BEFORE THE PUBLIC UTILITY COMMISSION

OF OREGON

UM 1265

AMERICAN CIVIL LIBERTIES UNION OF OREGON, INC. and AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF OREGON, INC., Complainants, v. VERIZON NORTHWEST, INC., and QWEST CORPORATION, Defendants.	FIRST AMENDED COMPLAINT

INTRODUCTION

1.

This proceeding seeks to remedy the unlawful systematic release by Defendants of protected information about the intrastate telephone calls of thousands of Oregonians in violation of 18 U.S.C. § 2511(1), 18 U.S.C. § 2702, OAR 860-032-0510, each Defendant's written privacy policy and thousands of Oregonians' right to privacy. Upon information and belief, Verizon Northwest, Inc. and Qwest Corporation are, and for some time have been, unlawfully providing persons or entities, public or private, with information concerning Oregonians'

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

private intrastate calls.

PARTIES

2.

The American Civil Liberties Union of Oregon, Inc. ("ACLU of Oregon") is a statewide nonprofit and nonpartisan public interest organization devoted to protecting the basic civil liberties of all persons in Oregon. The ACLU of Oregon represents approximately 15,000 members in Oregon. The ACLU of Oregon sues on its own behalf and on behalf of its members.

3.

The American Civil Liberties Union Foundation of Oregon, Inc. ("ACLU Foundation") is a tax exempt organization that primarily conducts legal and educational activities that are consistent with the mission and objectives of the ACLU of Oregon. Unless otherwise specified, the ACLU of Oregon and the ACLU Foundation are referred to jointly herein as "ACLU."

4.

Verizon Northwest, Inc. ("Verizon") and Qwest Corporation ("Qwest") are companies that provide telecommunications services to the citizens of Oregon, including the ACLU and its members.

JURISDICTION

5.

The Commission has jurisdiction to hear this dispute pursuant to ORS 756.500 and ORS 756.040(2) because Defendants are public telecommunications companies operating in Oregon and the Commission has the "power and jurisdiction to supervise and regulate every public *** telecommunications utility in this state, and to do all things necessary and convenient in the exercise of such power and jurisdiction."

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

FACTUAL ALLEGATIONS

6.

On December 15, 2005, the *New York Times* reported that the National Security Agency ("NSA") had been intercepting telephone calls involving domestic United States persons "without the court-approved warrants ordinarily required for domestic spying." James Risen and Eric Lichtblau, "Bush Secretly Lifted Some Limits on Spying in U.S. after 9/11," *New York Times* (December 15, 2005) (A copy of which is attached hereto as Ex. No. 1).

7.

In his December 19, 2005 Presidential News Conference, President Bush admitted that, "consistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to Al Qaida and related terrorist organizations" (hereafter the "Program"). Transcript, Presidential News Conference, Monday, December 19, 2005; 11:32 AM, White House Office of the Press Secretary (A copy of which is attached hereto as Ex. No. 2). President Bush went on to say that the "program is carefully reviewed approximately every 45 days to ensure it is being used properly. Leaders in the United States Congress have been briefed more than a dozen times on this program." *Id.* President Bush acknowledged that at that time he had "reauthorized this program more than 30 times since the September the 11th attacks, and [he] intend[s] to do so . . . for so long as the nation faces the continuing threat of an enemy that wants to kill American citizens."

8.

Under the Program, the NSA engages in "electronic surveillance."

/ / /

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

9.

Under the Program, the NSA intercepts vast quantities of the international telephone and Internet communications of people inside the United States, including citizens and lawful permanent residents.

10.

Under the Program, the NSA also intercepts purely domestic telephone communications, that is, communications among people all of whom are inside the United States.

11.

Under the Program, the NSA intercepts the communications of people inside the United States without probable cause to believe that the surveillance targets have committed or are about to commit any crime.

12.

Under the Program, the NSA intercepts the communications of people inside the United States without probable cause to believe that the surveillance targets are foreign powers or agents thereof.

13.

Under the Program, the NSA intercepts the communications of people inside the United States without obtaining authorization for each interception from the President or the Attorney General.

14.

Under the Program, NSA shift supervisors are authorized to approve NSA employees' requests to intercept the communications of people inside the United States.

/ / /

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

15.

Under the Program, the NSA does not obtain judicial review before or after intercepting the communications of people inside the United States.

16.

On May 11, 2006, the *USA Today* reported that at least three phone companies, AT&T, BellSouth, and Verizon, disclosed the personal calling details of customers, including telephone numbers called, time, date, and direction of calls. Leslie Cauley, "NSA has massive database of Americans' phone calls," *USA Today* (May 11, 2006) (A copy of which is attached hereto as Ex. No. 3). The *New York Times* has further reported on the phone companies' disclosure of customer data. John O'Neil, et. al, "Qwests Refusal of N.S.A. Query Is Explained," *New York Times* (May 12, 2006) (A copy of which is attached hereto as Ex. No. 4). Although the *USA Today* later acknowledged that it could not establish the existence of an actual contract between any phone company and the NSA, it stood by the core allegations of its earlier story. "A note to our readers," *USA Today* (June 30, 2006) (A copy of which is attached hereto as Ex. No. 5).

17.

The database reportedly includes multiple fields of information from calling records, including but not limited to, called and calling numbers, time, date, direction of calls and other information. Upon information and belief, using this information, the NSA can easily determine the names and addresses associated with these calls by cross-referencing other readily available databases. Cauley, *USA Today* (May 11, 2006); John Markoff, "Questions Raised for Phone Giants in Spy Data Furor," *N.Y. Times*, May 13, 2006 (A copy of which is attached hereto as Ex. No. 6); John O'Neil and Eric Lichtblau, "Qwest's Refusal of N.S.A Query Is Explained," *N.Y. Times,* May 12, 2006. It has been reported that in addition to the

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

NSA, the database might be accessible by the Central Intelligence Agency, the Federal Bureau of Investigation and the Drug Enforcement Agency. Cauley, *USA Today* (May 11, 2006).

18.

The ACLU of Oregon is a business subscriber of Qwest and, upon information and belief, in the normal course of its business it receives calls from Oregon residents who are local telecommunications customers of Verizon and/or Qwest.

19.

The ACLU Foundation provides legal and educational services to Oregonians. The ACLU Foundation employs lawyers and engages in telephone conferences between clients and outside counsel. Many of the ACLU Foundation's telephone communications are privileged attorney-client communications. Upon information and belief, in the normal course of its business it receives calls from Oregon residents who are local telecommunications customers of Verizon and/or Qwest.

20.

Verizon and Qwest each have written policies setting forth the specific terms of each company's agreement to maintain customer privacy. (Copies of which are attached hereto as Exhibit Nos. 7 & 8 respectively). Each company's written privacy policy states that customer information will not be disclosed to outside parties without customer consent, except in circumstances not present here and when required by law.

21.

On September 8, 2006, ACLU's counsel sent individual letters to Verizon, Qwest and another Oregon telecommunications company stating ACLU's interest in obtaining information critical to its decision about whether to proceed before this Commission in either manner set out in Administrative Law Judge Arlow's July 31,

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

2006 ruling in these proceedings. The September 8, 2006 letters asked each entity whether it had ever, "disclosed, provided or revealed to any person or entity, public or private, or enabled any person or entity, public or private, to obtain the contents of Oregon telecommunications customers' intrastate telecommunications, voice or data, other than in the following circumstances: a. in strict compliance with a warrant, subpoena, or other court order; or b. in strict compliance with federal law, including 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, and 50 U.S.C. § 1801-1811."

22.

The September 8, 2006 letters also inquired as to whether Verizon, Qwest or another Oregon telecommunications company had ever "disclosed, provided or revealed to any person or entity, public or private, or enabled any person or entity, public or private to obtain information about or data describing the intrastate telecommunication activity of Oregon telecommunications customers, voice or data, other than in the following circumstances: a. in strict compliance with a warrant, subpoena, or other court order; or b. in strict compliance with Or. Admin. R. 860-032-0510; or c. in strict compliance with federal law, including 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, and 50 U.S.C. § 1801-1811."

23.

The ACLU's September 8, 2006 letters did not inquire about any counter-terrorism program, did not seek information about the NSA and did not require the disclosure of any information protected by the state secrets privilege.

24.

Verizon responded on September 18, 2006 stating, in relevant part, that this "Commission would be unable to adduce any facts relating to, and thus [would be] unable to resolve, the issues raised in the ACLU's filings." (A copy of which is

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

attached hereto as Ex. No. 9). Verizon went on to state that "Verizon NW can neither confirm nor deny whether it has any relationship to the counter-terrorism program aimed at al Qaeda involving the National Security Agency. However, as Verizon has previously stated, it (including Verizon NW) has not knowingly disclosed, provided or revealed to another person or entity (or enabled another person or entity to obtain) the contents or phone records of Oregon telecommunications customers other than in compliance with applicable law." *Id.*

25.

Verizon's response carefully avoids the specific questions asked. By responding generically that it complies with "applicable law," it failed to identify whether it acted outside of the specific laws cited by the ACLU, namely, "a warrant, subpoena, or other court order; or b. in strict compliance with Or. Admin. R. 860-032-0510; or c. in strict compliance with federal law, including 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, and 50 U.S.C. § 1801-1811."

26.

Verizon's refusal to provide a direct answer to the specific questions asked by the ACLU provides the basis for the reasonable belief that Verizon disclosed, provided, revealed or enabled another person or entity, public or private, to obtain the contents or data relating to the private, purely intrastate telecommunications activities of Oregonians including ACLU and its members without "a warrant, subpoena, or other court order; or b. in strict compliance with Or. Admin. R. 860-032-0510; or c. in strict compliance with federal law, including 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, and 50 U.S.C. § 1801-1811."

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

27.

Qwest responded to ACLU's letter on September 18, 2006 stating that "[o]n June 14, 2006, Qwest filed its response with the Oregon Public Utility Commission in docket UM 1265, in which Qwest stated it had 'no comment or other response to Complainant's Complaint at this time.' Qwest continues to have no comment on these issues, and thus declines to comment on your letter or answer any questions raised in your letter." (A copy of which is attached hereto as Ex. No. 10). Qwest's blanket refusal to respond to the questions asked by the ACLU provides the basis for the reasonable belief Qwest knowingly and unlawfully disclosed or enabled a third party to obtain protected information about the contents of or data describing the intrastate telecommunications activities of Oregonians including the ACLU and its members. Had Qwest not disclosed nor enabled access to such content or data, or had it done so lawfully, it could have answered the ACLU's questions in the negative.

28.

A third Oregon telecommunications company answered each question in the negative. Therefore, the ACLU has elected to not name that company in this First Amended Complaint.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

(DECLARATION THAT QWEST AND VERIZON VIOLATED 18 U.S.C. § 2511(1))

29.

The ACLU incorporates by reference ¶¶ 1 – 28 above as if fully set out herein.

30.

Upon information and belief, Verizon and Qwest disclosed and permitted persons or entities, public or private, to intercept the purely intrastate wire, oral or electronic telecommunications of the ACLU, its members and other Oregonians.

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

31.

Upon information and belief, Verizon and Qwest were not lawfully authorized by a warrant, subpoena, other court order; 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811 to disclose or permit persons or entities, public or private, to intercept the contents of ACLU's, its members' and other Oregonian's intrastate wire, oral or electronic communications.

32.

The ACLU of Oregon and its members have been irreparably harmed by Verizon's and Qwest's unlawful disclosures, interceptions and permitted interceptions by others of private intrastate communications.

33.

Many of the ACLU Foundation's communications are privileged attorney-client communications. The ACLU Foundation has been irreparably harmed by Verizon's and Qwest's unlawful disclosures, interceptions and permitted interceptions by others of private intrastate electronic communications.

34.

The ACLU seeks a declaration that Verizon and Qwest violated 18 U.S.C. § 2511(1).

SECOND CLAIM FOR RELIEF

(DECLARATION THAT VERIZON AND QWEST VIOLATED 18 U.S.C. § 2702)

35.

The ACLU incorporates by reference ¶¶ 1 – 34 above as if fully set out herein.

36.

Upon information and belief, Verizon and Qwest knowingly divulged, or enabled divulgence of, to persons or entities, public or private, the contents of

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

ACLU's, its members' and other Oregonian's communications while in electronic storage by Verizon and Qwest.

37.

Upon information and belief, Verizon and Qwest were not lawfully authorized by a warrant, subpoena, other court order; 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811 to divulge, or enable divulgence of, the contents of the ACLU's, its members' and other Oregonian's communications while in electronic storage by Verizon and Qwest.

38.

Verizon's and Qwest's divulgence or enabled divulgence to persons or entities, public or private, of the contents of ACLU of Oregon's and its members' communications while in electronic storage by Verizon and Qwest has caused irreparable harm to the ACLU of Oregon and its members.

39.

Many of the ACLU Foundation's communications are privileged attorney-client communications. Verizon's and Qwest's divulgence or enabled divulgence to persons or entities, public or private, of the contents of the ACLU Foundation's communications while in electronic storage by Verizon and Qwest has caused irreparable harm to the ACLU Foundation.

40.

Complainants seek a declaration that Verizon and Qwest violated 28 U.S.C. §2702.

THIRD CLAIM FOR RELIEF

(DECLARATION THAT DEFENDANTS VIOLATED OAR 860-032-0510)

41.

The ACLU incorporates by reference ¶¶ 1 – 40 above as if fully set out herein.

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

42.

Upon information and belief, Verizon and Qwest disclosed or enabled disclosure to persons or entities, public or private, protected information about and data describing the intrastate telecommunication activity of thousands of Oregonians without customer consent or compliance with a warrant, subpoena, other court order, Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811.

43.

The conduct of Qwest and Verizon as alleged above violated OAR 860-032-0510.

44.

Verizon's and Qwest's violation of OAR 860-032-0510 has caused irreparable harm to the ACLU of Oregon and its members.

