not be as extensive. The Select International Roam Zone is restricted to select international wireless carrier(s). Select Canada/Mexico Roam Zone is restricted to select wireless carrier(s) and coverage areas within Canada and Mexico. See **att.com/dataconnectglobal (http://www.att.com/dataconnectglobal)** for a current list of participating carriers and eligible roam zones. With respect to the countries included in the Select International Roam Zone, you will be restricted from accessing Data Service through any non-participating Canada/international wireless carriers that may otherwise be included in our generally available Canada and international wireless data roam zones. With the DataConnect North America Plan, you will be restricted from accessing Data Service through any non-participating Canada/Mexico wireless carriers that may otherwise be included in our generally available Canada and international wireless data roam zones.

DATA GLOBAL ADD-ON- May only be used with eligible Equipment. Domestic data usage not included. Qualified domestic wireless data plan required. If combined with a wireless voice plan that includes international voice roaming, your international wireless voice roaming in countries included in the Global Data Add-On's Select International Roam Zone will be limited to the participating Canada/international wireless carriers and you will be restricted from voice roaming through any non-participating Canada/international

wireless carriers that may otherwise be included in our generally available Canada and international voice roam zones.

DATACONNECT GLOBAL/NORTH AMERICA PLANS - Requires minimum one-year Service Commitment and you must remain on the plan, for a minimum one-year term. Voice access is restricted and prohibited.

6.11 AT&T DataPlus℠/AT&T DataPro℠ Plans

6.11.1 AT&T Data Plans With Tethering

Tethering is a wireless or wired method in which your AT&T mobile device is used as a modem or router to provide a Internet Access connection to other devices, such as laptops, netbooks, tablets, smartphones, other phones, USB modems, network routers, mobile hotspots, media players, gaming consoles, and other data-capable devices. AT&T data plans with tethering enabled may be used for tethering your AT&T Mobile device to other devices. If you are on a data plan that does not include a monthly megabyte allowance and additional data usage rates, you agree that AT&T has the right to impose additional charges if you use more than 5 GB in a month; prior to the imposition of any additional charges, AT&T shall provide you with notice and you shall have the right to terminate your Service (early termination charges may apply).

6.11.2 Blackberry® Personal

Supports personal email access to up to 10 Internet email accounts. Users storing more than 1,000 emails or email older than 30 days, may have some emails automatically deleted. May not be used to access corporate email such as BlackBerry Enterprise Server.

6.11.3 Blackberry® Connect; Blackberry Enterprise; Blackberry International

Supports BlackBerry Enterprise Server™ for corporate access (valid Client Access License required), and personal email access to up to 10 Internet email accounts as per BlackBerry Personal. BlackBerry International requires a minimum one-year agreement.

6.12 GOOD Plan

Requires compatible Good Server and, as to each end user, a compatible Good Client Access License (CAL) for use with a qualifying AT&T data plan. Solution includes software, products and related services provided by Good Technology, Inc. ("Good"), which are subject to applicable Good terms and conditions. Good is solely responsible for all statements regarding, and technical support for, its software, products and services.

6.13 Microsoft® Direct Push

Requires compatible Microsoft® Exchange Server and, as to each end user, a compatible device, a Direct Push enabled email account, and a qualifying AT&T Data Plan. Plans include end user customer support from AT&T for compatible devices. AT&T does not sell, supply, install or otherwise support Microsoft® software, products or services (including without limitation, Exchange and Direct Push).

6.14 AT&T Mobile Share Plans (with Unlimited Talk and Text)

AT&T Mobile Share plans allow you to share a monthly allotment of domestic wireless data usage, along with unlimited domestic talk and texting services (for basic phones, quick messaging phones, smartphones, WHP Devices and Home Bases), among up to ten (10) 3G, HSPA+ or LTE Devices. You choose a specific allotment of monthly shared data usage for a monthly recurring charge and then pay an additional charge for each Device added to the Mobile Share plan you select. You must specifically identify the devices (the "Designated Devices") that will share your monthly allotment of data usage under the Mobile Share plan you select. If you add a WHP Device for unlimited talk only, it will be counted as one of the (10) Designated Devices under the Mobile Share plan. Designated Devices can include: smartphone(s), tablet(s), gaming device(s), modem(s), netbook(s), laptop (s), mobile hotspot(s), basic or quick messaging phone(s), WHP Device(s) or Home Base(s). If, during a billing period, your data usage exceeds the monthly allotment of data in the Mobile Share plan you select, you will automatically be charged for overage as specified in your rate plan. If, during a billing period, you do not use all

of the data allotment in the Mobile Share plan you select, you will forfeit that usage. Authorized users on the account may temporarily suspend data access for particular Device(s) during a specific billing cycle, but monthly charges for the suspended Device(s) will continue to apply. Tethering and/or mobile hotspot use is permitted with Mobile Share plans with capable Designated Devices; provided, however, that such use is limited to a maximum of five (5) simultaneous users per Device. An activation fee will be charged when converting from a prepaid or Session-Based plan to a Mobile Share plan or when you activate an additional Device on an existing Mobile Share plan. Access to corporate email, intranet sites and/or other business applications may be available for an additional monthly charge per Device. Discounts otherwise applicable to your Mobile Share rate plan do not apply to the additional monthly Device charge. Additional deposits and other restrictions may apply.

If you use a Mobile Share plan with any device that is not a Designated Data Device, for tethering or as a mobile hotspot with more than five (5) simultaneous users, or otherwise use the plan in any way that is inconsistent with its terms, you agree that AT&T may: (a) suspend or terminate service to the account; (b) place any non-complying Device on an appropriate Mobile Share plan; and/or (c) add any other required element of the plan.

6.15 AT&T Mobile Share - Data Plans (for Data-Only Devices)

AT&T Mobile Share – Data plans allow you to share a monthly allotment of domestic wireless data usage among up to ten (10) 3G, HSPA+ or LTE Devices (excluding smartphones and basic or quick messaging phones). You choose a specific allotment of monthly shared data usage for a monthly recurring charge and then pay an additional charge for each Device added to the Mobile Share - Data plan you select. You must specifically identify one or more eligible devices (the "Designated Data Devices") that will share your monthly allotment of data usage under the Mobile Share - Data plan you select. Designated Data Devices can include: tablet(s), gaming device(s), modem(s), netbook(s), laptop(s), or mobile hotspot(s). If, during a billing period, your data usage exceeds the monthly allotment of data in the Mobile Share - Data plan you select, you will automatically be charged for overage as specified in your rate plan. If, during a billing period, you do not use all of the data allotment in the Mobile Share - Data plan you select, you will forfeit that usage. Authorized users on the account may temporarily suspend data access for particular Designated Data Device(s) during a specific billing cycle, but monthly charges for the suspended Designated Data Device(s) will continue to apply. Tethering and/or mobile hotspot use is permitted with Mobile Share – Data plans with capable Designated Data Devices; provided, however, that such use is limited to a maximum of five (5) simultaneous users per Designated Data Device. An activation fee will be charged when converting from a prepaid or Session-Based plan to a Mobile Share - Data plan or when you activate an additional Designated Data Device on an existing Mobile Share - Data plan. Designated Data Devices that are capable of accessing corporate email, intranet sites and/or other business applications may do so for no additional monthly access charge. Discounts otherwise applicable to your Mobile Share - Data rate plan do not apply to the additional monthly Device charge. Additional deposits and other restrictions may apply.

If you use a Mobile Share - Data plan with a smartphone, with any device that is not a Designated Data Device, for tethering or as a mobile hotspot with more than five (5) simultaneous users, or otherwise use the plan in any way that is inconsistent with its terms, you agree that AT&T may: (a) suspend or terminate service to the account; (b) place any non-complying Device on an appropriate Mobile Share plan; and/or (c) add any other required element of the plan.

7.0 AT&T Wireless Home Services

7.1 AT&T Wireless Home Phone Service

AT&T Wireless Home Phone ("WHP") service utilizes mobile wireless gateway Equipment called an AT&T Wireless Home Phone device ("WHP Device") to which you connect a landline phone to place and receive calls over the AT&T wireless network. See Section 3.2 for more information about how AT&T wireless service works.

WHP service provides voice service only and requires that you subscribe to one of the following eligible wireless voice plan options: (1) Wireless Home Phone unlimited plan, (2) add a line to your FamilyTalk plan, or (3) add a WHP Device to your AT&T Mobile Share plan. If your WHP Device is used to roam on other carrier networks, AT&T's off-net usage restrictions apply. Text messaging, data services, features and international roaming are not supported by WHP service. If you use a wireless voice plan not designed for WHP service with your WHP

Device, AT&T reserves the right to switch you to an appropriate plan and bill you the associated fees for such plan.

911 calls are routed based on the wireless network's automatic location technology. You should expect to provide your location address to the emergency response center responsible for sending first responders (e.g. police, medical assistance, or fire) to your location. The WHP Device has battery backup power and will work in the event of a power outage. However, if you connect a landline phone to the WHP Device that itself requires external electric power to operate (e.g., a cordless phone), you will not be able to place and receive calls over that phone during a power outage.

7.2 Wireless Home Phone and Internet Service

AT&T Wireless Home Phone and Internet ("WHPI") service utilizes mobile wireless gateway Equipment called an AT&T Home Base ("Home Base"). The Home Base allows you to connect a landline phone to place and receive calls, and to connect up to eleven (11) Internet-capable devices (one (1) via Ethernet and ten (10) via Wi-Fi) to have mobile broadband Internet access over the AT&T wireless network. See Section 3.2 for more information about how AT&T wireless service works.

WHPI service requires that you subscribe to an eligible wireless voice and/or data plan to take advantage of one or both capabilities. Voice plan options include either a Home Base unlimited plan, or a line added to your FamilyTalk plan. Tiered data plan options allow you to share a monthly allotment of domestic wireless data usage among your connected internet-capable devices. If your data usage exceeds the monthly data allotment of the plan you select during a billing period, you automatically will be charged for overages as specified in your plan. If you do not use all of the monthly data allotment of the plan you select during a billing period, you forfeit that usage. You may also add your Home Base to your AT&T Mobile Share plan if the monthly allotment of domestic wireless data usage under your AT&T Mobile Share plan is 10 GB or more.

If your Home Base is used to roam on other carrier networks, AT&T's off-net usage restrictions apply. Messaging services and international roaming are not supported by WHPI service. If you use a wireless voice and/or data plan not designed for WHPI service with your Home Base, AT&T reserves the right to switch you to an appropriate plan and bill you the associated fees for such plan.

911 calls are routed based on the wireless network's automatic location technology. You should expect to provide your location address to the emergency response center responsible for sending first responders (e.g. police, medical assistance, or fire) to your location. The Home Base has battery backup power and will work in the event of a power outage. However, if you connect a landline phone to the Home Base that itself requires external electric power to operate (e.g., a cordless phone), you will not be able to place and receive calls over that phone during a power outage.

8.0 ARE THERE OTHER TERMS AND CONDITIONS THAT APPLY TO FEATURES AND APPLICATIONS?

Terms and conditions for certain features and applications are provided on the Device at the time of feature/application activation or first use. Certain features/applications will not be available in all areas at all times.

9.0 WHAT IS AT&T ROADSIDE ASSISTANCE & OPTIONAL AT&T MOBILE INSURANCE?

9.1 AT&T Roadside Assistance

AT&T Roadside Assistance ("RA") is an optional feature that costs $2.99/month per enrolled phone and is automatically billed to the wireless account. Customers may cancel at any time. New RA customers get the first 30 days for free. To cancel RA without incurring charges, contact AT&T by dialing 611 from your wireless phone within the first 30 days. RA covers up to four events per year with a maximum benefit of $50/event. Towing services are for mechanical problems only. RA service will be provided by Asurion Roadside Assistance Services, LLC, a licensed motor club, until October 12, 2012. After October 12, 2012, RA service will be provided by Allstate Insurance Company. Refer to the RA Welcome Kit for complete terms and conditions **wireless.att.com/learn/en_US/pdf/roadside_assistance.pdf (http://www.wireless.att.com/learn/en_US/pdf/roadside_assistance.pdf)**.

9.2 Optional AT&T Mobile Insurance

Mobile Insurance covers lost, stolen, damaged and out of warranty malfunctions. Enrollment must occur within 30 days of an activation or upgrade. Key terms include: 1. A monthly premium of $6.99/month per mobile number enrolled. 2. Each approved replacement is subject to a $50 (Tier 1), $125 (Tier 2), or a $199 (Tier 3) non-refundable deductible, depending on device. 3. Claims are limited to 2 within any consecutive 12 months with a maximum device value of $1500 per occurrence. 4. Replacement devices may be new or remanufactured and/or a different model. 5. You can cancel your coverage at any time and receive a pro-rated refund of your unearned premium. To view enrollment eligibility, complete terms and the applicable deductibles, visit www.att.com/mobileinsurance (http://www.att.com/mobileinsurance). AT&T Mobile Insurance is underwritten by Continental Casualty Company, a CNA company (CNA) and administered by Asurion Protection Services, LLC (In California, Asurion Protection Services Insurance Agency, LLC, CA Lic. #OD63161. In Puerto Rico, Asurion Protection Services of Puerto Rico, Inc.), CNA's licensed agent for the customers of AT&T. Eligibility varies by device. Terms and conditions are subject to change.