45.

Many of the ACLU Foundation's communications are privileged attorney-client communications. Verizon's and Qwest's violation of OAR 860-032-0510 has caused irreparable harm to the ACLU Foundation.

46.

The ACLU seeks a declaration that Verizon and Qwest violated OAR 860-032-0510.

FOURTH CLAIM FOR RELIEF

(DECLARATION THAT DEFENDANTS BREACHED WRITTEN PRIVACY POLICIES)

47.

The ACLU incorporates by reference ¶¶ 1 – 46 above as if fully set out herein.

/ / /

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

48.

Upon information and belief, Verizon and Qwest disclosed or enabled disclosure to persons or entities, public or private, protected information about the content of and data describing the intrastate telecommunication activity of thousands of Oregonians without customer consent or a warrant, subpoena, other court order, or compliance with Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811.

49.

Verizon and Qwest breached the terms of their written privacy policies when they disclosed or enabled disclosure to persons or entities, public or private, protected information about content of and data describing the intrastate telecommunication activity of thousands of Oregonians as alleged herein.

50.

The ACLU of Oregon and its members have been harmed by Verizon's and Qwest's breaches of their written privacy policies.

51.

Many of the ACLU Foundation's communications are privileged attorney-client communications. The ACLU Foundation has been harmed by Verizon's and Qwest's breach of their privacy policies.

52.

The ACLU seeks a declaration that Verizon and Qwest violated their written policies and procedures. The ACLU further seeks an order requiring Verizon and Qwest to modify their existing customer privacy notices to describe with particularity the policies and procedures they will apply in the event they are asked in the future to disclose or enable disclosure or interception of confidential information pursuant to a non-customer request when there is no lawful warrant, subpoena, other court

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

order, or compliance with Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811.

FIFTH CLAIM FOR RELIEF

(DECLARATION THAT DEFENDANTS INVADED THE ACLU'S AND ITS MEMBERS' PRIVACY)

53.

The ACLU incorporates by reference ¶¶ 1 – 52 above as if fully set out herein.

54.

Verizon and Qwest invaded the ACLU's and its members' privacy when, upon information and belief, Verizon and Qwest disclosed to persons or entities, public or private, or enabled such disclosure or interception of protected information about the content of and data describing intrastate telecommunication activity without customer consent, a warrant, subpoena, or other court order, or compliance with Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811.

55.

The ACLU of Oregon and its members have been damaged as a result of Verizon's and Qwest's invasion of their privacy as alleged herein.

56.

Many of the ACLU Foundation's communications are privileged attorney-client communications. The ACLU Foundation has been harmed by Verizon's and Qwest's invasion of its privacy.

57.

The ACLU seeks a declaration that Verizon and Qwest invaded the privacy of the ACLU of Oregon and its members and the privacy of the ACLU Foundation. The ACLU further seeks an order requiring Verizon and Qwest to modify their existing customer privacy notices to describe with particularity the policies and procedures

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

they will apply in the event they are asked in the future to disclose or enable disclosure or interception of confidential information pursuant to a non-customer request when there is no lawful warrant, subpoena, other court order, or compliance with Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811.

SIXTH CLAIM FOR RELIEF

(PERMANENT INJUNCTION)

58.

The ACLU incorporates by reference ¶¶ 1 – 57 above as if fully set out herein.

59.

The ACLU of Oregon and its members and the ACLU Foundation have been irreparably harmed by the conduct of Verizon and Qwest as alleged herein.

60.

The ACLU of Oregon and its members and the ACLU Foundation will continue to use their telephones for private professional and personal purposes.

61.

Unless this Commission enjoins Verizon and Qwest from disclosing or enabling disclosure or interception of private intrastate call content or data to third parties without customer consent, a warrant, subpoena, or other court order, or compliance with Or. Admin. R. 860-032-0510, 18 U.S.C. § 2510-2522, 18 U.S.C. § 2701-2712, or 50 U.S.C. § 1801-1811, Verizon and Qwest will continue to do so and the ACLU will suffer ongoing and irreparable harm for which they have no adequate remedy at law.

/ / /

/ / /

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

PRAYER FOR RELIEF

Wherefore, the American Civil Liberties Union of Oregon, Inc. and the American Civil Liberties Union Foundation of Oregon, Inc. hereby ask the Public Utility Commission to:

1. Declare that Verizon's disclosure or enabling disclosure of intrastate telecommunications data to persons or entities, public or private, violates OAR 860-032-0510;

2. Declare that Qwest's disclosure or enabling disclosure of intrastate telecommunications data to persons or entities, public or private, violates OAR 860-032-0510;

3. Declare that Verizon's disclosure or enabling disclosure of intrastate call content or data to persons or entities, public or private, violates the terms of its written Privacy Policy;

4. Declare that Qwest's disclosure or enabling disclosure of intrastate call content or data to persons or entities, public or private, violates the terms of its written Privacy Policy;

5. Declare that Verizon's disclosure or enabling disclosure of intrastate call content or data to persons or entities, public or private, invades the privacy of the ACLU and its members;

6. Declare that Qwest's disclosure or enabling disclosure of intrastate call content or data to persons or entities, public or private, invades the privacy of the ACLU and its members;

7. Declare that Verizon's disclosure and/or permitted interception of intrastate telecommunications to persons or entities, public or private, violates 18 U.S.C. § 2511(1);

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

8. Declare that Qwest's disclosure and/or permitted interception of intrastate telecommunications to persons or entities, public or private, violates 18 U.S.C. § 2511(1);

9. Declare that Verizon's disclosure or enabling disclosure of intrastate call content to persons or entities, public or private, violates 18 U.S.C. § 2702;

10. Declare that Qwest's disclosure or enabled disclosure of intrastate call content to persons or entities, public or private, violates 18 U.S.C. § 2702;

11. Enjoin Verizon from unlawfully providing, or enabling provision of, intrastate call content or data to persons or entities, public or private;

12. Enjoin Qwest from unlawfully providing, or enabling provision of, intrastate call content or data to persons or entities, public or private;

13. Require Verizon and Qwest to modify their existing customer privacy notices to describe with particularity the policies that they would apply in the *hypothetical* event they are asked in the future to disclose, or enable disclosure of, confidential customer information pursuant to a request from a government agency.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

14. Grant such other and additional relief as the Public Utilities Commission deems just.

DATED this 22nd day of September, 2006.

Respectfully submitted,

GARVEY SCHUBERT BARER

By

Keith S. Dubanevich, OSB #97520
E-Mail: kdubanevich@gsblaw.com
Mark E. Friedman, OSB #73094
E-Mail: mfriedman@gsblaw.com
Laura Caldera Taylor, OSB #99378
E-Mail: ltaylor@gsblaw.com
Telephone: (503) 228-3939
Facsimile: (503) 226-0259

Attorneys for Complainants American Civil Liberties Union of Oregon, Inc. and American Civil Liberties Union Foundation of Oregon, Inc.

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

CERTIFICATE OF SERVICE

I hereby certify that the foregoing First Amended Complaint was served on:

Alex M. Duarte
Corporate Counsel
Qwest Corporation
421 SW Oak Street, Ste. 810
Portland, OR 97204
E-Mail: alex.duarte@qwest.com

Jason Eisdorfer
Energy Program Director
Citizens' Utility Board of Oregon
610 SW Broadway, Ste. 308
Portland, OR 97205
E-Mail: Jason@oregoncub.org

Gregory Romano
General Counsel
Verizon Corporate Services
MC WA0105RA
1800 41st Street
Everett, WA 98201
E-mail: Gregory.m.romano@verizon.com

Renee Willer
Manager Regulatory &
Government Affairs
Verizon Corporate Services
MC: OR030156
20575 NW Von Neumann Dr., Ste 150
Hillsboro, OR 97006-4771
E-mail: renee.willer@verizon.com

Citizens' Utility Board of Oregon
OPUC Dockets
610 SW Broadway, Ste. 308
Portland, OR 97205
E-Mail: dockets@oregoncub.org

by mailing to them a copy of the original thereof, contained in sealed envelopes, addressed as above set forth, with postage prepaid, and deposited in the mail in Portland, Oregon, on September 22, 2006.

Keith S. Dubanevich
Of Attorneys for Complainants

PDX_DOCS:379582.4 [30186-00114]

GARVEY SCHUBERT BARER
A PARTNERSHIP OF PROFESSIONAL CORPORATIONS
eleventh floor
121 s.w. morrison street
portland, oregon 97204-3141
(503) 228-3939

The New York Times
nytimes.com

December 15, 2005

Bush Secretly Lifted Some Limits on Spying in U. S. After 9/11, Officials Say

By JAMES RISEN
and ERIC LICHTBLAU

WASHINGTON, Dec. 15 -- Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials.

Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.

The previously undisclosed decision to permit some eavesdropping inside the country without court approval represents a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches.

"This is really a sea change," said a former senior official who specializes in national security law. "It's almost a mainstay of this country that the N.S.A. only does foreign searches."

Nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for The New York Times because of their concerns about the operation's legality and oversight.

According to those officials and others, reservations about aspects of the program have also been expressed by Senator John D. Rockefeller IV, the West Virginia Democrat who is the vice chairman of the Senate Intelligence Committee, and a judge presiding over a secret court that oversees intelligence matters. Some of the questions about the agency's new powers led the administration to temporarily suspend the operation last year and impose more restrictions, the officials said.

The Bush administration views the operation as necessary so that the agency can move quickly to monitor communications that may disclose threats to this country, the officials said. Defenders of the program say it has been a critical tool in helping disrupt terrorist plots and prevent attacks inside the United States.

Administration officials are confident that existing safeguards are sufficient to protect the privacy and civil liberties of Americans, the officials say. In some cases, they said, the Justice Department eventually seeks warrants if it wants to expand the eavesdropping to include communications confined within the United States. The officials said the administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court, the secret Washington court that deals with national security issues.

The White House asked The New York Times not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted.

While many details about the program remain secret, officials familiar with it said the N.S.A. eavesdropped without warrants on up to 500 people in the United States at any given time. The list changes as some names are added and others dropped, so the number monitored in this country may have reached into the thousands over the past three years, several officials said. Overseas, about 5,000 to 7,000 people suspected of terrorist ties are monitored at one time, according to those officials.

Several officials said the eavesdropping program had helped uncover a plot by Iyman Faris, an Ohio trucker and naturalized citizen who pleaded guilty in 2003 to supporting Al Qaeda by planning to bring down the Brooklyn Bridge with blowtorches. What appeared to be another Qaeda plot, involving fertilizer bomb attacks on British pubs and train stations, was exposed last year in part through the program, the officials said. But they said most people targeted for N.S.A. monitoring have never been charged with a crime, including an Iranian-American doctor in the South who came under suspicion because of what one official described as dubious ties to Osama bin Laden.

Dealing With a New Threat

The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials. In response, President Bush significantly eased limits on American intelligence and law enforcement agencies and the military.

But some of the administration's antiterrorism initiatives have provoked an outcry from members of

Congress, watchdog groups, immigrants and others who argue that the measures erode protections for civil liberties and intrude on Americans' privacy. Opponents have challenged provisions of the USA Patriot Act, the focus of contentious debate on Capitol Hill this week, that expand domestic surveillance by giving the Federal Bureau of Investigation more power to collect information like library lending lists or Internet use. Military and F.B.I. officials have drawn criticism for monitoring what were largely peaceful antiwar protests. The Pentagon and the Department of Homeland Security were forced to retreat on plans to use public and private databases to hunt for possible terrorists. And last year, the Supreme Court rejected the administration's claim that those labeled "enemy combatants" were not entitled to judicial review of their open-ended detention.

Mr. Bush's executive order allowing some warrantless eavesdropping on those inside the United States - including American citizens, permanent legal residents, tourists and other foreigners - is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups, according to the officials familiar with the N.S.A. operation.

The National Security Agency, which is based at Fort Meade, Md., is the nation's largest and most secretive intelligence agency, so intent on remaining out of public view that it has long been nicknamed "No Such Agency." It breaks codes and maintains listening posts around the world to eavesdrop on foreign governments, diplomats and trade negotiators as well as drug lords and terrorists. But the agency ordinarily operates under tight restrictions on any spying on Americans, even if they are overseas, or disseminating information about them.

What the agency calls a "special collection program" began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda operatives overseas, including Abu Zubaydah, who was arrested in Pakistan in March 2002. The C.I.A. seized the terrorists' computers, cellphones and personal phone directories, said the officials familiar with the program. The N.S.A. surveillance was intended to exploit those numbers and addresses as quickly as possible, the officials said.

In addition to eavesdropping on those numbers and reading e-mail messages to and from the Qaeda figures, the N.S.A. began monitoring others linked to them, creating an expanding chain. While most of the numbers and addresses were overseas, hundreds were in the United States, the officials said.

Under the agency's longstanding rules, the N.S.A. can target for interception phone calls or e-mail messages on foreign soil, even if the recipients of those communications are in the United States. Usually, though, the government can only target phones and e-mail messages in this country by first obtaining a court order from the Foreign Intelligence Surveillance Court, which holds its closed sessions at the Justice Department.

Traditionally, the F.B.I., not the N.S.A., seeks such warrants and conducts most domestic eavesdropping. Until the new program began, the N.S.A. typically limited its domestic surveillance to

foreign embassies and missions in Washington, New York and other cities, and obtained court orders to do so.

Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation. Under the special program, the agency monitors their international communications, the officials said. The agency, for example, can target phone calls from someone in New York to someone in Afghanistan.

Warrants are still required for eavesdropping on entirely domestic-to-domestic communications, those officials say, meaning that calls from that New Yorker to someone in California could not be monitored without first going to the Federal Intelligence Surveillance Court.

A White House Briefing

After the special program started, Congressional leaders from both political parties were brought to Vice President Dick Cheney's office in the White House. The leaders, who included the chairmen and ranking members of the Senate and House intelligence committees, learned of the N.S.A. operation from Mr. Cheney, Gen. Michael V. Hayden of the Air Force, who was then the agency's director and is now the principal deputy director of national intelligence, and George J. Tenet, then the director of the C.I.A., officials said.

It is not clear how much the members of Congress were told about the presidential order and the eavesdropping program. Some of them declined to comment about the matter, while others did not return phone calls.

Later briefings were held for members of Congress as they assumed leadership roles on the intelligence committees, officials familiar with the program said. After a 2003 briefing, Senator Rockefeller, the West Virginia Democrat who became vice chairman of the Senate Intelligence Committee that year, wrote a letter to Mr. Cheney expressing concerns about the program, officials knowledgeable about the letter said. It could not be determined if he received a reply. Mr. Rockefeller declined to comment. Aside from the Congressional leaders, only a small group of people, including several cabinet members and officials at the N.S.A., the C.I.A. and the Justice Department, know of the program.

Some officials familiar with it say they consider warrantless eavesdropping inside the United States to be unlawful and possibly unconstitutional, amounting to an improper search. One government official involved in the operation said he privately complained to a Congressional official about his doubts about the legality of the program. But nothing came of his inquiry. "People just looked the other way because they didn't want to know what was going on," he said.

A senior government official recalled that he was taken aback when he first learned of the operation. "My first reaction was, ‘We're doing what?' " he said. While he said he eventually felt that adequate

safeguards were put in place, he added that questions about the program's legitimacy were understandable.

Some of those who object to the operation argue that is unnecessary. By getting warrants through the foreign intelligence court, the N.S.A. and F.B.I. could eavesdrop on people inside the United States who might be tied to terrorist groups without skirting longstanding rules, they say.

The standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant - intelligence officials only have to show probable cause that someone may be "an agent of a foreign power," which includes international terrorist groups - and the secret court has turned down only a small number of requests over the years. In 2004, according to the Justice Department, 1,754 warrants were approved. And the Foreign Intelligence Surveillance Court can grant emergency approval for wiretaps within hours, officials say.

Administration officials counter that they sometimes need to move more urgently, the officials said. Those involved in the program also said that the N.S.A.'s eavesdroppers might need to start monitoring large batches of numbers all at once, and that it would be impractical to seek permission from the Foreign Intelligence Surveillance Court first, according to the officials.

Culture of Caution and Rules

The N.S.A. domestic spying operation has stirred such controversy among some national security officials in part because of the agency's cautious culture and longstanding rules.

Widespread abuses - including eavesdropping on Vietnam War protesters and civil rights activists - by American intelligence agencies became public in the 1970's and led to passage of the Foreign Intelligence Surveillance Act, which imposed strict limits on intelligence gathering on American soil. Among other things, the law required search warrants, approved by the secret F.I.S.A. court, for wiretaps in national security cases. The agency, deeply scarred by the scandals, adopted additional rules that all but ended domestic spying on its part.

After the Sept. 11 attacks, though, the United States intelligence community was criticized for being too risk-averse. The National Security Agency was even cited by the independent 9/11 Commission for adhering to self-imposed rules that were stricter than those set by federal law.

Several senior government officials say that when the special operation first began, there were few controls on it and little formal oversight outside the N.S.A. The agency can choose its eavesdropping targets and does not have to seek approval from Justice Department or other Bush administration officials. Some agency officials wanted nothing to do with the program, apparently fearful of participating in an illegal operation, a former senior Bush administration official said. Before the 2004 election, the official said, some N.S.A. personnel worried that the program might come under scrutiny by Congressional or criminal investigators if Senator John Kerry, the Democratic nominee, was elected

president.

In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it.

For the first time, the Justice Department audited the N.S.A. program, several officials said. And to provide more guidance, the Justice Department and the agency expanded and refined a checklist to follow in deciding whether probable cause existed to start monitoring someone's communications, several officials said.

A complaint from Judge Colleen Kollar-Kotelly, the federal judge who oversees the Federal Intelligence Surveillance Court, helped spur the suspension, officials said. The judge questioned whether information obtained under the N.S.A. program was being improperly used as the basis for F.I.S.A. wiretap warrant requests from the Justice Department, according to senior government officials. While not knowing all the details of the exchange, several government lawyers said there appeared to be concerns that the Justice Department, by trying to shield the existence of the N.S.A. program, was in danger of misleading the court about the origins of the information cited to justify the warrants.

One official familiar with the episode said the judge insisted to Justice Department lawyers at one point that any material gathered under the special N.S.A. program not be used in seeking wiretap warrants from her court. Judge Kollar-Kotelly did not return calls for comment.

A related issue arose in a case in which the F.B.I. was monitoring the communications of a terrorist suspect under a F.I.S.A.-approved warrant, even though the National Security Agency was already conducting warrantless eavesdropping. According to officials, F.B.I. surveillance of Mr. Faris, the Brooklyn Bridge plotter, was dropped for a short time because of technical problems. At the time, senior Justice Department officials worried what would happen if the N.S.A. picked up information that needed to be presented in court. The government would then either have to disclose the N.S.A. program or mislead a criminal court about how it had gotten the information.

The Civil Liberties Question

Several national security officials say the powers granted the N.S.A. by President Bush go far beyond the expanded counterterrorism powers granted by Congress under the USA Patriot Act, which is up for renewal. The House on Wednesday approved a plan to reauthorize crucial parts of the law. But final passage has been delayed under the threat of a Senate filibuster because of concerns from both parties over possible intrusions on Americans' civil liberties and privacy.

Under the act, law enforcement and intelligence officials are still required to seek a F.I.S.A. warrant every time they want to eavesdrop within the United States. A recent agreement reached by Republican leaders and the Bush administration would modify the standard for F.B.I. wiretap warrants, requiring, for instance, a description of a specific target. Critics say the bar would remain too low to prevent

abuses.

Bush administration officials argue that the civil liberties concerns are unfounded, and they say pointedly that the Patriot Act has not freed the N.S.A. to target Americans. "Nothing could be further from the truth," wrote John Yoo, a former official in the Justice Department's Office of Legal Counsel, and his co-author in a Wall Street Journal opinion article in December 2003. Mr. Yoo worked on a classified legal opinion on the N.S.A.'s domestic eavesdropping program.

At an April hearing on the Patriot Act renewal, Senator Barbara A. Mikulski, Democrat of Maryland, asked Attorney General Alberto R. Gonzales and Robert S. Mueller III, the director of the F.B.I., "Can the National Security Agency, the great electronic snooper, spy on the American people?"

"Generally," Mr. Mueller said, "I would say generally, they are not allowed to spy or to gather information on American citizens." President Bush did not ask Congress to include provisions for the N. S.A. domestic surveillance program as part of the Patriot Act and has not sought any other laws to authorize the operation. Bush administration lawyers argued that such new laws were unnecessary, because they believed that the Congressional resolution on the campaign against terrorism provided ample authorization, officials said.

Seeking Congressional approval was also viewed as politically risky because the proposal would be certain to face intense opposition on civil liberties grounds. The administration also feared that by publicly disclosing the existence of the operation, its usefulness in tracking terrorists would end, officials said.

The legal opinions that support the N.S.A. operation remain classified, but they appear to have followed private discussions among senior administration lawyers and other officials about the need to pursue aggressive strategies that once may have been seen as crossing a legal line, according to senior officials who participated in the discussions.

For example, just days after the Sept. 11, 2001, attacks on New York and the Pentagon, Mr. Yoo, the Justice Department lawyer, wrote an internal memorandum that argued that the government might use "electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses."

Mr. Yoo noted that while such actions could raise constitutional issues, in the face of devastating terrorist attacks "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."

The next year, Justice Department lawyers disclosed their thinking on the issue of warrantless wiretaps in national security cases in a little-noticed brief in an unrelated court case. In that 2002 brief, the government said that "the Constitution vests in the President inherent authority to conduct warrantless

intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority."

Administration officials were also encouraged by a November 2002 appeals court decision in an unrelated matter. The decision by the Foreign Intelligence Surveillance Court of Review, which sided with the administration in dismantling a bureaucratic "wall" limiting cooperation between prosecutors and intelligence officers, noted "the president's inherent constitutional authority to conduct warrantless foreign intelligence surveillance."

But the same court suggested that national security interests should not be grounds "to jettison the Fourth Amendment requirements" protecting the rights of Americans against undue searches. The dividing line, the court acknowledged, "is a very difficult one to administer."

--

For Immediate Release
Office of the Press Secretary
December 19, 2005

Press Conference of the President

The East Room

en Español

VIDEO Multimedia

President's Remarks

view

10:32 A.M. EST

THE PRESIDENT: Welcome. Please be seated. Thanks.

Last night I addressed the nation about our strategy for victory in Iraq, and the historic elections that took place in the country last week. In a nation that once lived by the whims of a brutal dictator, the Iraqi people now enjoy constitutionally protected freedoms, and their leaders now derive their powers from the consent of the government. Millions of Iraqis are looking forward to a future with hope and optimism.

The Iraqi people still face many challenges. This is the first time the Iraqis are forming a government under their new constitution. The Iraqi constitution requires a two-thirds vote of the parliament for certain top officials. So the formation of the new government will take time as Iraqis work to build consensus. And once the new Iraqi government assumes office, Iraq's new leaders will face many important decisions on issues such as security and reconstruction, economic reform and national unity. The work ahead will require the patience of the Iraqi people and the patience and support of America and our coalition partners.

As I said last night, this election does not mean the end of violence, but it is the beginning of something new: a constitutional democracy at the heart of the Middle East. And we will keep working toward our goal of a democratic Iraq that can govern and self-sustain itself and defend itself.

Our mission in Iraq is critical in the victory in the global war on terror. After our country was attacked on September the 11th and nearly 3,000 lives were lost, I vowed to do everything within my power to bring justice to those who were responsible. I also pledged to the American people to do everything within my power to prevent this from happening again. What we quickly learned was that al Qaeda was not a conventional enemy. Some lived in our cities and communities, and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere. Then they boarded our airplanes and launched the worst attack on our country in our nation's history.

This new threat required us to think and act differently. And as the 9/11 Commission pointed out, to prevent this from happening again, we need to connect the dots before the enemy attacks, not after. And we need to recognize that dealing with al Qaeda is not simply a matter of law enforcement; it requires defending the country against an enemy that declared war against the United States of America.

As President and Commander-in-Chief, I have the constitutional responsibility and the constitutional authority to protect our country. Article II of the Constitution gives me that responsibility and the authority necessary to fulfill it. And after September the 11th, the United States Congress also granted me additional authority to use military force against al Qaeda.

After September the 11th, one question my administration had to answer was how, using the authorities I have, how do we effectively detect enemies hiding in our midst and prevent them from striking us again? We know that a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives. To save American lives, we must be able to act fast and to detect these conversations so we can prevent new attacks.

So, consistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to al Qaeda and related terrorist organizations. This program is carefully reviewed approximately every 45 days to ensure it is being used properly. Leaders in the United States Congress have been briefed more than a dozen times on this program. And it has been effective in disrupting the enemy, while safeguarding our civil liberties.

This program has targeted those with known links to al Qaeda. I've reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for so long as our nation is -- for so long as the nation faces the continuing threat of an enemy that wants to kill American citizens.

Another vital tool in the war on terror is the Patriot Act. After September the 11th, Congress acted quickly and responsibly by passing this law, which provides our law enforcement and intelligence community key tools to prevent attacks in our country. The Patriot Act tore down the legal and bureaucratic wall that kept law enforcement and intelligence authorities from sharing vital information about terrorist threats. It allows federal investigators to pursue terrorists with tools already used against other types of criminals. America's law enforcement personnel have used this critical tool to prosecute terrorist operatives and their supporters, and to breakup cells here in America.

Yet, key provisions of this law are set to expire in 12 days. The House of Representatives voted for reauthorization, but last week, a minority of senators filibustered the Patriot Act, blocking the Senate from voting to reauthorize key provisions of this vital law. In fact, the Senate Democratic leader boasted to a group of political supporters that the Senate Democrats had "killed the Patriot Act." Most of the senators now filibustering the Patriot Act actually voted for it in 2001. These senators need to explain why they thought the Patriot Act was a vital tool after the September the 11th attacks, but now think it's no longer necessary.

The terrorists want to strike America again, and they hope to inflict even greater damage than they did on September the 11th. Congress has a responsibility to give our law enforcement and intelligence officials the tools they need to protect the American people. The senators who are filibustering the Patriot Act must stop their delaying tactics, and the Senate must vote to reauthorize the Patriot Act. In the war on terror, we cannot afford to be without this law for a single moment.

As we fight the war on terror, we'll also continue to work to build prosperity for our citizens. Because we cut taxes and restrained non-security spending, our economy is strong and it is getting stronger. We added 215,000 new jobs in November. We've added nearly 4.5 million new jobs since May of 2003. The unemployment rate is down to 5 percent, lower than the average of the 1970s, 1980s and 1990s. Despite hurricanes and high gas prices, third quarter growth was 4.3 percent. More Americans own their own homes than at any time in our history. Inflation is low, productivity is high and consumer confidence is up. We're heading into a new year with an economy that is the envy of the world, and we have every reason to be optimistic about our economic future.

We made other important progress this year on the priorities of American families. We passed a good energy bill,

and we're putting America on the path to make our economy less dependent on foreign sources of oil. We were wise with taxpayer's money and cut non-security discretionary spending below last year's level. We passed the Central American Dominican Republic Free Trade Agreement to open up markets and help level the playing field for America's workers and farmers and small businesses. We passed bankruptcy reform and class action lawsuit reform. I appointed John Roberts as the 17th Chief Justice of the United States. Chief Justice Roberts is poised to lead the Supreme Court with integrity and prudence for decades to come.