10.0 WHAT OTHER TERMS AND CONDITIONS APPLY TO MY WIRELESS SERVICE?

10.1 Intellectual Property

You must respect the intellectual property rights of AT&T, our third-party content providers, and any other owner of intellectual property whose protected property may appear on any website and/or dialogue box controlled by AT&T or accessed through the AT&T's websites. Except for material in the public domain, all material displayed in association with the Service is copyrighted or trademarked. Except for personal, non-commercial use, trademarked and copyrighted material may not be copied, downloaded, redistributed, modified or otherwise exploited, in whole or in part, without the permission of the owner. The RIM and BlackBerry families of related marks, images and symbols are the exclusive properties and trademarks or registered trademarks of Research In Motion Limited - used by permission. Good, the Good logo and GoodLink are trademarks of Good Technology, Inc., in the United States and/or other countries. Good Technology, Inc., and its products and services are not related to, sponsored by or affiliated with Research In Motion Limited. All other marks contained herein are the property of their respective owners.

©2012 AT&T Intellectual Property. All rights reserved. AT&T, AT&T logo and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. Apple iPhone: ™ and © 2010 Apple Inc. All rights reserved. Apple is a trademark of Apple Inc., registered in the U.S. and other countries. iPhone is a trademark of Apple Inc.

10.2 Severability

If any provision of this Agreement is found to be unenforceable by a court or agency of competent jurisdiction, the remaining provisions will remain in full force and effect. The foregoing does not apply to the prohibition against class or representative actions that is part of the arbitration clause; if that prohibition is found to be unenforceable, the arbitration clause (but only the arbitration clause) shall be null and void.

10.3 Assignment; Governing Law; English Language

10.3.1 Assignment

AT&T may assign this Agreement, but you may not assign this Agreement without our prior written consent.

10.3.2 Governing Law

The law of the state of your billing address shall govern this Agreement except to the extent that such law is preempted by or inconsistent with applicable federal law. In the event of a dispute between us, the law of the state of your billing address at the time the dispute is commenced, whether in litigation or arbitration, shall govern except to the extent that such law is preempted by or inconsistent with applicable federal law.

10.3.3 English Language

The original version of this Agreement is in the English language. Any discrepancy or conflicts between the English version and any other language version will be resolved with reference to and by interpreting the English version.

10.4 Lifeline Services

As part of a federal government program, AT&T offers discounted wireless service to qualified low-income residents in selected states. For questions or to apply for Lifeline service, call 1-800-377-9450. Puerto Rico customers should contact 1-787-405-5463. For tips on how to protect against fraud, please visit the CPUC's website at, **CalPhoneInfo.com (http://www.CalPhoneInfo.com)**.

10.5 Trial Services

Trial Services are subject to the terms and conditions of this Agreement; may have limited availability; and may be withdrawn at any time.

10.6 NOTICE REGARDING TRANSMISSION OF WIRELESS EMERGENCY ALERTS (Commercial Mobile Alert Service)

AT&T has chosen to offer wireless emergency alerts within portions of its service area, as defined by the terms and conditions of its Agreement, on wireless emergency alert capable devices.

There is no additional charge for these wireless emergency alerts. Wireless emergency alerts may not be available on all devices or in the entire service area, or if a subscriber is outside of the AT&T service area. In areas in which the emergency alerts are transmitted, such alerts may not be received by a subscriber or user of AT&T's wireless service even though the subscriber has a device capable of receiving them.

For details on the availability of this service and wireless emergency alert capable devices, please ask a sales representative, or go to **att.com (http://www.att.com)** and click the Wireless Emergency Alerts link. This notice is required by FCC Rule 47 C.F.R. § 10.250 (Commercial Mobile Alert Service).

In transmitting emergency alerts pursuant to federal law, AT&T, including its officers, directors, employees, vendors, and agents, shall not be liable to any subscriber to, or user of, AT&T's wireless service or equipment for any act or omission related to or any harm resulting from the transmission of, or the failure to transmit, an emergency alert; or the release to a government entity or agency, public safety, fire service, law enforcement official, emergency medical service, or emergency facility of subscriber information used in connection with delivering an emergency alert.

11.0 WHAT TERMS APPLY ONLY TO SPECIFIC STATES?

11.1 California: What If There Are Unauthorized Charges Billed To My Device?

You are not liable for charges you did not authorize, but the fact that a call was placed from your Device is evidence that the call was authorized. Unauthorized charges may include calls made to or from your phone or other Device after it was lost or stolen. Once you report to us that the Device is lost or stolen and your Device is suspended, you will not be responsible for subsequent charges incurred by that Device. You can report your Device as lost or stolen and suspend Services without a charge by contacting us at the phone number listed on your bill or at **wireless.att.com (http://www.wireless.att.com)**.

If you notify us of any charges on your bill you claim are unauthorized, we will investigate. If there are charges on your bill for calls made after the Device was lost or stolen, but before you reported it to us, notify us of the disputed charges and we will investigate. You may submit documents, statements and other information to show any charges were not authorized. We will advise you of the result of our investigation within 30 days. If you do not agree with the outcome, you may file a complaint with the California Public Utilities Commission and you may have other legal rights. While an investigation is underway, you do not have to pay any charges you dispute or associated late charges, and we will not send the disputed amount to collection or file an adverse credit report about it. While your phone is suspended you will remain responsible for complying with all other obligations

under this Agreement, including but not limited to, your monthly fee. We both have a duty to act in good faith and in a reasonable and responsible manner including in connection with the loss or theft of your Device.

11.2 Connecticut: Questions About Your Service

If you have any questions or concerns about your AT&T Service, please call Customer Care at 1-800-331-0500, dial 611 from your wireless phone, or visit **att.com/wireless (http://www.att.com/wireless)**. If you have questions about the Unlimited Local or Unlimited Long Distance Service, please call 1-800-288-2020 or visit **att.com (http://www.att.com)**. If you are a Connecticut customer and we cannot resolve your issue, you have the option of contacting the Department of Public Utility Control (DPUC). Online: **state.ct.us/dpuc (http://www.state.ct.us/dpuc)**; Phone: 1-866-381-2355; Mail: Connecticut DPUC, 10 Franklin Square, New Britain, CT 06051.

11.3 Puerto Rico

If you are a Puerto Rico customer and we cannot resolve your issue, you may notify the Telecommunications Regulatory Board of Puerto Rico of your grievance. Mail: 500 Ave Roberto H. Todd, (Parada 18), San Juan, Puerto Rico 00907-3941; Phone: 1-787-756-0804 or 1-866-578-5500; Online: **jrtpr.gobierno.pr (http://www.jrtpr.gobierno.pr)**, in addition to having available arbitration, as provided in Section 2.0.

Return to Table of Contents (http://www.att.com/shop/en/legalterms.html?toskey=wirelessCustomerAgreement-list)

EXHIBIT 9

FILED
[redacted]
U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

~~TOP SECRET//HCS//COMINT//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]	Docket Number: PR/TT [redacted]

OPINION AND ORDER

This matter comes before the Court on an application of the Government for authority for the National Security Agency (NSA) to collect information regarding e-mail and certain other forms of Internet communications under the pen register and trap and trace provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846. This application seeks authority for a

Derived from: Pleadings in the above-captioned docket
Declassify on: [redacted]

much broader type of collection than other pen register/trap and trace applications and therefore presents issues of first impression.[1] For that reason, it is appropriate to explain why the Court concludes that the application should be granted as modified herein.

Accordingly, this Opinion and Order sets out the bases for the Court's findings that: (1) the collection activities proposed in the application involve the installation and use of "pen registers" and/or "trap and trace devices" as those terms are used in FISA, 50 U.S.C. §§ 1841-1846; (2) the application, which specifies restrictions on the retention, accessing, use, and dissemination of information obtained from these collection activities, "satisfies the requirements" of 50 U.S.C. § 1842 for the issuance of an order "approving the installation and use of a pen register or trap and trace device," id. § 1842(d)(1), subject to modifications stated herein;[2] and (3) the installation and use of these pen registers and/or trap and trace devices pursuant to

---

[1] The application was filed in two steps: an application filed on [redacted] followed by an addendum filed on [redacted] For ease of reference, the following discussion refers to both submissions collectively as the application.

[2] The Court has authority in this case to "enter an ex parte order as requested, or as modified." 50 U.S.C. § 1842(d)(1).

this Opinion and Order will comply with the First and Fourth Amendments.

In making these findings, the Court relies on factual representations made in the application, which was submitted by the Attorney General as applicant and verified by the Director of the NSA (DIRNSA); in the separate declaration of the DIRNSA (Attachment A to the application); and in the declaration of the [redacted] (Attachment B to the application). The Court has given careful consideration to the arguments presented in the Government's memorandum of law and fact (Attachment C to the application).

By letter dated [redacted] the Court directed the Government to respond to two questions necessary to its ruling on this application. The Court relies on the Government's responses to these questions, which were provided in a letter submitted on [redacted]

The Court also relies on information and arguments presented in a briefing to the Court on [redacted] which addressed the current and near-term threats posed by [redacted]

[3] One of these questions concerned First Amendment issues presented by the application. The other concerned the length of time that the Government expected the collected information to retain operational significance. These questions and the Government's responses are discussed more fully below.

[redacted] investigations conducted by the Federal Bureau of Investigation (FBI) to counter those threats, the proposed collection activities of the NSA (now described in the instant application), the expected analytical value of information so collected in efforts to identify and track operatives [redacted] and the legal bases for conducting these collection activities under FISA's pen register/trap and trace provisions.[4]

The principal statutory issues in this matter are whether the proposed collection constitutes the installation and use of "pen registers" and/or "trap and trace devices" and, if so, whether the certification pursuant to 50 U.S.C. § 1842(c)(2) is adequate. These issues are addressed below.

I. THE PROPOSED COLLECTION IS A FORM OF PEN REGISTER AND TRAP AND TRACE SURVEILLANCE.

For purposes of 50 U.S.C. §§ 1841-1846, FISA adopts the definitions of "pen register" and "trap and trace device" set out

[4] This briefing was attended by (among others) the Attorney General; [redacted] the DIRNSA; the Director of the FBI; the Counsel to the President; the Assistant Attorney General for the Office of Legal Counsel; the Director of the Terrorist Threat Integration Center (TTIC); and the Counsel for Intelligence Policy.

in 18 U.S.C. § 3127. See 50 U.S.C. § 1841(2). Section 3127 gives the following definitions:

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business;
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

These definitions employ three other terms - "electronic communication," "wire communication," and "contents" - that are themselves governed by statutory definitions "set forth for such terms in section 2510" of title 18. 18 U.S.C. § 3127(1). Section 2510 defines these terms as follows:

(1) "Electronic communication" is defined at 18 U.S.C. § 2510(12) as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole

or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication."[5]

(2) "Wire communication" is defined at 18 U.S.C. § 2510(1) as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

(3) "Contents" is defined at 18 U.S.C. § 2510(8) to "include[] any information concerning the substance, purport, or meaning" of a "wire, oral, or electronic communication."[6]

While the definitions of "pen register" and "trap and trace device" each contain several elements, the application of these

---

[5] The other exclusions to this definition at § 2510(12)(B)-(D) are not relevant to this case.