We've got more work to do in this coming year. To keep our economy growing, we need to keep taxes low, and make the tax relief permanent. We must restrain government spending, and I'm pleased that the House today has voted to rein in entitlement spending by $40 billion, and I urge the United States Senate to join them. We must reduce junk lawsuits and strengthen our education system and give more Americans the ability to obtain affordable health insurance. We must pass comprehensive immigration reform that protects our borders, strengthens enforcement and creates a new temporary worker program that relieves pressure on the border, but rejects amnesty.

I look forward to the Senate holding an up or down vote on Judge Sam Alito and confirming him by January 20th as Associate Justice of the Supreme Court. Judge Alito has more prior judicial experience than any Supreme Court nominee in more than 70 years. He's a highly respected and principled jurist and he will make our nation proud as a member of the high court.

As we prepare to spend time with our families this holiday season, we also stop to count our blessings. We're thankful for our courageous men and women in uniform who are spending the holidays away from loved ones, standing watch for liberty in distant lands. We give thanks for our military families who love and support them in their vital work, and who also serve our country. And we pray for the families of the fallen heroes. We hold them in our hearts and we lift them up in our prayers and we pledge that the sacrifice of their loved ones will never be forgotten.

I'll be glad to answer some questions here, starting with you, Terry.

Q Mr. President, thank you, sir. Are you going to order a leaks investigation into the disclosure of the NSA surveillance program? And why did you skip the basic safeguard of asking courts for permission for these intercepts?

THE PRESIDENT: Let me start with the first question. There is a process that goes on inside the Justice Department about leaks, and I presume that process is moving forward. My personal opinion is it was a shameful act for someone to disclose this very important program in a time of war. The fact that we're discussing this program is helping the enemy.

You've got to understand -- and I hope the American people understand -- there is still an enemy that would like to strike the United States of America, and they're very dangerous. And the discussion about how we try to find them will enable them to adjust. Now, I can understand you asking these questions and if I were you, I'd be asking me these questions, too. But it is a shameful act by somebody who has got secrets of the United States government and feels like they need to disclose them publicly.

Let me give you an example about my concerns about letting the enemy know what may or may not be happening. In the late 1990s, our government was following Osama bin Laden because he was using a certain type of telephone. And then the fact that we were following Osama bin Laden because he was using a certain type of telephone made it into the press as the result of a leak. And guess what happened? Saddam -- Osama bin Laden changed his behavior. He began to change how he communicated.

We're at war, and we must protect America's secrets. And so the Justice Department, I presume, will proceed forward with a full

investigation. I haven't ordered one, because I understand there's
kind of a natural progression that will take place when this kind of leak emerges.

The second part of the question is? Sorry -- I gave a long answer.

Q It was, why did you skip the basic safeguards of asking courts for permission for the intercepts?

THE PRESIDENT: First of all, I -- right after September the 11th, I knew we were fighting a different kind of war. And so I asked people in my administration to analyze how best for me and our government to do the job people expect us to do, which is to detect and prevent a possible attack. That's what the American people want. We looked at the possible scenarios. And the people responsible for helping us protect and defend came forth with the current program, because it enables us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent.

We use FISA still -- you're referring to the FISA court in your question -- of course, we use FISAs. But FISA is for long-term monitoring. What is needed in order to protect the American people is the ability to move quickly to detect.

Now, having suggested this idea, I then, obviously, went to the question, is it legal to do so? I am -- I swore to uphold the laws. Do I have the legal authority to do this? And the answer is, absolutely. As I mentioned in my remarks, the legal authority is derived from the Constitution, as well as the authorization of force by the United States Congress.

Adam.

Q Mr. President, you have hailed the Iraqi elections as a success, but some lawmakers say you are not focusing on the threat of civil war. Do you fear a civil war? And how hard will you push Iraq's competing political parties to get a government and a constitutional compromise?

THE PRESIDENT: I appreciate that. We look at all contingencies, but my optimism about a unified Iraq moving forward was confirmed when over 10 million people went to the polls under a -- and voted for a government under a new constitution. Constitutions tend to bind societies.

Now, there are some things we've got to watch, Adam, for certain. One, is we've got to help the Iraqi government as best as they need help, to stand up a government as quickly as possible. In other words, we're urging them: don't delay, move as quickly as you can, solve the -- get the political parties -- once the vote is completed, get the political parties together and come up with a government.

And it's going to take a while, because, first of all, the ballots won't be fully counted, I guess, until early January. And then, as I mentioned in my remarks, it take a two-thirds vote to -- first, to seat certain officials. Sometimes it's hard to achieve a two-thirds vote in legislative bodies. How about the Senate, for example? (Laughter.) But, nevertheless, it's going to take a while. And the American people have got to understand that we think in terms of elections, most of our elections end the day after the election. Sometimes they don't, Adam. (Laughter.) And so you're going to see a lot of give-and-take, and it's important for us to get this process moving forward.

Secondly, there is an opportunity to amend the constitution. You remember that was part of the deal with the Iraqis, in order to get this process moving. And we'll want to make sure we're monitoring and involved with that part. In other words, involvement doesn't mean telling the sovereign government what to do; involvement means giving advice as to how to move forward so a country becomes more unified. And I'm very optimistic about the way forward for the Iraqi people.

And the reason why is based upon the fact that the Iraqis have shown incredible courage. Think about what has happened in a brief period of time -- relatively brief. I know with all the TV stations and stuff in America, two-and-a-half years seems like an eternity. But in the march of history, it's not all that long. They have gone from tyranny to an amazing election last December. If I'd have stood up here a year ago, in one of my many press conferences, and told you that in the -- next year I make this prediction to you, that over 10 million Iraqis, including many Sunnis, will vote for a permanent government, I think you probably would have said, there he goes again.

But it happened. And it happened because the Iraqis want to live in a free society. And what's important about this election is that Iraq will become an ally in the war on terror, and Iraq will serve as a beacon for what is possible; a beacon of freedom in a part of the world that is desperate for freedom and liberty. And as I say in my speeches, a free Iraq will serve as such an optimistic and hopeful example for reformers from Tehran to Damascus. And that's an important part of a strategy to help lay the foundation of peace for generations.

John.

Q Thank you, Mr. President. So many questions, so little time.

THE PRESIDENT: Well, keep your question short, then. (Laughter.)

Q I'll do my best, sir. But, sir, you've shown a remarkable spirit of candor in the last couple of weeks in your conversation and speeches about Iraq. And I'm wondering if, in that spirit, I might ask you a question that you didn't seem to have an answer for the last time you were asked, and that is, what would you say is the biggest mistake you've made during your presidency, and what have you learned from it?

THE PRESIDENT: Answering Dickerson's question. No, I -- the last time those questions were asked, I really felt like it was an attempt for me to say it was a mistake to go into Iraq. And it wasn't a mistake to go into Iraq. It was the right decision to make.

I think that, John, there's going to be a lot of analysis done on the decisions on the ground in Iraq. For example, I'm fully aware that some have said it was a mistake not to put enough troops there immediately -- or more troops. I made my decision based upon the recommendations of Tommy Franks, and I still think it was the right decision to make. But history will judge.

I said the other day that a mistake was trying to train a civilian defense force and an Iraqi army at the same time, but not giving the civilian defense force enough training and tools necessary to be able to battle a group of thugs and killers. And so we adjusted.

And the point I'm trying to make to the American people in this, as you said, candid dialogue -- I hope I've been candid all along; but in the candid dialogue -- is to say, we're constantly changing our tactics to meet the changing tactics of an enemy. And that's important for our citizens to understand.

Thank you. Kelly.

Q Thank you, Mr. President. If you believe that present law needs to be faster, more agile concerning the surveillance of conversations from someone in the United States to someone outside the country --

THE PRESIDENT: Right.

Q -- why, in the four years since 9/11, has your administration not sought to get changes in the law instead of bypassing it, as some of your critics have said?

THE PRESIDENT: I appreciate that. First, I want to make clear to the people listening that this program is limited in nature to those that are known al Qaeda ties and/or affiliates. That's important. So it's a program that's limited, and you brought up something that I want to stress, and that is, is that these calls are not intercepted within the country. They are from outside the country to in the country, or vice versa. So in other words, this is not a -- if you're calling from Houston to L.A., that call is not monitored. And if there was ever any need to monitor, there would be a process to do that.

I think I've got the authority to move forward, Kelly. I mean, this is what -- and the Attorney General was out briefing this morning about why it's legal to make the decisions I'm making. I can fully understand why members of Congress are expressing concerns about civil liberties. I know that. And it's -- I share the same concerns. I want to make sure the American people understand, however, that we have an obligation to protect you, and we're doing that and, at the same time, protecting your civil liberties.

Secondly, an open debate about law would say to the enemy, here is what we're going to do. And this is an enemy which adjusts. We monitor this program carefully. We have consulted with members of the Congress over a dozen times. We are constantly reviewing the program. Those of us who review the program have a duty to uphold the laws of the United States, and we take that duty very seriously.

Let's see here -- Martha. Working my way around the electronic media, here.

Q Thank you, Mr. President. You say you have an obligation to protect us. Then why not monitor those calls between Houston and L.A.? If the threat is so great, and you use the same logic, why not monitor those calls? Americans thought they weren't being spied on in calls overseas -- why not within the country, if the threat is so great?

THE PRESIDENT: We will, under current law, if we have to. We will monitor those calls. And that's why there is a FISA law. We will apply for the right to do so. And there's a difference -- let me finish -- there is a difference between detecting so we can prevent, and monitoring. And it's important to know the distinction between the two.

Q But preventing is one thing, and you said the FISA laws essentially don't work because of the speed in monitoring calls overseas.

THE PRESIDENT: I said we use the FISA courts to monitor calls. It's a very important tool, and we do use it. I just want to make sure we've got all tools at our disposal. This is an enemy which is quick and it's lethal. And sometimes we have to move very, very quickly. But if there is a need, based upon evidence, we will take that evidence to a court, in order to be able to monitor calls within the United States.

Who haven't I called on, let's see here. Suzanne.

Q Democrats have said that you have acted beyond law, and that you have even broken the law. There are some Republicans who are calling for congressional hearings and even an independent investigation. Are you willing to go before members of Congress and explain this eavesdropping program? And do you support an independent investigation?

THE PRESIDENT: We have been talking to members of the United States Congress. We have met with them over 12 times. And it's important for them to be brought into this process. Again, I repeat, I understand people's concerns. But I also want to assure the American people that I am doing what you expect me to do, which is to safeguard civil liberties and at the same time protect the United States of America. And we've explained the authorities under which I'm making our decisions, and will continue to do so.

Secondly, there is a committee -- two committees on the Hill which are responsible, and that's the Intelligence Committee. Again, any public hearings on programs will say to the enemy, here's what they do; adjust. This is a war. Of course we consult with Congress and have been consulting with Congress and will continue to do so.

Wendell. You got a little problem there, Wendell? (Laughter.)

Q I'm caught, Mr. President.

THE PRESIDENT: Oh, you're caught. (Laughter.) Liberate him. (Laughter.)

Q You talked about your decision to go to war and the bad intelligence, and you've carefully separated the intelligence from the decision, saying that it was the right decision to go to war despite the problems with the intelligence, sir. But, with respect, the intelligence helped you build public support for the war. And so I wonder if now, as you look back, if you look at that intelligence and feel that the intelligence and your use of it might bear some responsibility for the current divisions in the country over the war, and what can you do about it?

THE PRESIDENT: I appreciate that. First of all, I can understand why people were -- well, wait a minute. Everybody thought there was weapons of mass destruction, and there weren't any. I felt the same way. We looked at the intelligence and felt certain that Saddam Hussein had weapons of mass destruction. Intelligence agencies around the world felt the same way, by the way. Members of the United States Congress looked at the

National Intelligence Estimate -- same intelligence estimate I looked at -- and came to the same conclusion, Wendell.

So in other words, there was universal -- there was a universal feeling that he had weapons of mass destruction. As a matter of fact, it was so universal that the United Nations Security Council passed numerous resolutions. And so when the weapons weren't there, like many Americans, I was concerned and wondered why. That's why we set up the Silberman-Robb Commission to address intelligence shortfalls, to hopefully see to it that this kind of situation didn't arise.

Now, having said all that, what we did find after the war was that Saddam Hussein had the desire to -- or the liberation -- Saddam had the desire to reconstitute his weapons programs. In other words, he had the capacity to reconstitute them. America was still his enemy. And of course, he manipulated the oil-for-food program in the hopes of ending sanctions. In our view, he was just waiting for the world to turn its head, to look away, in order to reconstitute the programs. He was dangerous then. It's the right decision to have removed Saddam.

Now, the American people -- I will continue to speak to the American people on this issue, to not only describe the decision-making process but also the way forward. I gave a speech prior to the liberation of Iraq, when I talked about a broader strategic objective, which is the establishment of democracy. And I've talked about democracy in Iraq. Certainly it's not the only rationale; I'm not claiming that. But I also want you to review that speech so that you get a sense for not only the desire to remove a threat, but also the desire to help establish democracy. And the amazing thing about -- in Iraq, as a part of a broader strategy, to help what I call "lay the foundation of peace," democracies don't war; democracies are peaceful countries.

And what you're seeing now is an historic moment, because I believe democracies will spread. I believe when people get the taste for freedom or see a neighbor with a taste for freedom, they will demand the same thing, because I believe in the universality of freedom. I believe everybody has the desire to be free. I recognize some don't believe that, which basically condemns some to tyranny. I strongly believe that deep in everybody's soul is the desire to live in liberty, and if given a chance, they will choose that path. And it's not easy to do that. The other day, I gave a speech and talked about how our road to our Constitution, which got amended shortly after it was approved, was pretty bumpy. We tried the Articles of Confederation. It didn't work. There was a lot of, kind of, civil unrest. But, nevertheless, deep in the soul is the desire to live in liberty, people -- make the -- have got the patience and the steadfastness to achieve that objective. And that is what we're seeing in Iraq.

And it's not going to be easy. It's still going to be hard, because we're getting rid of decades of bitterness. If you're a -- you know, you find these secret prisons where people have been tortured, that's unacceptable. And, yet, there are some who still want to have retribution against people who harmed them.

Now, I'll tell you an amazing story -- at least I thought it was amazing. We had people -- first-time voters, or voters in the Iraqi election come in to see me in the Oval. They had just voted that day, and they came in. It was exciting to talk to people. And one person said, how come you're giving Saddam Hussein a trial? I said, first of all, it's your government, not ours. She said, he doesn't deserve a trial; he deserves immediate death for what he did to my people. And it just struck me about how strongly she felt about the need to not have a rule of law, that there needed to be quick retribution, that he didn't deserve it. And I said to her, don't you see that the trial, itself, stands in such contrast to the tyrant that that in itself is a victory for freedom and a defeat for tyranny -- just the trial alone. And it's important that there be rule of law.

My only point to you is there's a lot of work to get rid of the past, yet we're headed in the right direction. And it's an exciting moment in history.

Stretch.

Q Thank you, Mr. President. Getting back to the domestic spying issue for a moment. According to FISA's own records, it's received nearly 19,000 requests for wiretaps or search warrants since 1979, rejected just five of them. It also operates in secret, so security shouldn't be a concern, and it can be applied retroactively. Given such a powerful tool of law enforcement is at your disposal, sir, why did you see fit to sidetrack that process?

THE PRESIDENT: We used the process to monitor. But also, this is a different -- a different era, a different war, Stretch. So what we're -- people are changing phone numbers and phone calls, and they're moving quick. And

we've got to be able to detect and prevent. I keep saying that, but this is a -- it requires quick action.

And without revealing the operating details of our program, I just want to assure the American people that, one, I've got the authority to do this; two, it is a necessary part of my job to protect you; and, three, we're guarding your civil liberties. And we're guarding the civil liberties by monitoring the program on a regular basis, by having the folks at NSA, the legal team, as well as the inspector general, monitor the program, and we're briefing Congress. This is a part of our effort to protect the American people. The American people expect us to protect them and protect their civil liberties. I'm going to do that. That's my job, and I'm going to continue doing my job.

Let's see here -- Sanger.

Q Thank you, Mr. President. Following up on Wendell's question about the intelligence failures ahead of Iraq, one of the side effects appears to have been that the United States has lost some credibility with its allies when it goes to them with new intelligence. You, for example, your administration, has been sharing with some of your allies the contents of a laptop computer that was found in Iran concerning their nuclear program. Yet you are still having --

THE PRESIDENT: Is that classified? (Laughter.) No, never mind, Sanger.

Q Yet you are still having some difficulty convincing people that Iran has a nuclear program. Can you tell us whether or not you think one of the side effects of the intelligence failure has been that it has limited your ability to deal with future threats like Iran, like North Korea, or any other future threats concerning terrorists?

THE PRESIDENT: Sanger, I hate to admit it, but that's an excellent question. No question, that the intelligence failure on weapons of mass destruction caused all intelligence services to have to step back and reevaluate the process of gathering and analyzing intelligence -- no doubt about that. And so there's been a lot of work done to work with other intelligence agencies to share information about what went right and what went wrong, as well as to build credibility among all services.

I think, David, where it is going to be most difficult to make the case is in the public arena. People will say, if we're trying to make the case on Iran, well, the intelligence failed in Iraq, therefore, how can we trust the intelligence in Iran? And part of the reason why there needs to be a public message on this is because the first hope and the first step is a diplomatic effort to get the Iranians to comply with the demands of the free world. If they don't, there's -- along the diplomatic path, there's always the United Nations Security Council. But that case of making -- beginning to say to the Iranians, there are consequences for not behaving, requires people to believe that the Iranian nuclear program is, to a certain extent, ongoing. And so we're working hard on that. I mean, it's no question that the credibility of intelligence is necessary for good diplomacy.

Q Do you intend to make that case publicly, too? You haven't yet laid out the evidence on Iran --

THE PRESIDENT: Well, I think that the best place to make the case now is still in the councils of government and convincing the EU3, for example, to continue working the diplomatic angle. Of course, we want this to be solved diplomatically, and we want the Iranians to hear a unified voice. I think people believe that -- I know this: People know that an Iran with the capacity to manufacture a nuclear weapon is not in the world's interest. That's universally accepted. And that should be accepted universally, particularly after what the President recently said about the desire to annihilate, for example, an ally of the United States.

And so the idea of Iran having a nuclear weapon is -- people say, well, we can't let that happen. The next step is to make sure that the world understands that the capacity to enrich uranium for a civilian program would lead to a weapons program. And so therefore we cannot allow the Iranians to have the capacity to enrich. One of the reasons why I proposed working with the Russians, the Russian idea of allowing Iran to have a civilian nuclear power plant industry without enriched material -- in other words, the enriched materials -- without enriching material, the enriching material would come from Russia, in this case, and be picked up by the Russians, was to prevent them from having the capacity to develop a nuclear weapon.

So I think there's universal agreement that we don't want them to have a weapon. And there is agreement that they should not be allowed to learn how to make a weapon. And beyond that, I think that's all I'm going to say.

But, appreciate it. Baker.

Q Thank you, Mr. President. I wonder if you can tell us today, sir, what, if any, limits you believe there are or should be on the powers of a President during a war, at wartime? And if the global war on terror is going to last for decades, as has been forecast, does that mean that we're going to see, therefore, a more or less permanent expansion of the unchecked power of the executive in American society?

THE PRESIDENT: First of all, I disagree with your assertion of "unchecked power."

Q Well --

THE PRESIDENT: Hold on a second, please. There is the check of people being sworn to uphold the law, for starters. There is oversight. We're talking to Congress all the time, and on this program, to suggest there's unchecked power is not listening to what I'm telling you. I'm telling you, we have briefed the United States Congress on this program a dozen times.

This is an awesome responsibility to make decisions on behalf of the American people, and I understand that, Peter. And we'll continue to work with the Congress, as well as people within our own administration, to constantly monitor programs such as the one I described to you, to make sure that we're protecting the civil liberties of the United States. To say "unchecked power" basically is ascribing some kind of dictatorial position to the President, which I strongly reject.

Q What limits do you --

THE PRESIDENT: I just described limits on this particular program, Peter. And that's what's important for the American people to understand. I am doing what you expect me to do, and at the same time, safeguarding the civil liberties of the country.

John.

Q Thank you, sir. Looking ahead to this time next year, what are the top three or top five -- take your pick -- accomplishments that you hope to have achieved? And in particular, what is your best-case scenario for troop levels in Iraq at this time next year?

THE PRESIDENT: This is kind of like -- this is the ultimate benchmark question. You're trying to not only get me to give benchmarks in Iraq, but also benchmarks domestically.

I hope the world is more peaceful. I hope democracy continues to take root around the world. And I hope people are able to find jobs. The job base of this country is expanding, and we need to keep it that way. We want people working. I want New Orleans and Mississippi to be better places. I appreciate very much the progress that Congress is making toward helping a vision of New Orleans rising up and the Gulf Coast of Mississippi being reconstructed. I think we can make good progress down there.

One of the key decisions our administration has made is to make sure that the levees are better than they were before Katrina in New Orleans. That will help -- people will have the confidence necessary to make investments and to take risk and to expand.

I appreciate the Congress, and I'm looking forward to the Senate affirming the U.S. Congress' decisions to fund the education or reimburse states for education. There's some good health care initiatives in the bill. We want to make sure that people don't get booted out of housing. We want to work carefully to make sure people understand that there are benefits or help available for them to find housing. We want to continue to move temporary housing on the Gulf Coast of Mississippi so people can get better -- closer to their neighborhoods, and get their homes rebuilt. We want to start helping Mayor Nagin get temporary housing near New Orleans so as this economy comes back people will be able to find jobs.

I appreciate the fact that the Congress passed the GO Zone tax incentives in order to attract capital into the region. So one of my hopes is, is that people are able to find hope and optimism after the Katrina disaster down

there, that people's lives get up and running again, that people see a brighter future. I've got a lot of hopes, and I'm looking forward to working with Congress to get those -- to achieve some big goals.

Joe.

Q (Inaudible.)

THE PRESIDENT: You see, I hope by now you've discovered something about me, that when I say we're not going to have artificial timetables of withdrawal, and/or try to get me out on a limb on what the troop levels will look like -- the answer to your question on troop levels is, it's conditions-based. We have an objective in Iraq, and as we meet those objectives, our commanders on the ground will determine the size of the troop levels.

Nice try. End of your try.

Joe.

Q Mr. President, you said last night that there were only two options in Iraq -- withdraw or victory. And you asked Americans, especially opponents of the war, to reject partisan politics. Do you really expect congressional Democrats to end their partisan warfare and embrace your war strategy? And what can you do about that to make that happen?

THE PRESIDENT: Actually, I said that victory in Iraq is much larger than a person, a President, or a political party. And I've had some good visits with Senate and House Democrats about the way forward. They share the same concerns I share. You know, they want our troops out of Iraq as quickly as possible, but they don't want to do so without achieving a victory. These are good, solid Americans that agree that we must win for the sake of our security. And I'm interested in, Joe, their ideas, and will continue to listen carefully to their ideas.

On the other hand, there are some in this country that believe, strongly believe that we ought to get out now. And I just don't agree with them. It's a wrong strategy, and I'd like to tell you again why. One, it would dishearten the Iraqis. The Iraqis are making a great -- showing great courage to setting up a democracy. And a democracy in Iraq -- I know I've said this, and I'm going to keep saying it because I want the American people to understand -- a democracy in Iraq is vital in the long run to defeating terrorism. And the reason why is, is because democracy is hopeful and optimistic.

Secondly, it sends the wrong signal to our troops. We've got young men and women over their sacrificing. And all of a sudden, because of politics or some focus group or some poll, they stand up and say, we're out of there. I can't think of anything more dispiriting to a kid risking his or her life than to see decisions made based upon politics.

Thirdly, it sends the wrong signal to the enemy. It just says, wait them out; they're soft, they don't have the courage to complete the mission -- all we've got to do is continue to kill and get these images on the TV screens, and the Americans will leave. And all that will do is embolden these people. Now, I recognize there is a debate in the country, and I fully understand that, about the nature of the enemy. I hear people say, because we took action in Iraq, we stirred them up, they're dangerous. No, they were dangerous before we went into Iraq. That's what the American people have got to understand. That's why I took the decision I took on the NSA decision, because I understand how dangerous they are. And they want to hit us again.

Let me say something about the Patriot Act, if you don't mind. It is inexcusable for the United States Senate to let this Patriot Act expire. You know, there's an interesting debate in Washington, and you're part of it, that says, well, they didn't connect the dots prior to September the 11th -- "they" being not only my administration, but previous administrations. And I understand that debate. I'm not being critical of you bringing this issue up and discussing it, but there was a -- you might remember, if you take a step back, people were pretty adamant about hauling people up to testify, and wondering how come the dots weren't connected.

Well, the Patriot Act helps us connect the dots. And now the United States Senate is going to let this bill expire. Not the Senate -- a minority of senators. And I want senators from New York or Los Angeles or Las Vegas to go home and explain why these cities are safer. It is inexcusable to say, on the one hand, connect the dots, and not

give us a chance to do so. We've connected the dots, or trying to connect the dots with the NSA program. And, again, I understand the press and members of the United States Congress saying, are you sure you're safeguarding civil liberties. That's a legitimate question, and an important question. And today I hope I'll help answer that. But we're connecting dots as best as we possibly can.

I mentioned in my radio address -- my live TV radio address -- that there was two killers in San Diego making phone calls prior to the September the 11th attacks. Had this program been in place then, it is more likely we would have been able to catch them. But they're making phone calls from the United States, overseas, talking about -- who knows what they're talking about, but they ended up killing -- being a part of the team that killed 3,000 Americans. And so -- I forgot what got me on the subject, but nevertheless I'm going to -- we're doing the right thing.

April.

Q Mr. President, in making the case for domestic spying, could you tell us about the planned attacks on the U.S. that were thwarted through your domestic spying plan? And also, on the issue of race, since you brought up the issue of Katrina, 2005 gave us your defense of yourself on race, and some are still not sold on that. In 2006, what are you giving to the nation on the issue of race, as we're looking to the renewal of the Voting Rights Act in 2007 and things of that nature?

THE PRESIDENT: Yes, thanks. April, the fact that some in America believe that I am not concerned about race troubles me. One of the jobs of the President is to help people reconcile and to move forward and to unite. One of the most hurtful things I can hear is, Bush doesn't care about African Americans, for example. First of all, it's not true. And, secondly, I believe that -- obviously I've got to do a better job of communicating, I guess, to certain folks, because my job is to say to people, we're all equally American, and the American opportunity applies to you just as much as somebody else. And so I will continue to do my best, April, to reach out.

Now, you talked about -- and we have an opportunity, by the way, in New Orleans, for example, to make sure the education system works, to make sure that we promote ownership. I think it is vitally important for ownership to extend to more than just a single community. I think the more African Americans own their own business, the better off America is. I feel strongly that if we can get people to own and manage their own retirement accounts, like personal accounts and Social Security, it makes society a better place. I want people to be able to say, this is my asset. Heretofore, kind of asset accumulation may have been only a part of -- a single -- a part of -- a segmented part of our strategy. We want assets being passed from one generation to the next. I take pride in this statistic, that more African Americans own a home or more minorities own a home now than ever before in our nation's history, not just African Americans; that's positive.

I still want to make sure, though, that people understand that I care about them and that my view of the future, a bright future, pertains to them as much as any other neighborhood.

Now, you mentioned it's the Voting Rights Act. Congress needs to reauthorize it and I'll sign it.