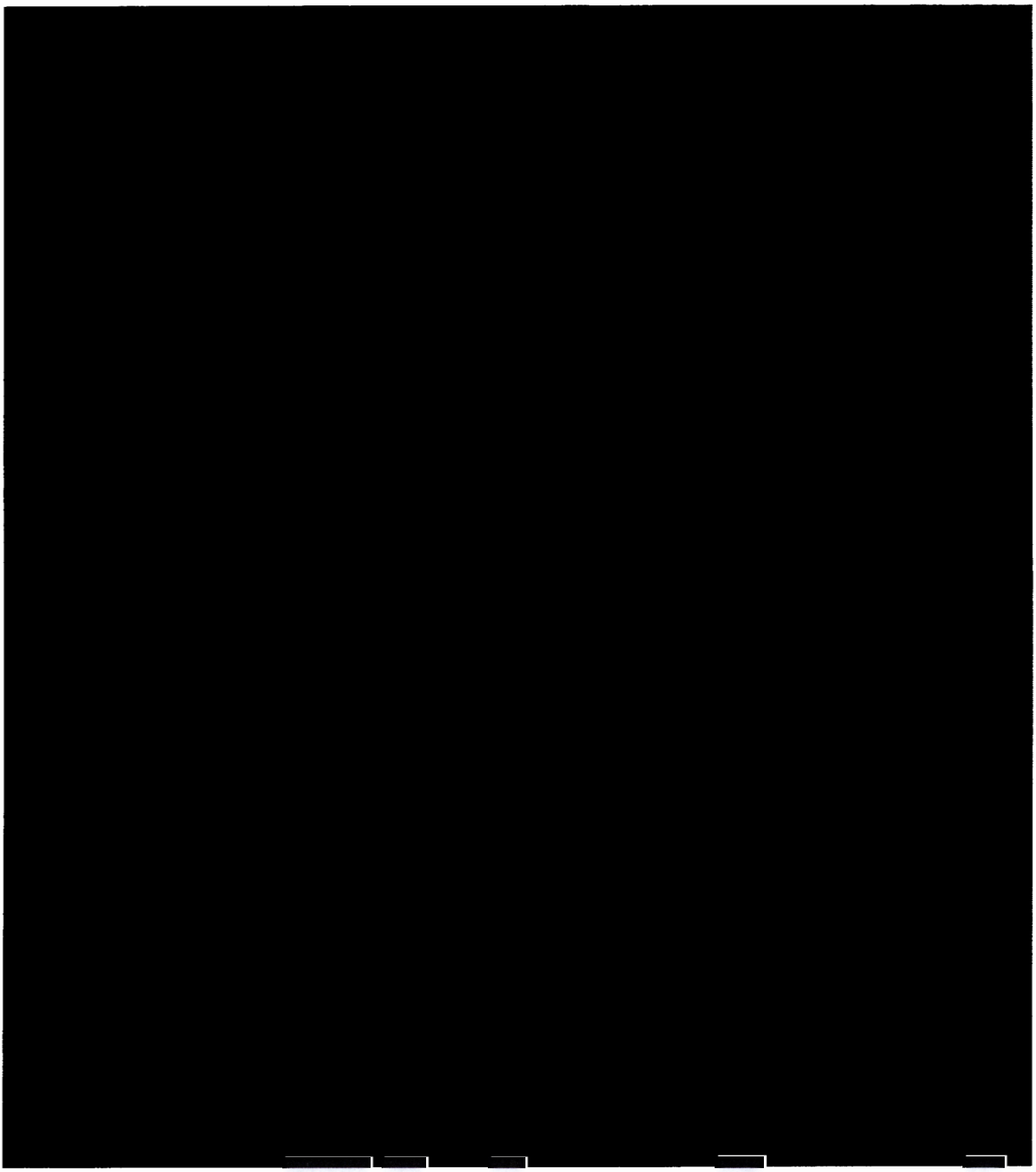
[6] Different definitions of "wire communication" and "contents" are provided at 50 U.S.C. § 1801(l), (n). However, the definitions set forth in § 1801 apply to terms "[a]s used in this subchapter," i.e., in 50 U.S.C. §§ 1801-1811 (FISA subchapter on electronic surveillance), and thus have no bearing on the meaning of "wire communication" and "contents" as used in the definitions of "pen register" and "trap and trace device" applicable to §§ 1841-1846 (separate FISA subchapter on pen registers and trap and trace devices).

definitions to the devices described in the application presents two primary questions: (1) Does the information to be obtained constitute "dialing, routing, addressing, or signaling information" that does not include the "contents" of any communication? (2) Does the means by which such information would be obtained come within the definition of "pen register" or "trap and trace device?" In addressing these questions, the Court is mindful that "when the statute's language is plain, the sole function of the courts - at least where the disposition required by the text is not absurd - is to enforce it according to its terms." Lamie v. United States Trustee, 124 S. Ct. 1023, 1030 (2004) (internal quotations and citations omitted).

A. The Information to Be Obtained Is "Dialing, Routing, Addressing, or Signaling Information" and Not "Contents."

The Government uses the umbrella term "meta data" to designate the categories of information it proposes to collect. This meta data comprises [redacted] categories:

[redacted]



~~TOP SECRET//HCS//COMINT//NOFORN~~





[redacted]

Also, the address from which an e-mail was sent and [redacted] are not part of the e-mail's "contents."

---

[8] This is the first application presented to this Court for authority to [redacted] under pen register/trap and trace authority. The Court understands that FBI devices implementing prior pen register/trap and trace surveillance authorized by this Court have not obtained [redacted] See Memorandum of Law and Fact at 23-24 n.14. The fact that prior applications did not seek authority for this specific form of collection sheds no light on the merits of the instant application.

[redacted] but this isolated fact does not provide "information concerning the substance, purport, or meaning" of the e-mail. 18 U.S.C. § 2510(8).[9]

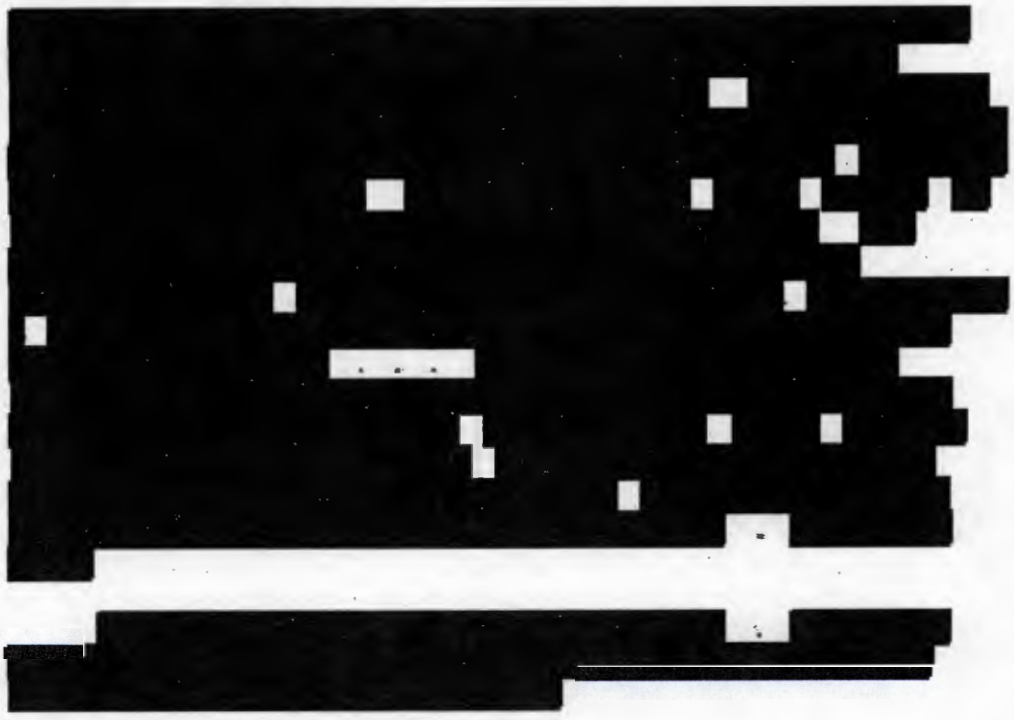
The DIRNSA Declaration mentions other types of information that are not described in the application as forms of meta data to be collected.[10] The Court understands such references to pertain to information or inferences that could be gleaned from accumulating meta data in Categories [redacted] above and/or analyzing meta data, perhaps in conjunction with information from other sources. This Opinion and Order authorizes only the collection of information in Categories [redacted]

[9] The finding that the [redacted] meta data do not constitute "content" is also supported by the assurance that meta data "does not include information from either the `subject' or 're' line of the E-mail [redacted] DIRNSA Declaration at 3 n.1.

[10] These references in the DIRNSA Declaration include [redacted] at 12, and information said to pertain to elements of [redacted]

B. The Methods By Which NSA Proposes to Obtain This Information Involve the Use of "Pen Registers" and "Trap and Trace Devices."

NSA proposes to obtain meta data in the above-described Categories [redacted]



[redacted]

Because the application of the definitions of "pen register" and "trap and trace device" to this means of collection involves a similar analysis for meta data in Categories [redacted], these groups of information are discussed separately below.

1. The Methods of Collecting Categories [redacted] Fall Within the Plain Meaning of the Statutory Definitions.

The above-described means of collecting information in Categories [redacted] satisfies each of the elements of the applicable statutory definition of a "pen register." It consists of "a device or process which records or decodes" non-content routing or addressing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). [redacted]

[redacted]

[11] "Transmit" means "1. To convey or dispatch from one person, thing, or place to another. . . . 4. *Electron.* To send (a signal), as by wire or radio." Webster's II New College Dictionary 1171 (2001).

[redacted]

Finally, the proposed collection does not involve "any device or process used . . . for billing, or recording as an incident to billing, for communications services . . . or . . . for cost accounting or other like purposes," which is excluded from the definition of "pen register" under section 3127(3).

Accordingly, based on "the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose," Engine Mfrs. Ass'n v. South Coast Air Quality Mgmt. Dist., 124 S. Ct. 1756, 1761 (2004) (internal quotations and citation omitted), the Court concludes that the means by which the NSA proposes to collect

---

[12] For ease of reference, this Opinion and Order generally speaks of "electronic communications." The communication involved will usually be an "electronic communication" under the above-quoted definition at 18 U.S.C. § 2510(12). In the event that the communication consists of an "aural transfer," i.e., "a transfer containing the human voice at any point between and including the point of origin and the point of reception," id. § 2510(18), then it could fall instead under the above-quoted definition of "wire communication" at § 2510(1). In either case, the communication would be "a wire or electronic communication," as required to fall within the definitions at §§ 3127(3) and 3127(4).

meta data in Categories [redacted] above falls under the definition of "pen register" at section 3127(3).

The application also seeks authority to collect at least some of the same meta data by the same means under the rubric of a "trap and trace device" as defined at section 3127(4). Although it appears to the Court that all of the collection authorized herein comes within the definition of "pen register," the Court additionally finds that such collection, as it pertains to meta data in Categories [redacted] (for example, information from the "from" line of an e-mail), also satisfies the definition of "trap and trace device" under section 3127(4).

Under section 3127(4), a "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other [non-content] dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." As discussed above, the proposed collection would use a device or process to obtain non-content meta data [redacted]

[redacted] Thus, based on the plain meaning of

---

[13] "Capture" is defined as, inter alia, " . . . 3. To succeed in preserving in a permanent form." Webster's II New College Dictionary 166 (2001).

[redacted]

[redacted]

Such a result could be argued to violate the "cardinal principle of statutory construction that we must give effect, if possible, to every clause and word of a statute." Williams v. Taylor, 529 U.S. 362, 404 (2000) (internal quotations and citation omitted).

[redacted]

the applicable definitions, the proposed collection involves a form of both pen register and trap and trace surveillance.

[redacted]

[redacted] The Court accordingly finds that the plain meaning of sections 3127(3) and 3127(4) encompasses the proposed collection of meta data.

Alternatively, the Court finds that any ambiguity on this point should be resolved in favor of including this proposed collection within these definitions, since such an interpretation would promote the purpose of Congress in enacting and amending FISA regarding the acquisition of non-content addressing information. Congress amended FISA in 1998, and again in 2001,

to relax the requirements for Court-authorized surveillance to obtain non-content addressing information through pen register and trap-and-trace devices, recognizing that such information is not protected by the Fourth Amendment. See page 29 below. As part of the USA PATRIOT Act in 2001, Congress also amended FISA to provide for Court orders for the production of "any tangible things," such as business records, under the same relevance standard as was adopted for pen register/trap and trace authorizations. See Pub. L. No. 107-56, Title II, § 215, 115 Stat. 290, codified at 50 U.S.C. § 1861.

[redacted] like other forms of meta data, is not protected by the Fourth Amendment because users of e-mail do not have a reasonable expectation of privacy in such information. See pages 59-62 below. It is a form of non-content addressing information, which Congress has determined should receive a limited form of statutory protection under a relevance standard if obtained through pen register/trap and trace devices pursuant to 50 U.S.C. § 1842, and/or through compelled production of business records (e.g., toll records for long-distance phone calls) under 50 U.S.C. § 1861.

A narrow reading of the definitions of "pen register" and "trap-and-trace device" to exclude [redacted] would

remove this particular type of non-content addressing information from the statutory framework that Congress specifically created for it. Based on such a narrow interpretation, this information could not be collected through pen register/trap and trace surveillance, even where it unquestionably satisfies the relevance standard. Nor could this information be obtained under the business records provision, because it is not generally retained by communications service providers. See page 41 below.

There is no indication that Congress believed that the availability of non-content addressing information under the relevance standard should hinge on the technical means of collection. If anything, the legislative history, see 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Patrick Leahy) (supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"), and the adoption of an identical relevance standard for the production of business records and other tangible things under section 1861, suggest otherwise.

Accordingly, the Court alternatively finds that, if the application of sections 3127(3) and 3127(4) to the [redacted] were thought to be ambiguous, such

ambiguity should be resolved in favor of an interpretation of the definitions of "pen register" and "trap and trace device" that encompasses the proposed collection.

3. The Proposed Collection is Consistent With Other Provisions of FISA

Nothing that is fairly implied by other provisions of FISA governing pen register and trap and trace surveillance would prevent authorization of the proposed collection as a form of pen register/trap and trace surveillance. One provision requires that an order authorizing a pen register or trap and trace surveillance specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(A)(ii). Plainly, there is no requirement to state the identity of such a person if it is not "known." However, this provision might still be read to imply that Congress expected that such facilities would be leased or listed to some particular person, even if the identity of that person were unknown in some cases. However, even if Congress had such a general expectation, the language of the statute does not require that there be such a person for every facility to which a pen register or trap and trace device is to be attached or applied. Drawing the contrary conclusion

from the wording of § 1842(d)(2)(A)(ii) would make the applicability of the statute depend on the commercial or administrative practices of particular communications service providers - a result that here would serve no apparent purpose of Congress. Cf. Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding that the "fortuity of whether or not the phone company elects to make [for its own commercial purposes] a quasi-permanent record of a particular number dialed" is irrelevant to whether the Fourth Amendment applies to use of a pen register).[16]

In this case [redacted]

[redacted]

[16] Similarly, for purposes of the subchapter on pen register/trap and trace surveillance, FISA defines an "aggrieved person," in relevant part, as any person "whose communication instrument or device was subject to the use of a pen register or trap and trace device . . . to capture incoming electronic or other communications impulses." 50 U.S.C. § 1841(3)(B). The term "whose" suggests a relationship between some person and "a communication instrument or device" that was "subject to the use of a pen register or trap and trace device." [redacted] Indeed, the use of different language implies that these phrases can refer to different objects, so that the definition of "aggrieved person" sheds no light on whether a "facility" under § 1842(d)(2)(A)(ii)-(iii) is necessarily associated with an individual user.

[redacted] The Court is satisfied that this Opinion and Order complies with the specification requirements of § 1842(d)(2)(A).

The Court recognizes that, by concluding that these definitions do not restrict the use of pen registers and trap and trace devices to communication facilities associated with individual users, it is finding that these definitions encompass an exceptionally broad form of collection. Perhaps the opposite result would have been appropriate under prior statutory language.[17] However, our "starting point" must be "the existing

[17] Prior to amendments in 2001 by the USA PATRIOT Act, Public Law 107-56, Title II, § 216(c), 18 U.S.C. § 3127(3) defined "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached," and § 3127(4) defined "trap and trace device" as a "device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C.A. § 3127(3), (4) (2000). Despite this textual focus on telephone communications, especially in § 3127(3), many (though not all) courts expansively construed both definitions to apply as well to e-mail communications. Memorandum of Law and [illegible] at 25-26 & n.16; Orin S. Kerr, Internet Surveillance Law

(continued...)

statutory text," not "predecessor statutes," Lamie, 124 S. Ct. at 1030, and analysis of that text shows that collecting information in Categories [redacted] above by the means described in the application involves use of "pen registers" and "trap and trace devices."[18]

Of course, merely finding that the proposed collection falls within these definitions does not mean that the requirements for an order authorizing such collection have been met. We turn now to those requirements.

---

[17](...continued)
After the USA PATRIOT Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 633-36 (2003). Extending these prior definitions to bulk collection regarding e-mail communications would have required further departure from the pre-USA PATRIOT Act statutory language.

[18] The legislative history of the USA PATRIOT Act indicates that Congress sought to make the definitions of "pen register" and "trap and trace device" "technology neutral" by confirming that they apply to Internet communications. See footnote 45 below. It does not suggest that Congress specifically gave thought to whether the new definitions would encompass collection in bulk from communications facilities that are not associated with individual users. The silence of the legislative history on this point provides no basis for departing from the plain meaning of the current definitions. See Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 495 n.13 (1985).

II. THE STATUTORY REQUIREMENTS FOR ISSUING AN ORDER AUTHORIZING THE PROPOSED PEN REGISTER AND TRAP AND TRACE SURVEILLANCE HAVE BEEN MET.

Under FISA's pen register/trap and trace provisions:

> Notwithstanding any other provision of law, the Attorney General . . . may make an application for an order . . . authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the [FBI] under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

50 U.S.C. § 1842(a)(1). This authority "is in addition to the authority . . . to conduct . . . electronic surveillance" under §§ 1801-1811. Id. § 1842(a)(2).

> Such applications shall include, inter alia, a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.

Id. § 1842(c)(2). "Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register

or trap and trace device if the judge finds that the application satisfies the requirements of [§ 1842]." Id. § 1842(d)(1).

Obviously, the application has been made by the Attorney General, § 1842(a)(1), has been approved by the Attorney General, § 1842(c), and has been submitted in writing and under oath to a judge of this Court. § 1842(b)(1). The application, at 5, identifies the DIRNSA as "the Federal officer seeking to use the pen register or trap and trace device." § 1842(c)(1).

The application also contains a certification by the Attorney General, at 26, containing the language specified in § 1842(c)(2). The Government argues that FISA prohibits the Court from engaging in any substantive review of this certification. In the Government's view, the Court's exclusive function regarding this certification would be to verify that it contains the words required by § 1842(c)(2); the basis for a properly worded certification would be of no judicial concern. See Memorandum of Law and Fact at 28-34.

The Court has reviewed the Government's arguments and authorities and does not find them persuasive.[19] However, in

---

[19] For example, the Government cites legislative history that "Congress intended to 'authorize[] FISA judges to issue a pen register or trap and trace order upon a certification that the information sought is relevant to'" an FBI investigation. (continued...)

this case the Court need not, and does not, decide whether it would be obliged to accept the applicant's certification without any explanation of its basis. Arguing in the alternative, the Government has provided a detailed explanation of 1) the threat currently posed by [redacted] 2) the reason the bulk collection described in the application is believed necessary as a means for NSA [redacted] 3) how that information will contribute to FBI investigations to protect against [redacted] and 4) what safeguards will be observed to ensure that the information collected will not be used for unrelated purposes or

---

[19](...continued)
Memorandum of Law and Fact at 30 (quoting S. Rep. No. 105-185, at 27 (1998). However, authorizing the Court to issue an order when a certification is made, and requiring it to do so without resolving doubts about the correctness of the certification, are quite different.

The Government also cites United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990), in arguing that the Court should not review the basis of the certification. However, the Hallmark court reserved the analogous issue under Title 18 - "the precise nature of the court's review under 18 U.S.C. § 3123" of the relevancy certification in an application for a law enforcement pen register or trap and trace device - and expressed "no opinion as to whether the court may, for instance, inquire into the government's factual basis for believing the pen register or trap and trace information to be relevant to a criminal investigation." Id. at 402 n.3.

otherwise misused. The Government also provides legal arguments that, under these specific circumstances, the proposed collection satisfies the relevancy requirement of § 1842(c)(2), despite its resulting in the collection of meta data from an enormous volume of communications, the large majority of which will be unrelated to international terrorism. In view of this record, the Court will assume for purposes of this case that it may and should consider the basis of the certification under § 1842(c)(2).

Nonetheless, the Court is mindful that FISA does not require any finding of probable cause in order for pen register and trap and trace surveillance to be authorized. In this regard, the statutory provisions that govern this case contrast sharply with those that apply to other forms of electronic surveillance and physical search.[20] Before Congress amended FISA in 1998 to add §§ 1841-1846, this Court could authorize pen register and trap and trace surveillance only upon the same findings as would be required to authorize interception of the full contents of

---

[20] To issue an electronic surveillance order, the Court must find "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power" and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3). Similar probable cause findings are required for warrants authorizing physical search under id. § 1824(a)(3).

communications. See S. Rep. 105-185, at 27 (1998). When it originally enacted §§ 1841-1846 in 1998, Congress recognized that pen register and trap and trace information is not protected by the Fourth Amendment and concluded that a lower standard for authorization "was necessary in order to permit, as is the case in criminal investigations, the use of this very valuable investigative tool at the critical early stages of foreign intelligence and international terrorism investigations." Id. These 1998 provisions included a form of a "reasonable suspicion" standard for pen register/trap and trace authorizations.[21] As part of the USA PATRIOT Act in 2001, Congress lowered the standard again, to the current requirement of relevance.[22] Given this history, it is obvious that Congress intended pen register

---

[21] Under the provisions enacted in 1998, a pen register or trap and trace application had to include "information which demonstrates that there is reason to believe" that a communication facility "has been or is about to be used in communication with," inter alia, "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities." Public Law 105-272 § 601(2).

[22] The legislative history of the USA PATRIOT Act reflects that, "in practice," the standard passed in 1998 was "almost as burdensome as the requirement to show probable cause required . . . for more intrusive techniques" and that the FBI "made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations." 147 Cong. Rec. S11003 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

and trap and trace authorizations to be more readily available than authorizations for electronic surveillance to acquire the full contents of communications.

The Court also recognizes that, for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats[23] and in determining the potential significance of intelligence-related information.[24] Such deference is particularly

---

[23] See, e.g., Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471, 491 (1999) ("a court would be ill equipped to determine [the] authenticity and utterly unable to assess [the] adequacy" of the executive's security or foreign policy reasons for treating certain foreign nationals as "a special threat"); Regan v. Wald, 468 U.S. 222, 243 (1984) (giving "the traditional deference to executive judgment" in foreign affairs in sustaining President's decision to restrict travel to Cuba against a Due Process Clause challenge); cf. Department of Navy v. Egan, 484 U.S. 518, 529 (1988) (outside body reviewing executive branch decisions on eligibility for security clearances could not "determine what constitutes an acceptable margin of error in assessing the potential risk").

[24] The Supreme Court has observed that, in deciding whether disclosing particular information might compromise an intelligence source, what "may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotation and citation omitted). Accordingly, the decisions of [redacted] "who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential

(continued...)

appropriate in this context, where the Court is not charged with making independent probable cause findings.

A. The Government Has Provided Information In Support of the Certification of Relevance.

In support of the certification of relevance, the Government relies on the following facts and circumstances:

1. The Threat Currently Posed [redacted]

[redacted]

[24](...continued)
risks at stake." Id. at 179.

[25] For simplicity, this opinion standardizes the variant spellings of foreign names appearing in different documents submitted in support of the application.

[redacted]

[redacted]

[redacted]

2. FBI Investigations to Track and Identify [redacted] in the United States

[redacted]

[redacted]

3. The Use of the Internet by [redacted]

[redacted]

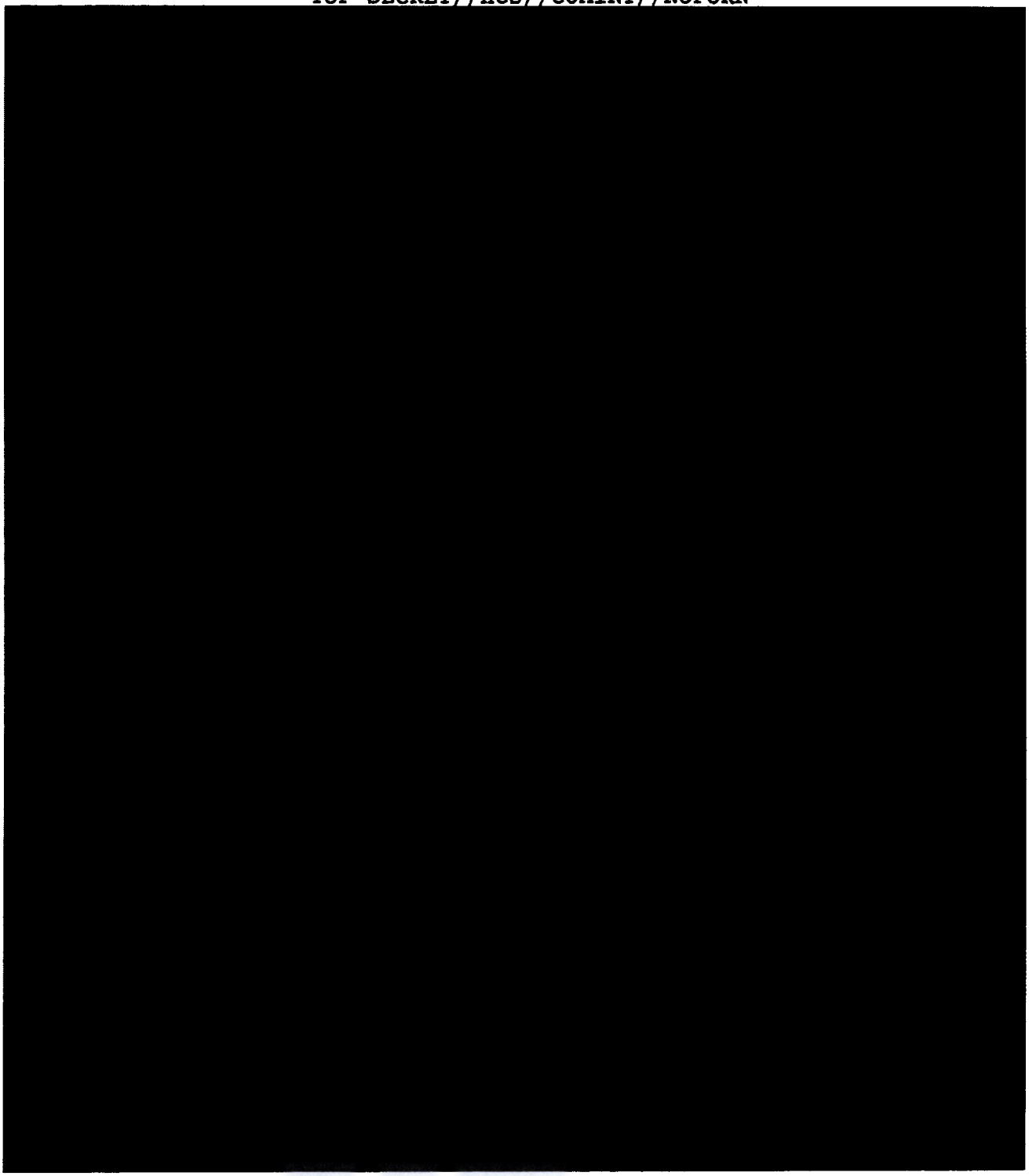
[redacted]