The other question was?

Q Sir --

THE PRESIDENT: You asked a multiple-part question.

Q Yes, I did.

THE PRESIDENT: Thank you for violating the multiple-part question rule.

Q I didn't know there was a law on that. (Laughter.)

THE PRESIDENT: There's not a law. It's an executive order. (Laughter.) In this case, not monitored by the Congress -- (laughter) -- nor is there any administrative oversight. (Laughter.)

Q Well, without breaking any laws, on to -- back on domestic spying. Making the case for that, can you give us some example --

THE PRESIDENT: Oh, I got you. Yes, sorry. No, I'm not going to talk about that, because it would help give the enemy notification and/or, perhaps, signal to them methods and uses and sources. And we're not going to do that, which is -- it's really important for people to understand that the protection of sources and the protections of methods and how we use information to understand the nature of the enemy is secret. And the reason it's secret is because if it's not secret, the enemy knows about it, and if the enemy knows about it, adjusts.

And again, I want to repeat what I said about Osama bin Laden, the man who ordered the attack that killed 3,000 Americans. We were listening to him. He was using a type of cell phone, or a type of phone, and we put it in the newspaper -- somebody put it in the newspaper that this was the type of device he was using to communicate with his team, and he changed. I don't know how I can make the point more clear that any time we give up -- and this is before they attacked us, by the way -- revealing sources, methods, and what we use the information for simply says to the enemy: change.

Now, if you don't think there's an enemy out there, then I can understand why you ought to say, just tell us all you know. I happen to know there's an enemy there. And the enemy wants to attack us. That is why I hope you can feel my passion about the Patriot Act. It is inexcusable to say to the American people, we're going to be tough on terror, but take away the very tools necessary to help fight these people. And by the way, the tools exist still to fight medical fraud, in some cases, or other -- drug dealers. But with the expiration of the Patriot Act, it prevents us from using them to fight the terrorists. Now, that is just unbelievable. And I'm going to continue talking about this issue and reminding the American people about the importance of the Patriot Act and how necessary it is for us in Washington, D.C. to do our job to protect you.

Let's see, who else? Jackson -- Action Jackson. Got him a new job and everything.

Q Thank you, sir. One of the things we've seen this year is the reduction in your approval rating. And I know how you feel about polls, but it appears to be taking something out of your political clout, as evidenced by the Patriot Act vote. What do you attribute your lower polls to, and are you worried that independents are losing confidence in your leadership?

THE PRESIDENT: David, my job is to confront big challenges and lead. And I fully understand everybody is not going to agree with my decisions. But the President's job is to do what he thinks is right, and that's what I'm going to continue to do.

Secondly, if people want to play politics with the Patriot Act, it's -- let me just put it -- it's not in the best interests of the country, David. And yesterday -- or this morning I spoke to the Speaker, who called me. He said, Mr. President, we had a pretty good couple of days; got your budget passed, got the Katrina relief package going forward; we're supporting our troops; we've got the free trade -- we talked about passing CAFTA in the past. I mean, we've done a lot. And it's good for the country, by the way.

So I'm just going to keep doing my job. Maybe you can keep focusing on all these focus groups and polls, and all that business. My job is to lead, keep telling the American people what I believe, work to bring people together to achieve a common objective, stand on principle, and that's the way I'm going to lead. I did so in 2005, and I'm going to do so in 2006.

Thank you all for coming, and happy holidays to you. Appreciate it.

END 11:28 A.M. EST

NSA has massive database of Americans' phone calls

Updated 5/11/2006 10:38 AM ET
By Leslie Cauley, USA TODAY

The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth, people with direct knowledge of the arrangement told USA TODAY.

The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans — most of whom aren't suspected of any crime. This program does not involve the NSA listening to or recording conversations. But the spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity, sources said in separate interviews.

QUESTIONS AND ANSWERS: The NSA record collection program

"It's the largest database ever assembled in the world," said one person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation. The agency's goal is "to create a database of every call ever made" within the nation's borders, this person added.

For the customers of these companies, it means that the government has detailed records of calls they made — across town or across the country — to family members, co-workers, business contacts and others.

The three telecommunications companies are working under contract with the NSA, which launched the program in 2001 shortly after the Sept. 11 terrorist attacks, the sources said. The program is aimed at identifying and tracking suspected terrorists, they said.

The sources would talk only under a guarantee of anonymity because the NSA program is secret.

Air Force Gen. Michael Hayden, nominated Monday by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic call-tracking program. Hayden declined to comment about the program.

The NSA's domestic program, as described by sources, is far more expansive than what the White House has acknowledged. Last year, Bush said he had authorized the NSA to eavesdrop — without warrants — on international calls and international e-mails of people suspected of having links to terrorists when one party to the communication is in the USA. Warrants have also not been used in the NSA's efforts to create a national

call database.

In defending the previously disclosed program, Bush insisted that the NSA was focused exclusively on international calls. "In other words," Bush explained, "one end of the communication must be outside the United States."

As a result, domestic call records — those of calls that originate and terminate within U.S. borders — were believed to be private.

Sources, however, say that is not the case. With access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans. Customers' names, street addresses and other personal information are not being handed over as part of NSA's domestic program, the sources said. But the phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information.

Don Weber, a senior spokesman for the NSA, declined to discuss the agency's operations. "Given the nature of the work we do, it would be irresponsible to comment on actual or alleged operational issues; therefore, we have no information to provide," he said. "However, it is important to note that NSA takes its legal responsibilities seriously and operates within the law."

The White House would not discuss the domestic call-tracking program. "There is no domestic surveillance without court approval," said Dana Perino, deputy press secretary, referring to actual eavesdropping.

She added that all national intelligence activities undertaken by the federal government "are lawful, necessary and required for the pursuit of al-Qaeda and affiliated terrorists." All government-sponsored intelligence activities "are carefully reviewed and monitored," Perino said. She also noted that "all appropriate members of Congress have been briefed on the intelligence efforts of the United States."

The government is collecting "external" data on domestic phone calls but is not intercepting "internals," a term for the actual content of the communication, according to a U.S. intelligence official familiar with the program. This kind of data collection from phone companies is not uncommon; it's been done before, though never on this large a scale, the official said. The data are used for "social network analysis," the official said, meaning to study how terrorist networks contact each other and how they are tied together.

Carriers uniquely positioned

AT&T recently merged with SBC and kept the AT&T name. Verizon, BellSouth and AT&T are the nation's three biggest telecommunications companies; they provide local and wireless phone service to more than 200 million customers.

The three carriers control vast networks with the latest communications technologies. They provide an array of services: local and long-distance calling, wireless and high-speed broadband, including video. Their direct access to millions of homes and businesses has them uniquely positioned to help the government keep tabs on the calling habits of Americans.

Among the big telecommunications companies, only Qwest has refused to help the NSA, the sources said. According to multiple sources, Qwest declined to participate because it was uneasy about the legal implications of handing over customer information to the government without warrants.

Qwest's refusal to participate has left the NSA with a hole in its database. Based in Denver, Qwest provides local phone service to 14 million customers in 14 states in the West and Northwest. But AT&T and Verizon also provide some services — primarily long-distance and wireless — to people who live in Qwest's region. Therefore, they can provide the NSA with at least some access in that area.

Created by President Truman in 1952, during the Korean War, the NSA is charged with protecting the United States from foreign security threats. The agency was considered so secret that for years the government refused to even confirm its existence. Government insiders used to joke that NSA stood for "No Such Agency."

In 1975, a congressional investigation revealed that the NSA had been intercepting, without warrants, international

communications for more than 20 years at the behest of the CIA and other agencies. The spy campaign, code-named "Shamrock," led to the Foreign Intelligence Surveillance Act (FISA), which was designed to protect Americans from illegal eavesdropping.

Enacted in 1978, FISA lays out procedures that the U.S. government must follow to conduct electronic surveillance and physical searches of people believed to be engaged in espionage or international terrorism against the United States. A special court, which has 11 members, is responsible for adjudicating requests under FISA.

Over the years, NSA code-cracking techniques have continued to improve along with technology. The agency today is considered expert in the practice of "data mining" — sifting through reams of information in search of patterns. Data mining is just one of many tools NSA analysts and mathematicians use to crack codes and track international communications.

Paul Butler, a former U.S. prosecutor who specialized in terrorism crimes, said FISA approval generally isn't necessary for government data-mining operations. "FISA does not prohibit the government from doing data mining," said Butler, now a partner with the law firm Akin Gump Strauss Hauer & Feld in Washington, D.C.

The caveat, he said, is that "personal identifiers" — such as names, Social Security numbers and street addresses — can't be included as part of the search. "That requires an additional level of probable cause," he said.

The usefulness of the NSA's domestic phone-call database as a counterterrorism tool is unclear. Also unclear is whether the database has been used for other purposes.

The NSA's domestic program raises legal questions. Historically, AT&T and the regional phone companies have required law enforcement agencies to present a court order before they would even consider turning over a customer's calling data. Part of that owed to the personality of the old Bell Telephone System, out of which those companies grew.

Ma Bell's bedrock principle — protection of the customer — guided the company for decades, said Gene Kimmelman, senior public policy director of Consumers Union. "No court order, no customer information — period. That's how it was for decades," he said.

The concern for the customer was also based on law: Under Section 222 of the Communications Act, first passed in 1934, telephone companies are prohibited from giving out information regarding their customers' calling habits: whom a person calls, how often and what routes those calls take to reach their final destination. Inbound calls, as well as wireless calls, also are covered.

The financial penalties for violating Section 222, one of many privacy reinforcements that have been added to the law over the years, can be stiff. The Federal Communications Commission, the nation's top telecommunications regulatory agency, can levy fines of up to $130,000 per day per violation, with a cap of $1.325 million per violation. The FCC has no hard definition of "violation." In practice, that means a single "violation" could cover one customer or 1 million.

In the case of the NSA's international call-tracking program, Bush signed an executive order allowing the NSA to engage in eavesdropping without a warrant. The president and his representatives have since argued that an executive order was sufficient for the agency to proceed. Some civil liberties groups, including the American Civil Liberties Union, disagree.

Companies approached

The NSA's domestic program began soon after the Sept. 11 attacks, according to the sources. Right around that time, they said, NSA representatives approached the nation's biggest telecommunications companies. The agency made an urgent pitch: National security is at risk, and we need your help to protect the country from attacks.

The agency told the companies that it wanted them to turn over their "call-detail records," a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation's calling habits.

The sources said the NSA made clear that it was willing to pay for the cooperation. AT&T, which at the time was headed by C. Michael Armstrong, agreed to help the NSA. So did BellSouth, headed by F. Duane Ackerman; SBC, headed by Ed Whitacre; and Verizon, headed by Ivan Seidenberg.

With that, the NSA's domestic program began in earnest.

AT&T, when asked about the program, replied with a comment prepared for USA TODAY: "We do not comment on matters of national security, except to say that we only assist law enforcement and government agencies charged with protecting national security in strict accordance with the law."

In another prepared comment, BellSouth said: "BellSouth does not provide any confidential customer information to the NSA or any governmental agency without proper legal authority."

Verizon, the USA's No. 2 telecommunications company behind AT&T, gave this statement: "We do not comment on national security matters, we act in full compliance with the law and we are committed to safeguarding our customers' privacy."

Qwest spokesman Robert Charlton said: "We can't talk about this. It's a classified situation."

In December, *The New York Times* revealed that Bush had authorized the NSA to wiretap, without warrants, international phone calls and e-mails that travel to or from the USA. The following month, the Electronic Frontier Foundation, a civil liberties group, filed a class-action lawsuit against AT&T. The lawsuit accuses the company of helping the NSA spy on U.S. phone customers.

Last month, U.S. Attorney General Alberto Gonzales alluded to that possibility. Appearing at a House Judiciary Committee hearing, Gonzales was asked whether he thought the White House has the legal authority to monitor domestic traffic without a warrant. Gonzales' reply: "I wouldn't rule it out." His comment marked the first time a Bush appointee publicly asserted that the White House might have that authority.

Similarities in programs

The domestic and international call-tracking programs have things in common, according to the sources. Both are being conducted without warrants and without the approval of the FISA court. The Bush administration has argued that FISA's procedures are too slow in some cases. Officials, including Gonzales, also make the case that the USA Patriot Act gives them broad authority to protect the safety of the nation's citizens.

The chairman of the Senate Intelligence Committee, Sen. Pat Roberts, R-Kan., would not confirm the existence of the program. In a statement, he said, "I can say generally, however, that our subcommittee has been fully briefed on all aspects of the Terrorist Surveillance Program. ... I remain convinced that the program authorized by the president is lawful and absolutely necessary to protect this nation from future attacks."

The chairman of the House Intelligence Committee, Rep. Pete Hoekstra, R-Mich., declined to comment.

One company differs

One major telecommunications company declined to participate in the program: Qwest.

According to sources familiar with the events, Qwest's CEO at the time, Joe Nacchio, was deeply troubled by the NSA's assertion that Qwest didn't need a court order — or approval under FISA — to proceed. Adding to the tension, Qwest was unclear about who, exactly, would have access to its customers' information and how that information might be used.

Financial implications were also a concern, the sources said. Carriers that illegally divulge calling information can be subjected to heavy fines. The NSA was asking Qwest to turn over millions of records. The fines, in the aggregate, could have been substantial.

The NSA told Qwest that other government agencies, including the FBI, CIA and DEA, also might have access to the database, the sources said. As a matter of practice, the NSA regularly shares its information — known as "product" in intelligence circles — with other intelligence groups. Even so, Qwest's lawyers were troubled by the expansiveness of the NSA request, the sources said.

The NSA, which needed Qwest's participation to completely cover the country, pushed back hard.