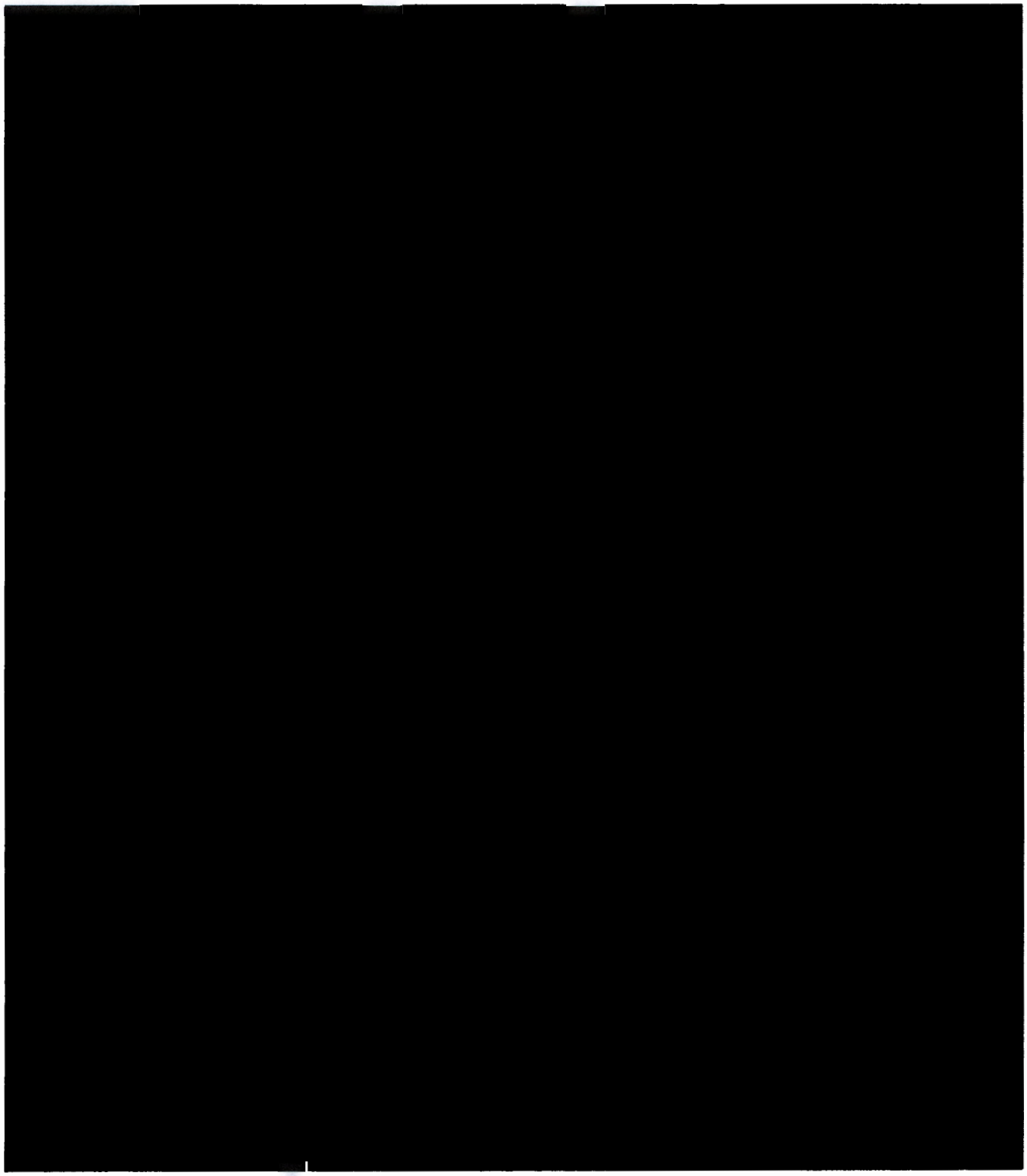
4. The Scope of the Proposed Collection of Meta Data

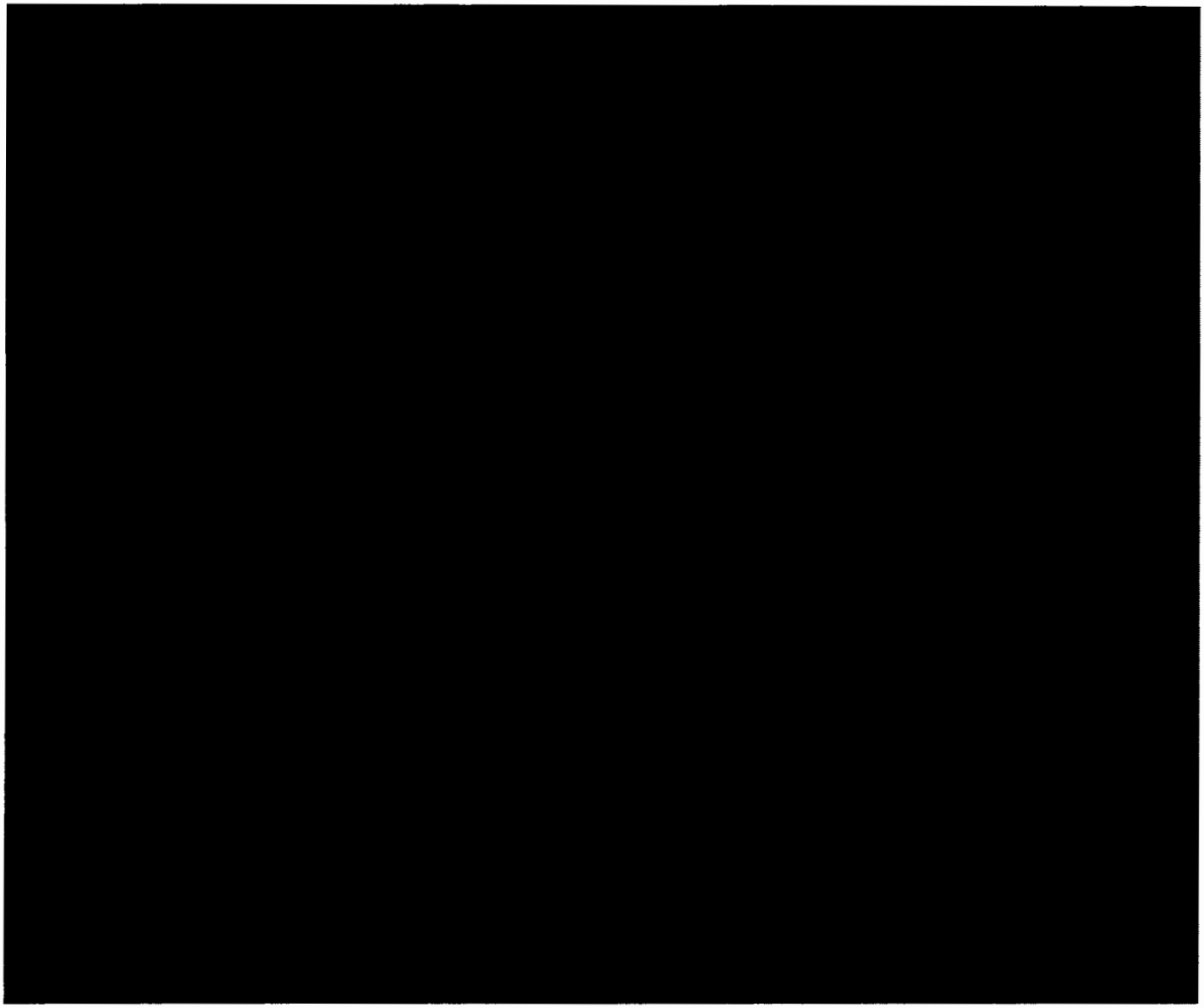
In an effort both to identify unknown and to track known operatives [redacted] through their Internet communications, NSA seeks to acquire meta data, as described above, from all e-mail [redacted] are described in detail in the application and the DIRNSA Declaration. In brief, they are:

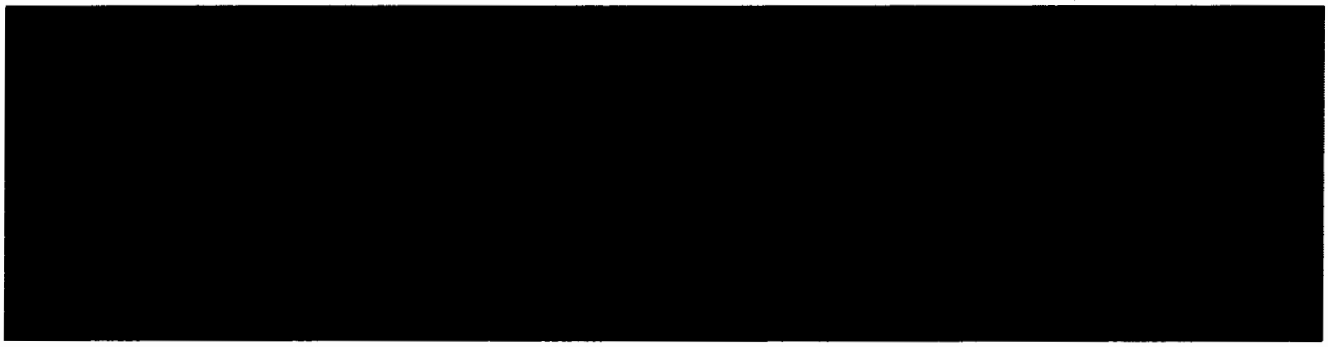
[redacted]

[27] For ease of reference, the term [redacted] is used to mean [redacted]









[redacted]

The raw volume of the proposed collection is enormous. NSA estimates that this collection will encompass [redacted] In absolute terms, the proposed surveillance "will result in the collection of meta data pertaining to [redacted] electronic communications, including meta data pertaining to communications of United States persons located within the United States who are not the subject of any FBI investigation." Application at 4. Some proportion of these communications - less than half, but still a huge number in absolute terms - can be expected to be communications [redacted]

[redacted] who bear no relation to [redacted]

[redacted]

5. How NSA Proposes to Use this Data to Track Known [redacted]

As noted above, the purpose of this collection is to track known operatives and to identify unknown operatives of [redacted] through their Internet communications. NSA

---

[29] As noted above, collection of meta data from [redacted]

[redacted]

states that even identified operatives [redacted]

[redacted]

Through the proposed bulk collection, NSA would acquire an archive of meta data for large volumes of communications that, in NSA's estimation, represent a relatively rich environment for finding [redacted] communications through later analysis.[31]

[31] See DIRNSA Declaration at 5 [redacted]

NSA asserts that more precisely targeted forms of collection against known accounts would tend to screen out the "unknowns" that NSA wants to discover, so that NSA needs bulk collection in order to identify unknown [redacted] communications. See id. at 14 ("It is not possible . . . to target collection solely to known terrorist E-mail accounts and at the same time use the advantages of meta data analysis to discover the enemy."), 15 ("To be able to fully exploit meta data, the data must be collected in bulk. Analysts know that terrorists' E-mails are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where.")

NSA proposes to employ two analytic methods on the body of archived meta data it seeks to collect. Both these methods involve querying the archived meta data regarding a particular "seed" account. In the Government's proposal, an account would qualify as a seed account only if NSA concludes, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted]

[redacted]

[redacted] Application at 19-20; accord DIRNSA Declaration at 19. The two methods are:

(1) Contact chaining. NSA will use computer algorithms to identify within the archived meta data all e-mail [redacted] accounts that have been in contact with the seed account, as well as all accounts that have been in contact with an account within the first tier of accounts that had direct contact with the seed account, and [redacted] DIRNSA Declaration at 15-16.

[redacted]

An example may illustrate the claimed benefits of bulk collection and subsequent analysis of meta data. [redacted] Without an archive of meta data, the Government could target prospective collection on that account, but information about past use would be unavailable. [redacted].[32]

However, if an archive of meta data were available, NSA could use the newly discovered account as a "seed" account. Accounts previously in contact with the "seed" account could be identified and further investigation could be pursued to determine if the users of those accounts are [redacted]

[32] Assuming that applicable legal requirements could be met, the Government also could collect the full contents of future messages by electronic surveillance of the account and of stored prior messages by physical search of the account. However, [redacted] could thwart these forms of collection also.

[redacted]

These avenues of discovery made possible by archived meta data provide the basis for NSA's assertion that bulk collection to accumulate a meta data archive "will substantially increase NSA's ability to detect and identify members of [redacted] DIRNSA Declaration at 15.

6. How FBI Investigations Would Benefit from the NSA's Collection and Analysis

The Government asserts that NSA's collection and analysis of this meta data will be relevant to [redacted] FBI investigations in two ways. First, ongoing FBI investigations may develop grounds for reasonable suspicion that particular accounts are used in furtherance of [redacted] The FBI may identify such accounts to NSA for use as "seed" accounts. Using the methods described above, NSA may obtain from the archived data other accounts that are in contact with, or appear to have the same user as, the "seed" account. This information may then be passed to the FBI as investigative leads in furtherance of its investigation. Memorandum of Law and Fact at 27-28. Alternatively, NSA querying of the archived meta data based on information from sources other than the FBI may identify accounts that appear to be used by someone involved in

[redacted] activities. If such accounts are relevant to FBI investigative responsibilities - for example, if it appears that their users are in the United States - then NSA will provide information to the FBI, which may prove relevant to ongoing FBI investigations or provide the predicate for new investigations of persons involved in [redacted] Under the proposed program, NSA estimates that roughly 400 accounts would be "tipped" to the FBI and CIA[33] annually, with an estimated twenty-five percent of that number associated with U.S. persons. DIRNSA Declaration at 20.

7. The Government's Proposed Procedures for Accessing, Retaining, and Disseminating Collected Information

The application specifies proposed procedures and restrictions for accessing, retaining, and disseminating information from this bulk collection of meta data. Application at 18-24. These procedures and restrictions, with certain modifications, are set out at pages 82-87 below.

[33] As long as the proposed collection satisfies the standard of relevance to an FBI investigation described in section 1842(a)(1), (c)(2), dissemination of information to other agencies when it is relevant to their responsibilities is appropriate.

B. The Information To Be Obtained is Likely to be Relevant to Ongoing FBI Investigations to Protect Against International Terrorism

As shown above, the application and supporting materials demonstrate that the FBI has numerous pending investigations on [redacted] subjects and that a major challenge faced by the FBI is the identification of [redacted] within the United States. [redacted] The application and DIRNSA declaration provide detailed explanations of why NSA regards bulk collection of meta data as necessary for contact chaining [redacted] and how those analytical methods can be expected to uncover and monitor unknown [redacted] who could otherwise elude detection. The DIRNSA also explains why NSA has chosen the proposed [redacted] and selection criteria in order to build a meta data archive that will be, in relative terms, richly populated with [redacted] related communications. On each of these points, the Court has received sufficient information to conclude that the Government's

assessments are fully considered and plausibly grounded in facts submitted to the Court.

Accordingly, the Court accepts for purposes of this application that the proposed bulk collection of meta data is necessary for NSA to employ contact chaining [redacted] The Court similarly accepts that those analytic tools are likely to generate useful investigative leads for ongoing efforts by the FBI (and other agencies) to identify and track [redacted] potentially including unidentified operatives in place to facilitate or execute imminent large scale attacks within the United States.

The question remains whether these circumstances adequately support the certification that "the information likely to be obtained . . . is relevant to an ongoing investigation to protect against international terrorism," § 1842(c)(2), even though only a very small percentage of the information obtained will be from [redacted] communications and therefore directly relevant to such an investigation. As the Government points out, the meaning of "relevant" is broad enough, at least in some contexts, to encompass information that may reasonably lead to the discovery of directly relevant information. Memorandum of Law and Fact at 34. Here, the bulk collection of meta data - i.e.,

the collection of both a huge volume and high percentage of unrelated communications - is necessary to identify the much smaller number of [redacted] communications.

The Court is persuaded that, in the circumstances of this case, the scope of the proposed collection is consistent with the certification of relevance.[34] In so finding, the Court concludes that, under the circumstances of this case, the applicable relevance standard does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [redacted]

---

[34] The Government analogizes this case to ones in which the Court has authorized overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811. Memorandum of Fact and Law at 42-43. The Court has authorized the latter form of collection where it is not technologically possible to acquire [redacted] The two situations are similar in that they both involve collection of an unusually large volume of non-foreign intelligence information as a necessary means of obtaining the desired foreign intelligence information. Yet there are also important differences between these cases. An overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811 requires probable cause to believe that the target is an agent of a foreign power and uses the particular facility at which surveillance will be directed. § 1805(a)(3). In this case under 50 U.S.C. §§ 1841-1846, no probable cause findings are required, and the bulk collection is justified as necessary to discover unknown [redacted] persons and facilities, rather than to acquire communications to and from identified agents of a foreign power. Because of these differences, the authorization of bulk collection under §§ 1841-1846 should not be taken as precedent for similar collection of the full contents of communications under §§ 1801-1811.

[redacted] FBI investigations. In reaching this conclusion, the Court finds instructive Supreme Court precedents on when a search that is not predicated on individualized suspicion may nonetheless be reasonable under the Fourth Amendment. See Memorandum of Law and Fact at 43-48.[35]

The Supreme Court has recognized a "longstanding principle that neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." National Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989); accord, e.g., Board of Educ. of Indep. School Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 829 (2002); United States v. Martinez-Fuerte, 428 U.S. 543, 560-61 (1976). Specifically, the Court has held that, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's

[35] For the reasons explained below at pages 59-66, the Court finds that there is no privacy interest protected by the Fourth Amendment in the meta data to be collected. Nevertheless, the Court agrees with the Government's suggestion that the balancing methodology used to assess the reasonableness of a Fourth Amendment search or seizure is helpful in applying the relevance standard to this case. Memorandum of Law and Fact at 43.

interests to determine whether it is impractical to require a warrant or individualized suspicion in the particular context." Von Raab, 489 U.S. at 665-66; accord, e.g., Earls, 536 U.S. at 829.

This balancing analysis considers "the nature of the privacy interest allegedly compromised" and "the character of the intrusion" upon that interest. Earls, 536 U.S. at 830, 832. The privacy interest in the instant meta data is not of a stature protected by the Fourth Amendment. See pages 59-66 below. Moreover, the nature of the intrusion is mitigated by the restrictions on accessing and disseminating this information, under which only a small percentage of the data collected will be seen by any person. Cf. Earls, 536 U.S. at 833 (finding that restrictions on access to drug-testing information lessen the testing program's intrusion on privacy).

The assessment of reasonableness under the Fourth Amendment also considers "the nature and immediacy of the government's concerns and the efficacy of the [program] in meeting them." Id. at 834. In this case, the Government's concern is to identify and track [redacted] operatives, and ultimately to thwart terrorist attacks. This concern clearly involves national

security interests beyond the normal need for law enforcement[36] and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion. See, e.g., Earls (drug testing of secondary school students engaged in extracurricular activities); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (highway checkpoints to identify drunk drivers); Von Raab (drug testing of Customs Service employees applying for promotion to sensitive positions); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989) (drug and alcohol testing of railroad workers).[37] The Government's interest here has even greater "immediacy" in view of the above-described intelligence reporting and assessment regarding ongoing plans for large scale attacks within the United States.

As to efficacy under the Fourth Amendment analysis, the Government need not make a showing that it is using the least intrusive means available. Earls, 536 U.S. at 837; Martinez-

---

[36] See In Re Sealed Case, 310 F.3d 717, 744-46 (Foreign Int. Surv. Ct. Rev. 2002) (per curiam) (discussing the prevention of terrorist attacks as a special need beyond ordinary law enforcement).

[37] Moreover, the Government's need in this case could be analogized to the interest in discovering or preventing danger from "latent or hidden conditions," which may justify suspicionless searches. See, e.g., Von Raab, 489 U.S. at 668.

Fuerte, 428 U.S. at 556-57 n.12. Rather, the question is whether the Government has chosen "a reasonably effective means of addressing" the need. Earls, 536 U.S. at 837. In structuring a program involving suspicionless search or seizure, e.g., in positioning roadblocks at certain points, "the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources." Sitz, 496 U.S. at 453-54; see also Martinez-Fuerte, 428 U.S. at 566 ("deference is to be given to the administrative decisions of higher ranking officials"). A low percentage of positive outcomes among the total number of searches or seizures does not necessarily render a program ineffective.[38]

In this case, senior responsible officials, whose judgment on these matters is entitled to deference, see pages 30-31 above, have articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [redacted] operatives whose Internet communications would

[38] See Sitz, 496 U.S. at 454 ("detention of the 126 vehicles that entered the checkpoint resulted in the arrest of two drunken drivers"); Martinez-Fuerte, 428 U.S. at 546 & n.1, 554 (checkpoint near border to detect illegal migrants: out of "roughly 146,000 vehicles" temporarily "'seized,'" 171 were found to contain deportable aliens).

otherwise go undetected in the huge streams of [redacted] These officials have also explained why they seek to collect meta data [redacted] identified in the application. Based on these explanations, the proposed collection appears to be a reasonably effective means to this end.

In summary, the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted] related operatives and thereby obtaining information likely to be [redacted] to ongoing FBI investigations. In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's [redacted] investigations.

---

[19] Cf. Martinez-Fuerte, 428 U.S. at 557 (requiring reasonable suspicion for stops at highway checkpoints "on major routes . . . would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car").

C. The Pertinent FBI Investigations of U.S. Persons Are Not Conducted Solely Upon the Basis of First Amendment Activities.

When the information likely to be obtained concerns a U.S. person, § 1842(c)(2) requires a certification that the "ongoing investigation . . . of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." The certification in this case states that the pertinent investigation is not being conducted on such a basis. Application at 26. The application refers to numerous FBI National Security investigations "being conducted under guidelines approved by the Attorney General pursuant to Executive Order No. 12,333."[40] Id. at 6.

> Those investigations are being conducted on the basis of activities of [redacted] and unknown [redacted] affiliates in the United States and abroad, and to the extent these subjects of investigation are United States persons, not solely on the basis of activities that are protected by the First Amendment to the Constitution.

Id.

Thus, the certification and application contain the proper assurance that the relevant investigations of U.S. persons are

---

[40] § 1842(a)(1) permits the filing of applications for installation and use of pen register and trap and trace devices to obtain information relevant to certain investigations "under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order."

not being conducted solely on the basis of activities protected by the First Amendment. However, the unusual breadth of this collection and its relation to the pertinent FBI investigations calls for further attention to this issue. In the usual case, the FBI conducts pen register and trap and trace surveillance of a particular communications facility (e.g., a phone number or e-mail address) because it carries communications of a person who is the subject of an FBI investigation. The required certification typically varies depending on whether the subject is a U.S. person: if not, the certification will state, in the language of § 1842(c)(2), that the information likely to be obtained "is foreign intelligence information not concerning a United States person;" if the subject is a U.S. person, the certification will state that such information is "relevant to an ongoing investigation to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This usual practice conforms to the clear statutory purpose that pen register/trap and trace information about the communications of U.S. persons will not be targeted for collection unless it is relevant to an

investigation that is not solely based upon First Amendment activities.

In this case, the initial acquisition of information is not directed at facilities used by particular individuals of investigative interest, but meta data concerning the communications of such individuals' [redacted] Here, the legislative purpose is best effectuated at the querying stage, since it will be at a point that an analyst queries the archived data that information concerning particular individuals will first be compiled and reviewed. Accordingly, the Court orders that NSA apply the following modification of its proposed criterion for querying the archived data: [redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known [redacted] is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First

Amendment to the Constitution.[41] For example, an e-mail account used by a U.S. person could not be a seed account if the only information thought to support the belief that the account is associated with [redacted] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of "advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action." Brandenberg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

III. THE PROPOSED COLLECTION AND HANDLING OF META DATA DO NOT VIOLATE THE FIRST OR FOURTH AMENDMENTS.

Because this case presents a novel use of statutory authorities for pen register/trap and trace surveillance, the Court will also explain why it is satisfied that this surveillance comports with the protections of the Fourth Amendment and the First Amendment.

A. Fourth Amendment Issues

The foregoing analysis has observed at various points that the Fourth Amendment does not apply to the proposed collection of

---

[41] This modification will realize more fully the Government's suggestion that "[t]he information actually viewed by any human being . . . will be just as limited - and will be based on the same targeted, individual standards - as in the case of an ordinary pen register or trap and trace device." Government's Letter of [redacted] at 3.

meta data. See, e.g., pages 19, 50-51 above. This section explains the basis for that conclusion.