Trying to put pressure on Qwest, NSA representatives pointedly told Qwest that it was the lone holdout among the big telecommunications companies. It also tried appealing to Qwest's patriotic side: In one meeting, an NSA representative suggested that Qwest's refusal to contribute to the database could compromise national security, one person recalled.

In addition, the agency suggested that Qwest's foot-dragging might affect its ability to get future classified work with the government. Like other big telecommunications companies, Qwest already had classified contracts and hoped to get more.

Unable to get comfortable with what NSA was proposing, Qwest's lawyers asked NSA to take its proposal to the FISA court. According to the sources, the agency refused.

The NSA's explanation did little to satisfy Qwest's lawyers. "They told (Qwest) they didn't want to do that because FISA might not agree with them," one person recalled. For similar reasons, this person said, NSA rejected Qwest's suggestion of getting a letter of authorization from the U.S. attorney general's office. A second person confirmed this version of events.

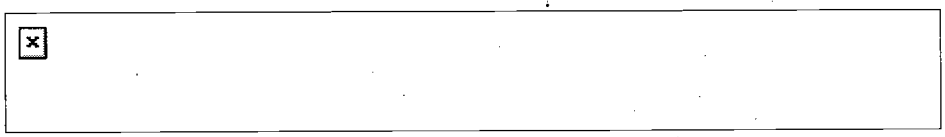
In June 2002, Nacchio resigned amid allegations that he had misled investors about Qwest's financial health. But Qwest's legal questions about the NSA request remained.

Unable to reach agreement, Nacchio's successor, Richard Notebaert, finally pulled the plug on the NSA talks in late 2004, the sources said.

Contributing: John Diamond

Find this article at:
http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

☐ Check the box to include the list of links referenced in the article.



The New York Times
nytimes.com

May 12, 2006

Qwest's Refusal of N.S.A. Query Is Explained

By JOHN O'NEIL and ERIC LICHTBLAU

WASHINGTON, May 12 — The telecommunications company Qwest turned down requests by the National Security Agency for private telephone records because it concluded that doing so would violate federal privacy laws, a lawyer for the telephone company's former chief executive said today.

In a statement released this morning, the lawyer said that the former chief executive, Joseph N. Nacchio, made the decision after asking whether "a warrant or other legal process had been secured in support of that request."

Mr. Nacchio learned that no warrant had been granted and that there was a "disinclination on the part of the authorities to use any legal process," said the lawyer, Herbert J. Stern. As a result, the statement said, Mr. Nacchio concluded that "the requests violated the privacy requirements of the Telecommunications Act."

A Qwest spokesman, Robert Toevs, declined to discuss anything to do with security issues or the statement by Mr. Nacchio's lawyer.

Qwest was the only phone company to turn down requests from the security agency for phone records as part of a program to compile a vast database of numbers and other information on virtually all domestic calls. The program's scope was first described in an article published on Thursday by USA Today that led to an outpouring of demands for information from Congressional Republicans and Democrats. The article said that AT&T, BellSouth and Verizon had agreed to provide the information to the security agency.

On Thursday, those companies said they were following the law in protecting customers' privacy but would not discuss details of the report. Separately today Verizon issued a statement saying that it provided customer information to a government agency "only where authorized by law for appropriately-defined and focused purposes."_ The company cited unspecified "factual errors in press coverage,"_ about the way it the company handles customer information in general.

The statements came as Gen. Michael V. Hayden, who was the head of the National Security Agency at the time the program began, continued to seek support today for his nomination as C.I.A. director in meetings with senators on Capitol Hill.

Speaking to reporters with Senator Chuck Hagel, Republican of Nebraska, General Hayden declined to comment

on the article about the National Security Agency program.

"Everything that the agency has done has been lawful," he said. "It's been briefed to the appropriate members of Congress."

Mr. Hagel, a member of the Intelligence Committee, which will conduct General Hayden's confirmation hearings, said that General Hayden was "the right choice" for the C.I.A.'s top post.

But he also said he supported plans announced Thursday by Senator Arlen Specter, the Republican chairman of the Senate Judiciary Committee, to hold separate hearings into the collection of phone records.

Mr. Hagel called that "appropriate."

"I think this issue needs to be clearly aired," he said. "I think people need to have confidence in their government."

Mr. Hagel said the confirmation hearings would certainly involve "tough questions" for General Hayden. Members of Congress have said they want information both about the collection of phone records and about a program of warrantless wiretaps on calls between people in the United States and people overseas suspected of having ties to terrorism.

The White House continued to express its support of General Hayden today and to sidestep questions about the program to collect telephone records.

Tony Snow, the White House press secretary, told reporters that "we're 100 percent behind Michael Hayden."

Mr. Snow also said that the White House was "confident that he is going to comport himself well and answer all the questions and concerns that members of the United States Senate may have in the process of confirmation."

On Tuesday, President Bush responded to an outcry over the article by assuring the country that "we're not mining or trolling through the personal lives of millions of innocent Americans."

One senior government official, who was granted anonymity to speak publicly about the classified program, confirmed that the N.S.A. had access to records of most telephone calls in the United States. But the official said the call records were used for the limited purpose of tracing regular contacts of "known bad guys."

"To perform such traces," the official said, "you'd have to have all the calls or most of them. But you wouldn't be interested in the vast majority of them."

The New York Times first reported in December that the president had authorized the N.S.A. to conduct eavesdropping without warrants.

The Times also reported in December that the agency had gained the cooperation of American telecommunications companies to get access to records of vast amounts of domestic and international phone calls and e-mail messages.

The agency analyzes communications patterns, the report said, and looks for evidence of terrorist activity at home and abroad.

The USA Today article on Thursday went further, saying that the N.S.A. had created an enormous database of all calls made by customers of the three phone companies in an effort to compile a log of "every call ever made" within this country.

Mr. Nacchio's statement today made a point of saying that the N.S.A. requests occurred "at a time when there was no investigation of Qwest or Mr. Nacchio." Mr. Nacchio, who left Qwest in 2002 amid allegations of fraud at the company, was indicted in December on 42 charges of insider selling.

Prosecutors say Mr. Nacchio did not make investors aware of warnings from his managers that the company's revenue and profit forecasts were too optimistic. They say Mr. Nacchio kept this information to himself yet also sold 2.5 million shares of Qwest stock over five months in 2001 that netted $100 million. The case could go to trial later this year.On Thursday, some Republicans, including Representative Peter Hoekstra of Michigan, chairman of the House Intelligence Committee, defended the N.S.A.'s activities and denounced the disclosure. Mr. Hoekstra said the report "threatens to undermine our nation's safety."

"Rather than allow our intelligence professionals to maintain a laser focus on the terrorists, we are once again mired in a debate about what our intelligence community may or may not be doing," he said.

But many Democrats and civil liberties advocates said they were disturbed by the report, invoking images of Big Brother and announcing legislation aimed at reining in the N.S.A.'s domestic operations. Fifty-two members of Congress asked the president to name a special counsel to investigate the N.S.A.'s domestic surveillance programs.

Senator Arlen Specter, the Pennsylvania Republican who heads the Judiciary Committee, said the reported data-mining activities raised serious constitutional questions. He said he planned to seek the testimony of telephone company executives.

The House majority leader, John A. Boehner of Ohio, said he wanted more information on the program because "I am not sure why it would be necessary to keep and have that kind of information."

Mr. Bush did not directly confirm or deny the existence of the N.S.A. operation but said that "as a general matter, every time sensitive intelligence is leaked it hurts our ability to defeat this enemy."

Seeking to distinguish call-tracing operations from eavesdropping, the president said that "the government does

not listen to domestic phone calls without court approval."

The phone records include numbers called; time, date and direction of calls; and other details, but not the words spoken, telecommunications experts said. Customers' names and addresses are not included in the companies' call records, though they could be cross-referenced to obtain personal data.

The law on data-mining activities is murky, and legal analysts were divided Thursday on the question of whether the N.S.A.'s tracing and analysis of huge streams of American communications data would require the agency to use subpoenas or court warrants.

Kate Martin, director of the Center for National Security Studies, said, "If they don't get a court order, it's a crime." Ms. Martin said that while the F.B.I. might be able to get access to phone collection databases by using an administrative subpoena, her reading of federal law was that the N.S.A. would be banned from doing so without court approval.

But another expert on the law of electronic surveillance, Kenneth C. Bass III, said that if access to the call database was granted in response to a national security letter issued by the government, "it would probably not be illegal, but it would be very troubling."

"The concept of the N.S.A. having near-real-time access to information about every call made in the country is chilling," said Mr. Bass, former counsel for intelligence policy at the Justice Department. He said the phone records program resembled Total Information Awareness, a Pentagon data-mining program shut down by Congress in 2003 after a public outcry.

The N.S.A. refused to discuss the report, but said in a statement that it "takes its legal responsibilities seriously and operates within the law."

AT&T, Verizon and BellSouth all issued statements saying they had followed the law in protecting customers' privacy but would not discuss details of the report.

"AT&T has a long history of vigorously protecting customer privacy," said Selim Bingol, a company spokesman. "We also have an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare."

Mr. Specter said in an interview that he would press for information on the operations of the N.S.A. program to determine its legality.

"I don't think we can really make a judgment on whether warrants would be necessary until we know a lot more about the program," he said.

One central question is whether the N.S.A. uses its analysis of phone call patterns to select people in the United States whose phone calls and e-mail messages are monitored without warrants. The Times has reported that the agency is believed to have eavesdropped on the international communications of about 400 to 500 people at a time within the United States and of thousands of people since the Sept. 11 attacks.

Democrats said they would use the new disclosures to push for more answers from General Hayden at his confirmation hearing, set for May 18.

Senator Dianne Feinstein, Democrat of California, predicted "a major Constitutional confrontation on Fourth Amendment guarantees of unreasonable search and seizure" and said the new disclosures presented "a growing impediment to the confirmation of General Hayden."

Scott Shane contributed reporting from Washington for this article.

Lawmakers: NSA database incomplete

Updated 6/30/2006 8:51 AM ET

A NOTE TO OUR READERS

On May 11, USA TODAY reported that the National Security Agency, with the cooperation of several of America's leading telecommunications companies, had compiled a database of domestic phone call records in an effort to monitor terrorist activity.

Several days later, BellSouth and Verizon specifically denied that they were among the companies that had contracted with the NSA to provide bulk calling records.

The denial was unexpected. USA TODAY had spoken with BellSouth and Verizon for several weeks about the substance of the report. The day before the article was published, the reporter read the sections of the article concerning BellSouth and Verizon to representatives of the companies and asked for a denial before publication.

At the time, BellSouth did not deny participation in the program, but it issued a statement saying the company "does not provide any confidential customer information to the NSA or any government agency without proper legal authority." Verizon said that it would not comment on national security matters and that it acts "in full compliance with the law" and with respect for customers' privacy.

On May 15, BellSouth said it could not categorically deny participation in the program until it had conducted a detailed investigation. BellSouth said that internal review concluded that the company did not contract with the NSA or turn over calling records.

USA TODAY continued to pursue details of the database, speaking with dozens of sources in the telecommunications, intelligence and legislative communities, including interviews with members of Congress who have been

WASHINGTON — Members of the House and Senate intelligence committees confirm that the National Security Agency has compiled a massive database of domestic phone call records. But some lawmakers also say that cooperation by the nation's telecommunication companies was not as extensive as first reported by USA TODAY on May 11.

Several lawmakers, briefed in secret by intelligence officials about the program after the story was published, described a call records database that is enormous but incomplete. Most asked that they not be identified by name, and many offered only limited responses to questions, citing national security concerns.

In the May 11 article that revealed the database, USA TODAY reported that its sources said AT&T, BellSouth and Verizon had agreed to provide the NSA with call records.

AT&T, which is the nation's largest telecommunications company, providing service to tens of millions of Americans, hasn't confirmed or denied its participation with the database. BellSouth and Verizon have denied that they contracted with the NSA to turn over phone records. On May 12, an attorney for former Qwest CEO Joseph Nacchio confirmed the USA TODAY report that Qwest had declined to participate in the NSA program.

Most members of the intelligence committees wouldn't discuss which companies cooperated with the NSA. However, several did offer more information about the program's breadth and scope, confirming some elements of USA TODAY's report and contradicting others:

• Nineteen lawmakers who had been briefed on the program verified that the NSA has built a database that includes records of Americans' domestic phone calls. The program collected records of the numbers dialed and the length of calls, sources have said, but did not involve listening to the calls or recording

briefed by senior intelligence officials on the domestic calls program.

In the adjoining article, USA TODAY reports that five members of the congressional intelligence committees said they had been told in secret briefings that BellSouth did not turn over call records to the NSA, three lawmakers said they had been told that Verizon had not participated in the NSA database, and four said that Verizon's subsidiary MCI did turn over records to the NSA.

USA TODAY also spoke again with the sources who had originally provided information about the scope and contents of the domestic calls database. All said the published report accurately reflected their knowledge and understanding of the NSA program, but none could document a contractual relationship between BellSouth or Verizon and the NSA, or that the companies turned over bulk calling records to the NSA.

Based on its reporting after the May 11 article, USA TODAY has now concluded that while the NSA has built a massive domestic calls record database involving the domestic call records of telecommunications companies, the newspaper cannot confirm that BellSouth or Verizon contracted with the NSA to provide bulk calling records to that database.

USA TODAY will continue to report on the contents and scope of the database as part of its ongoing coverage of national security and domestic surveillance.

HOW PHONE COMPANIES MOVE CALLS AROUND THE COUNTRY

their content.

• Five members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program.

AT&T, asked to comment, issued a written statement Thursday. "The U.S. Department of Justice has stated that AT&T may neither confirm nor deny AT&T's participation in the alleged NSA program because doing so would cause 'exceptionally grave harm to national security' and would violate both civil and criminal statutes," it said. "Under these circumstances, AT&T is not able to respond to such allegations."

• Five members of the intelligence committees said they were told that BellSouth did not turn over domestic call records to the NSA.