First, as a general matter, there is no reasonable expectation of privacy under the Fourth Amendment in the meta data to be collected. This conclusion follows directly from the reasoning of Smith v. Maryland, 442 U.S. 735 (1979), which concerned the use of a pen register on a home telephone line. In that case, the Supreme Court found that it was doubtful that telephone users had a subjective expectation of privacy in the numbers they dialed, id. at 742-43, and that in any case such an expectation "is not 'one that society is prepared to recognize as reasonable.'" Id. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)). The Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," since he "assume[s] the risk" that the third party would reveal that information to the government. Id. at 743-44.[42] The Court found this principle applicable to dialed phone numbers, regardless of the automated means by which the call is placed and the "fortuity of whether or

[42] This principle applies even if there is an understanding that the third party will treat the information as confidential. See SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).

not the phone company in fact elects to make a quasi-permanent record of a particular number dialed." Id. at 744-45.[43]

The same analysis applies to the meta data involved in this application. Users of e-mail [redacted] voluntarily expose addressing information for communications they send and receive to communications service providers. Having done so, they lack any legitimate expectation of privacy in such information for Fourth Amendment purposes.[44] Moreover, the relevant statutes put this form of pen register/trap and trace surveillance on a par with pen register/trap and trace surveillance of telephone calls, on the

---

[43] While Smith involved a pen register, its reasoning equally applies to trap and trace devices that capture the originating numbers of incoming calls. See, e.g., United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).

[44] Cf. Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (users of computer bulletin board service lacked reasonable expectation of privacy in subscriber information that they provided to systems operator); United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000) (no reasonable expectation of privacy in subscriber information provided to ISP); United States v. Hambrick, 55 F.Supp.2d 504, 508-09 (W.D. Va. 1999) (no reasonable expectation of privacy in screen name and other information provided to ISP), aff'd, 225 F.3d 656 (4th Cir. 2000) (Table).

premise that neither form of surveillance involves a Fourth Amendment search or seizure.[45]

This conclusion is equally well-founded for the proposed collection of [redacted] Nothing in the Smith analysis depends on the fact that a telephone pen register acquires addressing information for a call while it is being placed, rather than from data [redacted] Indeed, the controlling principle - that voluntary disclosure of information to a third party vitiates any legitimate expectation that the third party will not provide it to the government - has been applied to records [redacted] See Jerry T. O'Brien, Inc., 467 U.S. at 737-38, 743 (records of prior stock

[45] The USA PATRIOT Act amended 18 U.S.C. § 3127 to clarify that its definitions of "pen register" and "trap and trace device" applied to Internet communications. See Public Law 107-56, Title II, § 216(c); 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (noting that prior statutory language was "ill-equipped" for Internet communications and supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"). Authorization to install such devices requires relevance to an investigation, but not any showing of probable cause. See 18 U.S.C. § 3123(a)(1), (2) (ordinary criminal investigation); 50 U.S.C. § 1842(a)(1), (c)(2) (investigation conducted under guidelines approved under Executive Order 12333).

trading); Miller, 425 U.S. at 436-38, 443 (checks, deposit slips, and other bank records).[46]

For these reasons, it is clear that, in ordinary circumstances, pen register/trap and trace surveillance of Internet communications does not involve a Fourth Amendment search or seizure. However, since this application involves unusually broad collection and distinctive modes of analyzing information, the Court will explain why these special circumstances do not alter its conclusion that no Fourth Amendment search or seizure is involved.

First, regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy. Whether a large number of persons are otherwise affected by the government's conduct is irrelevant. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched."

[redacted]

Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("'Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.'") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)). Since the Fourth Amendment bestows "a personal right that must be invoked by an individual," a person "claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable." Minnesota v. Carter, 525 U.S. 83, 88 (1998). So long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the proposed pen register/trap and trace surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur.

Regarding the proposed analytical uses of the archived meta data, it might be thought that [redacted] not immediately available from conventional pen register/trap and

trace surveillance might itself implicate the Fourth Amendment.[47] However, that suggestion would be at odds with precedent that the subsequent use of the results of a search cannot itself involve an additional or continuing violation of the Fourth Amendment. For example, in United States v. Calandra, 414 U.S. 338 (1974), it was argued that each question before a grand jury "based on evidence obtained from an illegal search and seizure constitutes a fresh and independent violation of the witness' constitutional rights," and that such questioning involved "an additional intrusion" into the privacy of the witness "in violation of the

---

[47] The public disclosure of aggregated and compiled data has been found to impinge on privacy interests protected under the Freedom of Information Act (FOIA), even if the information was previously available to the public in a scattered, less accessible form. See United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989) (FBI "rap sheets," including public-record information on arrests and disposition of criminal charges, qualified for "personal privacy" exemption from disclosure under FOIA, 5 U.S.C. § 552(b)(7)(C)); but cf. Paul v. Davis, 424 U.S. 693, 712-13 (1976) (circulating a flyer publicizing an arrest for shoplifting did not violate constitutional right to privacy). In this case, because section 1842 authorizes the Attorney General to apply for pen register/trap and trace authorities "[n]othwithstanding any other provision of law," 50 U.S.C. § 1842(a)(1), and states that the Court "shall enter an ex parte order . . . approving the installation and use of a pen register or trap and trace device" upon a finding "that the application satisfies the requirements of [section 1842]," id. § 1842(d)(1), the Court has no need to consider how other statutes, such as the Privacy Act, 5 U.S.C. § 552a, might apply to the proposed activities of the Government.

Fourth Amendment." 414 U.S. at 353 & n.9 (internal quotations omitted). The Court rejected this argument, explaining:

> The purpose of the Fourth Amendment is to prevent unreasonable governmental intrusions into the privacy of one's person, house, papers, or effects. . . . That wrong . . . is fully accomplished by the original search without probable cause. Grand jury questions based on evidence obtained thereby involve no independent governmental invasion of one's person, house, papers, or effects . . . . Questions based on illegally obtained evidence are only a derivative use of the product of a past unlawful search and seizure. They work no new Fourth Amendment wrong.

414 U.S. at 354 (emphasis added); accord United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990); United States v. Leon, 468 U.S. 897, 906 (1984); see also United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information.").

In this case, sophisticated analysis of archived meta data may yield more information about a person's Internet communications than what would at first be apparent. Nevertheless, such analysis would, like the grand jury questioning in Calandra, involve merely a derivative use of information already obtained, rather than an independent governmental invasion of matters protected by the Fourth

Amendment. Accordingly, the Court finds that the proposed collection and analysis does not involve a search or seizure under the Fourth Amendment.

B. First Amendment Issues

By letter dated [redacted] the Court asked the Government to address "the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons." In response, the Government acknowledges that surveillance that acquires "the contents of communications might in some cases implicate First Amendment interests, in particular the freedom of association," Government's Letter of [redacted] at 1, but denies or minimizes the First Amendment implications of surveillance that only acquires non-content addressing information.

The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation. See Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1051 (D.C. Cir. 1978) (First Amendment protects activities "subject to the general and incidental

burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves" directed at First Amendment conduct; accordingly, subpoenas to produce reporters' telephone toll records without prior notice did not violate the First Amendment) (emphasis in original); United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989) (use of undercover informants "to infiltrate an organization engaged in protected first amendment activities" must be part of investigation "conducted in good faith; i.e., not for the purpose of abridging first amendment freedoms"); United States v. Gering, 716 F.2d 615, 620 (9th Cir. 1983) (mail covers targeting minister at residence and church upheld against First Amendment challenge absent showing "that mail covers were improperly used and burdened . . . free exercise or associational rights"). Conversely,

> all investigative techniques are subject to abuse and can conceivably be used to oppress citizens and groups, rather than to further proper law enforcement goals. In some cases, bad faith use of these techniques may constitute an abridgment of the First Amendment rights of the citizens at whom they are directed.

Reporters Comm., 593 F.2d at 1064.[48]

---

[48] Part of Judge Wilkey's opinion in Reporters Comm. categorically concludes that the First Amendment affords no protections against government investigation beyond what is (continued...)

Here, the proposed collection of meta data is not for ordinary law enforcement purposes, but in furtherance of the compelling national interest of identifying and tracking [redacted] and ultimately of thwarting terrorist attacks. The overarching investigative effort against [redacted] is not aimed at curtailing First Amendment activities and satisfies the "good faith" requirement described in the above-cited cases. However, the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons. For this reason, special restrictions on the accessing, retention, and dissemination of such information are necessary to guard against such misuse. See pages 82-87 below. With such restrictions in place, the proposed collection of non-

---

[49](...continued)
provided by the Fourth and Fifth Amendments. Id. at 1053-60. However, that part of the opinion was not joined by the other judge in the majority, who opined that the result of First Amendment analysis "may not always coincide with that attained by application of Fourth Amendment doctrine." Id. at 1071 n.4 (Robinson, J.).

content addressing information does not violate the First Amendment.[49]

IV. TO ENSURE LAWFUL IMPLEMENTATION OF THIS SURVEILLANCE AUTHORITY, NSA IS ORDERED TO COMPLY WITH THE PROPOSED RESTRICTIONS AND PROCEDURES, AS MODIFIED BY THE COURT.

The proposed collection involves an extraordinarily broad implementation of a type of surveillance that Congress has regulated by statute, even in its conventional, more narrowly targeted form. To ensure that this authority is implemented in a lawful manner, NSA is ordered to comply with the restrictions and procedures set out below at pages 82-87, which the Court has adapted from the Government's application.[50] Adherence to them

---

[49] The court in Paton v. La Prade, 469 F. Supp. 773, 780-82 (D.N.J. 1978), held that a mail cover on a dissident political organization violated the First Amendment because it was authorized under a regulation that was overbroad in its use of the undefined term "national security." In contrast, this pen register/trap and trace surveillance does not target a political group and is authorized pursuant to statute on the grounds of relevance to an investigation to protect against "international terrorism," a term defined at 50 U.S.C. § 1801(c). This definition has been upheld against a claim of First Amendment overbreadth. See United States v. Falvey, 540 F. Supp. 1306, 1314-15 (E.D.N.Y. 1982).

[50] The principal changes that the Court has made from the procedures described in the application are the inclusion of a "First Amendment proviso" as part of the "reasonable suspicion" standard for an [redacted] to be used as the basis for querying archived meta data, see pages 57-58 above, the adoption of a date after which meta data may not be retained, see pages 70-71 below, and an enhanced role for the NSA's Office of

(continued...)

will help ensure that this information is used for the stated purpose of its collection - the identification and tracking of [redacted] their Internet communications - thereby safeguarding the continued validity of the certification of relevance under § 1842(c)(2). These procedures will also help effectuate 50 U.S.C. § 1845(a)(2), which directs that no information from a Court-authorized pen register or trap and trace device "may be used or disclosed by Federal officers or employees except for lawful purposes," and ensure that such use and disclosure will not abridge First Amendment rights.

The Court's letter of [redacted] asked the Government to explain "[f]or how long . . . the information collected under this authority [would] continue to be of operational value to the counter-terrorism investigation(s) for which it is collected." The Government's letter of [redacted], stated that such information "would continue to be of significant operational value for at least 18 months," based on NSA's "analytic judgment." [redacted] Letter at 3. During that period, meta

---

[50](...continued)
General Counsel in the implementation of this authority, see pages 84-85 below. The Court recognizes that, as circumstances change and experience is gained in implementing this authority, the Government may propose other modifications to these procedures.

data would be available to analysts online for authorized querying. After 18 months, NSA "believes that there continues to be operational value in retaining e-mail meta data . . . in an 'off-line' storage system," since "in certain circumstances" information of that age could "provide valuable leads for the investigation into [redacted]" Id. However, the value of such information "would diminish over time," so that "NSA assesses that meta data would have operational value in off-line storage for a period of three years, and could be destroyed after that time (that is, a total of four and one-half years after it was initially collected)." Id. In accordance with this assessment, NSA is ordered to destroy archived meta data collected under this authority no later than four and one-half years after its initial collection.

* * *

Accordingly, a verified application having been made by the Attorney General of the United States for an order authorizing installation and use of pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846, and full consideration having been given

to the matters set forth therein, the Court finds, on the grounds explained above, that:

1. The Attorney General is authorized to approve applications for pen registers and trap and trace devices under the Act and to make such applications under the Act.

2. The applicant has certified that the information likely to be obtained from the requested pen registers and trap and trace devices is relevant to an ongoing investigation to protect against international terrorism that is not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

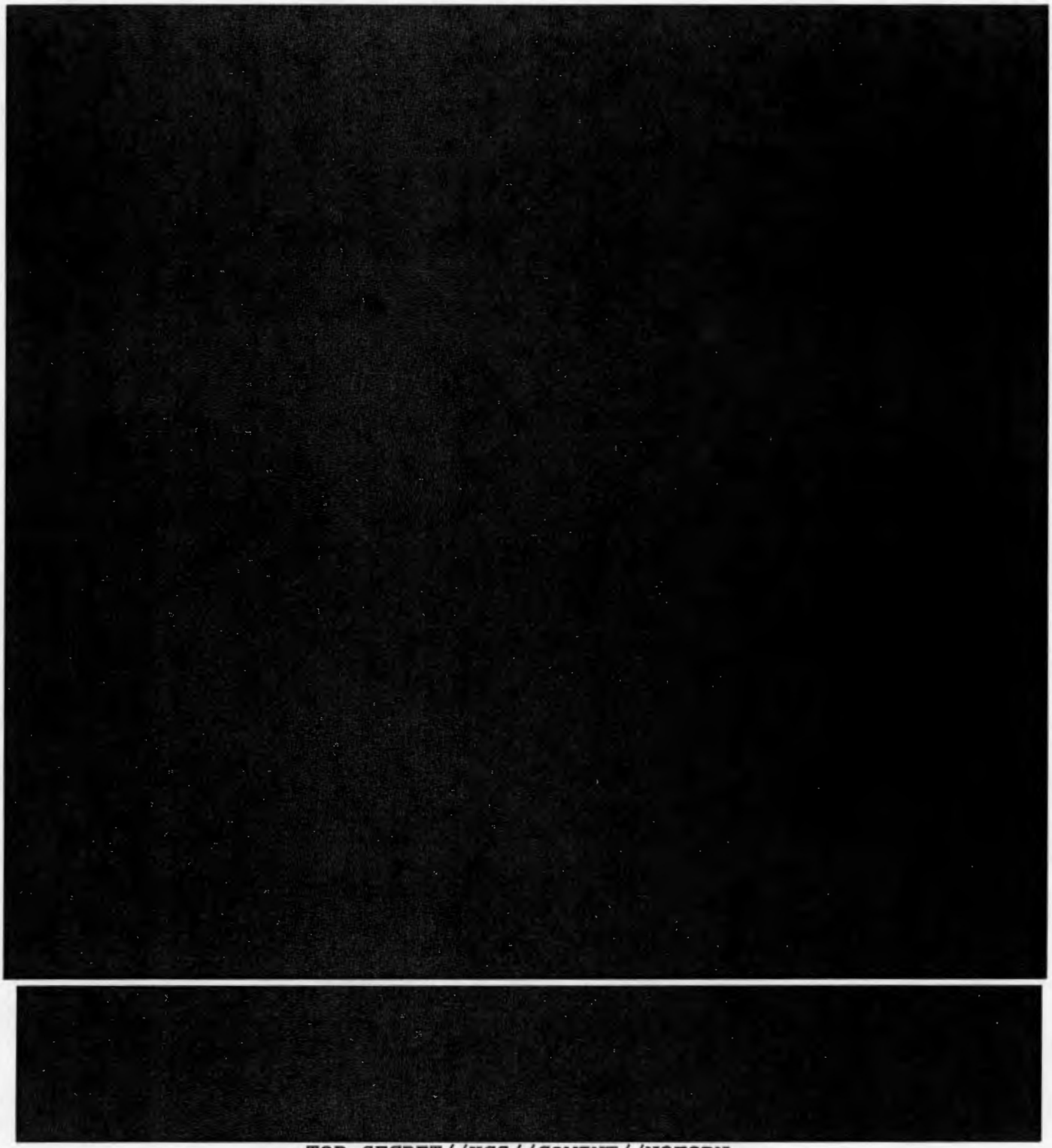
3. [redacted] in the United States and abroad are the subjects of National Security investigations conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to Executive Order No. 12333.

4. The pen registers and trap and trace devices [redacted]

[redacted]

[51] The Government has represented that it is overwhelmingly likely that at [redacted]

[52] The Government has represented that it is overwhelmingly likely that [redacted]

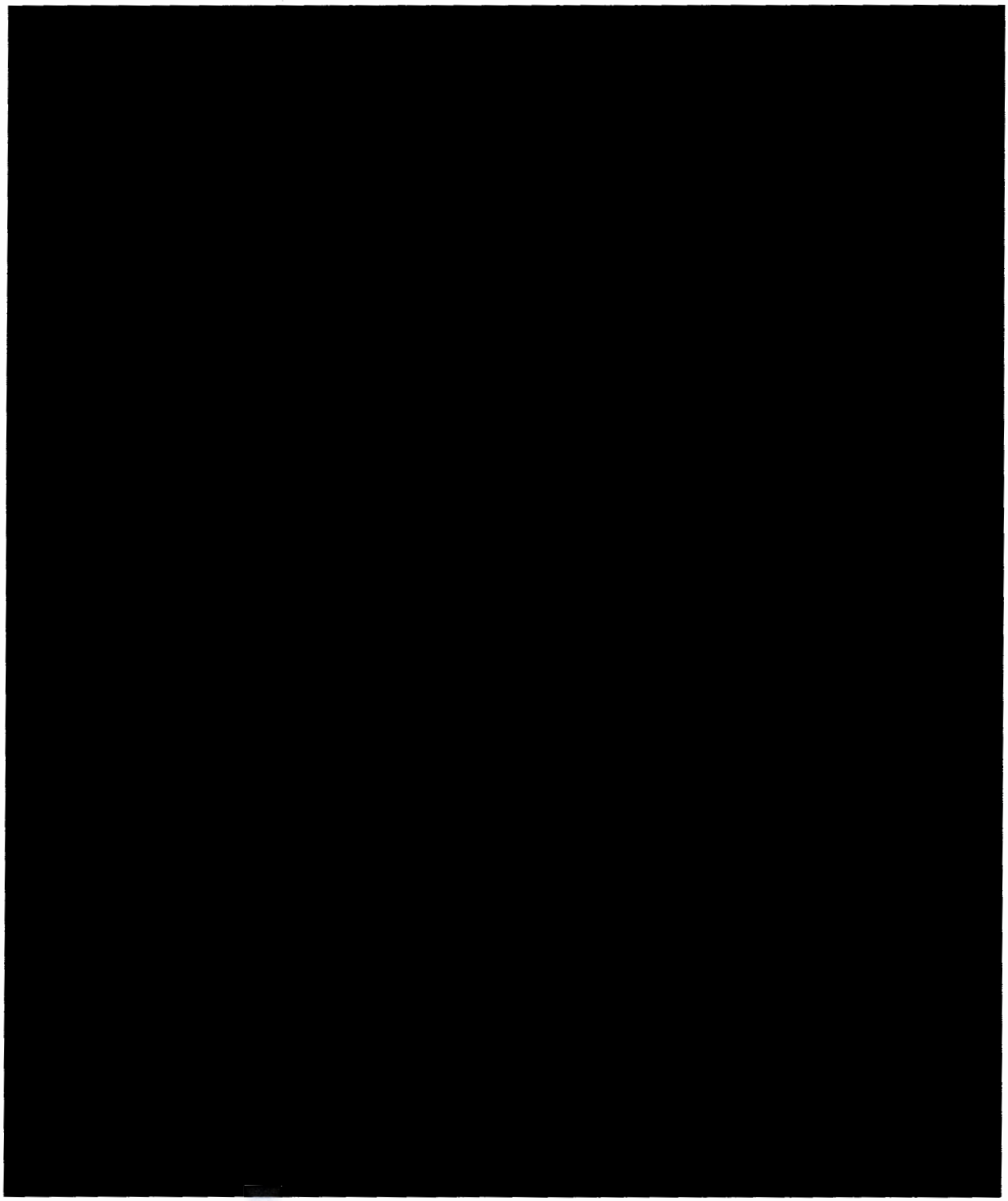


~~TOP SECRET//HCS//COMINT//NOFORN~~

[redacted]

[53] The Government has represented that it is overwhelmingly likely that [redacted]

~~TOP SECRET//HCS//COMINT//NOFORN~~



[redacted]

[54] The Government has represented that the majority of the communications [redacted]

[redacted]

[55] Because electronic communications will [redacted]

[redacted]

[redacted]

[redacted]

WHEREFORE, the Court finds that the application of the United States [redacted] pen registers and trap and trace devices, as described in the application, satisfies the requirements of the Act and specifically of 50 U.S.C. § 1842 and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, AS MODIFIED HEREIN, and it is

FURTHER ORDERED, as follows:

(1) Installation and use of pen registers and trap and trace devices as requested in the Government's application is authorized for a period of **ninety days** from the date of this Opinion and Order, unless otherwise ordered by this Court, as follows: installation and use of pen registers and/or trap and

trace devices as described above to collect all addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications identified above on [redacted] identified above, including the "to," "from," "cc," and "bcc" fields for those communications [redacted] Collection of the contents of such communications as defined by 18 U.S.C. § 2510(8) is not authorized.

(2) The authority granted is within the United States.

(3) As requested in the application, [redacted] (specified persons), are directed to furnish the NSA with

---

[57] Although the application makes clear that the assistance of these specified persons is contemplated, it does not expressly request that the Court direct these specified persons to assist the surveillance. However, because the application, at 24, requests that the Court enter the proposed orders submitted with the application and those proposed orders would direct the specified persons to provide assistance, the application effectively requests the Court to direct such assistance.

any information, facilities, or technical assistance necessary to accomplish the installation and operation of pen registers and trap and trace devices in such a manner as will protect their secrecy and produce a minimum amount of interference with the services each specified person is providing to its subscribers. Each specified person shall not disclose the existence of the investigation or of the pen registers and trap and trace devices to any person, unless or until ordered by the Court, and shall maintain all records concerning the pen registers and trap and trace devices, or the aid furnished to the NSA, under the security procedures approved by the Attorney General [redacted] that have previously been or will be furnished to each specified person and are on file with this Court.

(4) The NSA shall compensate the specified person(s) referred to above for reasonable expenses incurred in providing such assistance in connection with the installation and use of the pen registers and trap and trace devices herein.

(5) The NSA shall follow the following procedures and restrictions regarding the storage, accessing, and disseminating of information obtained through use of the pen register and trap and trace devices authorized herein:

a. The NSA shall store such information in a manner that ensures that it will not be commingled with other data.

b. The ability to access such information shall be limited to ten specially cleared analysts and to specially cleared administrators. The NSA shall ensure that the mechanism for accessing such information will automatically generate a log of auditing information for each occasion when the information is accessed, to include the accessing user's login, IP address, date and time, and retrieval request.

c. Such information shall be accessed only through queries using the contact chaining [redacted] methods described at page 43 above. Such queries shall be performed only on the basis of a particular known [redacted] after the NSA has concluded, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable articulable suspicion that [redacted] is associated with [redacted] provided, however, that [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted]

[redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. Queries shall only be conducted with the approval of one of the following NSA officials: the Program Manager, Counterterrorism Advanced Analysis; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or a Counterterrorism Advanced Analysis Shift Coordinator in the Analysis and Production Directorate of the Signals Intelligence Directorate.

d. Because the implementation of this authority involves distinctive legal considerations, NSA's Office of General Counsel shall:

i) ensure that analysts with the ability to access such information receive appropriate training and guidance regarding the querying standard set out in paragraph c. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information.

ii) monitor the designation of individuals with access to such information under paragraph b. above and the functioning of the automatic logging of auditing information required by paragraph b. above.

iii) to ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of meta data in online or "off-line" storage based on seed accounts used by U.S. persons.[58]

e. The NSA shall apply the Attorney General-approved guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application) to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein. Prior to disseminating any U.S. person information outside of the NSA, the Chief of Customer Response in the NSA's Signals Intelligence Directorate shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.

f. Information obtained from the authorized pen registers and trap and trace devices shall be available

---

[58] The Court notes that, in conventional pen register/trap and trace surveillances, there is judicial review of the application before any [redacted] In this case, the analogous decision to use a particular e-mail account as a seed account takes place [redacted] In these circumstances, it shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the basis of such queries, including the First Amendment proviso, set out in paragraph c. above.

online for querying, as described in paragraphs b. and c. above, for eighteen months. After such time, such information shall be transferred to an "off-line" tape system, which shall only be accessed by a cleared administrator in order to retrieve information that satisfies the standard for online accessing stated in paragraph c. above and is reasonably believed, despite its age, to be relevant to an ongoing investigation of [redacted] Searches of meta data in "off-line" storage shall be approved by one of the officials identified in paragraph c. above.

g. Meta data shall be destroyed no later than 18 months after it is required to be put into "off-line" storage, i.e., no later than four and one-half years after its initial collection.

h. Any application to renew or reinstate the authority granted herein shall include:

i) a report discussing queries that have been made since the prior application to this Court and the NSA's application of the standard set out in paragraph c. above to those queries.

ii) detailed information regarding [redacted] proposed to be added to such authority.

iii) any changes in the description of the [redacted] above or in the nature of the communications [redacted]

iv) any changes in the proposed means of collection, to include [redacted] the pen register and/or trap and trace devices [redacted]

Signed [redacted] 10:30 a.m. E.D.T.
Date Time

This authorization regarding [redacted] **in the United States and Abroad** expires on the [redacted] at 5:00 p.m., Eastern Daylight Time.

Colleen Kollar-Kotelly

COLLEEN KOLLAR-KOTELLY
Presiding Judge, United States Foreign Intelligence Surveillance Court