Asked about BellSouth's denial, Sen. Saxby Chambliss, R-Ga., a member of the Senate Intelligence Committee, said, "What they said appears to be accurate."

Still, BellSouth customers' call records could end up in the NSA database, he said. "Obviously, a BellSouth customer can contract with AT&T (for long-distance phone service). There is a possibility that numbers are available from other phone companies."

• Three lawmakers said that they had been told that Verizon did not turn over call records to the NSA. However, those three and another lawmaker said MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government.

While Verizon has denied providing call records to the NSA, it has declined to comment on whether MCI participated in the calls database program.

"The President has referred to an NSA program, which he authorized, directed against al-Qaeda," Verizon said in a written statement May 12. "Because that program is highly classified, Verizon cannot comment on that program, nor can we confirm or deny whether we have had any relationship to it." The statement also said the company was now "ensuring that Verizon's policies are implemented at that entity (MCI) and that all its activities fully comply with law."

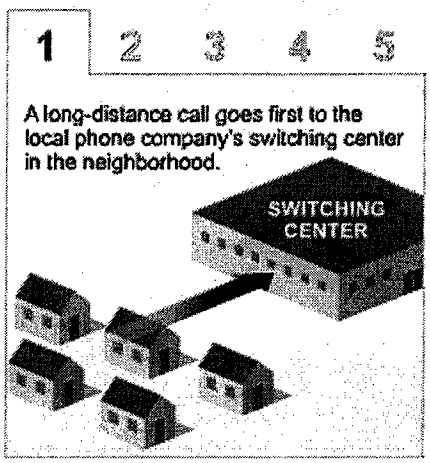
In the weeks since the database was revealed, congressional and intelligence sources have offered other new details about its scope and effectiveness.

"It was not cross-city calls. It was not mom-and-pop calls," said Sen. Ted Stevens, R-Alaska, who receives briefings as chairman of the Senate Appropriations Defense subcommittee. "It was long-distance. It was targeted on (geographic) areas of interest, places to which calls were believed to have come from al-Qaeda affiliates and from which calls were made to al-Qaeda

Phone companies handle billions of calls a day, routing them to and from local and long-distance networks.

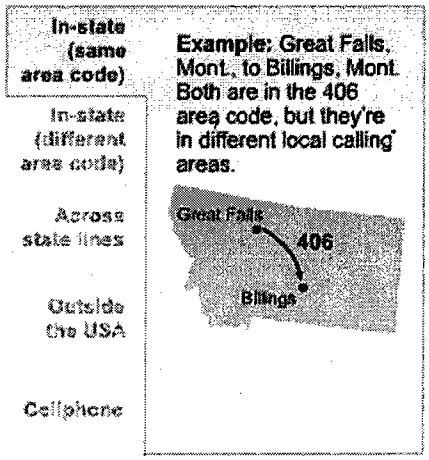
What local and long-distance companies do

- **LOCAL**
  A local call is relayed to the local phone company's switching center and then sent to the person being called in the local area.
- **LONG-DISTANCE**



What is a long-distance call?

Long-distance carriers handle calls that cross two or more local calling areas, sometimes even when the calling areas fall within the same local phone company's service territory. Types of calls phone customers might make that would be handled by their long-distance carrier:



Sources: Yankee Group, Telegeography, Bell Labs

By Ron Coddington, Marcy E. Mullins and Julie Snider, USA TODAY

affiliates."

Other lawmakers who were briefed about the program expressed concerns that gaps in the database could undercut its usefulness in identifying terrorist cells.

"It's difficult to say you're covering all terrorist activity in the United States if you don't have all the (phone) numbers," Chambliss said. "It probably would be better to have records of every telephone company."

"The database is not complete," said another lawmaker who was briefed on the program, speaking on condition of anonymity because the information is classified. "We don't know if this works yet."

Other publications have characterized the breadth of the database and how it is used.

The New York Times reported on May 12, for instance, that a senior government official had confirmed that the NSA had access to records of most telephone calls in the USA but said the records are used in a limited way to track "known bad guys."

The Washington Post reported on May 12 that "sources with knowledge of the program" said that the Bush administration had been collecting the domestic telephone records in "gargantuan databases" and that the "companies cooperating with the NSA dominate the U.S. telecommunications market and connect hundreds of billions of telephone calls each year."

President Bush and his top aides have defended the legality of the program, although they haven't directly confirmed its existence.

Three days after the USA TODAY story was published, national security adviser Stephen Hadley said on CBS' *Face the Nation* that he couldn't "confirm or deny the claims that are in the USA TODAY story."

He went on: "But it's very interesting what that story does not claim. It does not claim that the government was listening on domestic phone calls. It does not claim that names were passed, that addresses were passed, that content was passed. It's really about calling records, if you read the story. ... There are a variety of ways in which those records lawfully can be provided to the government."

At a news conference two weeks later, Attorney General Alberto Gonzales made a similar point. "There has been no confirmation about any details relating to the USA TODAY story," he said. "I will say that what was in the USA TODAY story did relate to business records." Citing a 1979 Supreme Court decision, he said, "There is no reasonable expectation of privacy in those kinds of records."

Lawmakers who were briefed about the program disagree about whether it's legal.

"It was within the president's inherent powers," said Sen. Orrin Hatch, R-Utah, a member of the Senate Intelligence Committee.

Rep. Anna Eshoo, D-Calif., a member of the House Intelligence Committee, said there was a "schizophrenia in the presentation" by the administration. Officials say, " 'It's legal,' " she said. "But in the same breath they say, 'Perhaps we should take another look at FISA.' " FISA refers to the 1978 Foreign Intelligence Surveillance Act, which established a secret court that can grant warrants for eavesdropping.

Rep. Rush Holt, D-N.J., another member of the House Intelligence Committee, said, "I find it interesting that it seems the government is asking telephone companies to do things that their customers and shareholders would find totally unpalatable."

Debate over the database continues in several areas:

• In federal courts, at least 20 class-action lawsuits have been filed alleging that the government and phone companies have violated the rights of people whose calls have been reviewed by the NSA. The Justice Department signaled its intention in a court filing in Chicago this month to assert the "military and state secrets privilege" in all of them. That privilege allows the government to seek the dismissal of lawsuits if pursuing them would imperil national security.

• In New Jersey, the state attorney general is investigating whether telephone companies released confidential information without the consent of their customers. The federal government asked a court this month to quash subpoenas the state had issued to phone companies seeking information.

• At the Federal Communications Commission, the American Civil Liberties Union requested this month that approval of AT&T's acquisition of BellSouth be withheld until the commission reviews the companies' dealings with the NSA. However, FCC Chairman Kevin Martin said last month that the commission couldn't investigate complaints about the phone companies and the NSA because the reported activities were classified.

• On Capitol Hill, Vice President Cheney held private talks this month with Republicans on the Senate Judiciary Committee. Cheney discouraged them from supporting Judiciary Chairman Arlen Specter's vow to call telecommunications executives before the panel to answer questions about the database. Specter, R-Pa., protested to Cheney in an angry public letter.

The White House then agreed to talks with Specter on legislation he has drafted that would give the administration the option of putting the NSA's warrantless-surveillance program — which includes domestic wiretapping without a court warrant when one participant in a conversation is overseas — under the scrutiny of the FISA court.

"I'm prepared to defer, on a temporary basis, calling in the telephone companies," Specter said. If the discussions on his legislation fall through, however, he said, he will move again to demand testimony from the telephone executives about the database.

This story was reported by Leslie Cauley, John Diamond, Jim Drinkard, Peter Eisler, Thomas Frank, Kevin Johnson and Susan Page. It was written by Page.

Posted 6/30/2006 5:03 AM ET

Updated 6/30/2006 8:51 AM ET

The NY Times: Questions Raised for Phone Giants in Spy Data Furor

JOHN MARKOFF
The New York Times
May 13, 2006

The former chief executive of Qwest, the nation's fourth-largest phone company, rebuffed government requests for the company's calling records after 9/11 because of "a disinclination on the part of the authorities to use any legal process," his lawyer said yesterday.

The statement on behalf of the former Qwest executive, Joseph P. Nacchio, followed a report that the other big phone companies — AT&T, BellSouth and Verizon — had complied with an effort by the National Security Agency to build a vast database of calling records, without warrants, to increase its surveillance capabilities after the Sept. 11 attacks.

Those companies insisted yesterday that they were vigilant about their customers' privacy, but did not directly address their cooperation with the government effort, which was reported on Thursday by USA Today. Verizon said that it provided customer information to a government agency "only where authorized by law for appropriately defined and focused purposes," but that it could not comment on any relationship with a national security program that was "highly classified."

Legal experts said the companies faced the prospect of lawsuits seeking billions of dollars in damages over cooperation in the program, citing communications privacy legislation stretching back to the 1930's. A federal lawsuit was filed in Manhattan yesterday seeking as much as $50 billion in civil damages against Verizon on behalf of its subscribers.

For a second day, there was political fallout on Capitol Hill, where Senate Democrats intend to use next week's confirmation hearings for a new C.I.A. director to press the Bush administration on its broad surveillance programs.

As senior lawmakers in Washington vowed to examine the phone database operation and possibly issue subpoenas to the telephone companies, executives at some of the companies said they would comply with requests to appear on Capitol Hill but stopped short of describing how much would be disclosed, at least in public sessions.

"If Congress asks us to appear, we will appear," said Selim Bingol, a spokesman at AT&T. "We will act within the laws and rules that apply."

Qwest was apparently alone among the four major telephone companies to have resisted the requests to cooperate with the government effort. A statement issued on behalf of Mr. Nacchio yesterday by his lawyer, Herbert J. Stern, said that after the government's first approach in the fall of 2001, "Mr. Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request."

"When he learned that no such authority had been granted, and that there was a disinclination on the part of the authorities to use any legal process," Mr. Nacchio concluded that the requests violated federal privacy requirements "and issued instructions to refuse to comply."

The statement said the requests continued until Mr. Nacchio left in June 2002. His departure came amid accusations of fraud at the company, and he now faces federal charges of insider trading.

The database reportedly assembled by the security agency from calling records has dozens of fields of information, including called and calling numbers and the duration of calls, but nothing related to the substance of the calls. But it could permit what intelligence analysts and commercial data miners refer to as "link analysis," a statistical technique for investigators to identify calling patterns in a seemingly impenetrable mountain of digital data.

The law governing the release of phone company data has been modified repeatedly to grapple with changing computer and communications technologies that have increasingly bedeviled law enforcement agencies. The laws include the Communications Act, first passed in 1934, and a variety of provisions of the Electronic Communications and Privacy Act, including the Stored Communications Act, passed in 1986.

Wiretapping — actually listening to phone calls — has been tightly regulated by these laws. But in general, the laws have set a lower legal standard required by the government to obtain what has traditionally been called pen register or trap-

and-trace information — calling records obtained when intelligence and police agencies attached a specialized device to subscribers' telephone lines.

Those restrictions still hold, said a range of legal scholars, in the face of new computer databases with decades' worth of calling records. AT&T created such technology during the 1990's for use in fraud detection and has previously made such information available to law enforcement with proper warrants.

Orin Kerr, a former federal prosecutor and assistant professor at George Washington University, said his reading of the relevant statutes put the phone companies at risk for at least $1,000 per person whose records they disclosed without a court order. "This is not a happy day for the general counsels" of the phone companies, he said. "If you have a class action involving 10 million Americans, that's 10 million times $1,000 — that's 10 billion."

The New Jersey lawyers who filed the federal suit against Verizon in Manhattan yesterday, Bruce Afran and Carl Mayer, said they would consider filing suits against BellSouth and AT&T in other jurisdictions.

"This is almost certainly the largest single intrusion into American civil liberties ever committed by any U.S. administration," Mr. Afran said. "Americans expect their phone records to be private. That's our bedrock governing principle of our phone system." In addition to damages, the suit seeks an injunction against the security agency to stop the collection of phone numbers.

Several legal experts cited ambiguities in the laws that may be used by the government and the phone companies to defend the National Security Agency program.

"There's a loophole," said Mark Rasch, the former head of computer-crime investigations for the Justice Department and now the senior vice president of Solutionary, a computer security company. "Records of phones that have called each other without identifying information are not covered by any of these laws."

Civil liberties lawyers were quick to dispute that claim.

"This is an incredible red herring," said Kevin Bankston, a lawyer for the Electronic Frontier Foundation, a privacy rights group that has sued AT&T over its cooperation with the government, including access to calling records. "There is no legal process that contemplates getting entire databases of data."

The group sued AT&T in late January, contending that the company was violating the law by giving the government access to its customer call record data and permitting the agency to tap its Internet network. The suit followed reports in The New York Times in December that telecommunications companies had cooperated with such government requests without warrants.

A number of industry executives pointed to the national climate in the wake of the Sept. 11 attacks to explain why phone companies might have risked legal entanglement in cooperating with the requests for data without warrants.

An AT&T spokesman said yesterday that the company had gotten some calls and e-mail messages about the news reports, but characterized the volume as "not heavy" and said there were responses on both sides of the issue.

Reaction around the country also appeared to be divided.

Cathy Reed, 45, a wealth manager from Austin, Tex., who was visiting Boston, said she did not see a problem with the government's reviewing call logs. "I really don't think it matters," she said. "I bet every credit card company already has them."

Others responded critically. Pat Randall, 63, a receptionist at an Atlanta high-rise, said, "Our phone conversations are just personal, and to me, the phone companies that cooperated, I think we should move our phone services to the company that did not cooperate."

While the telephone companies have both business contracts and regulatory issues before the federal government, executives in the industry yesterday dismissed the notion that they felt pressure to take part in any surveillance programs. The small group of executives with the security clearance necessary to deal with the government on such matters, they said, are separate from the regulatory and government contracting divisions of the companies.

Reporting for this article was contributed by Ken Belson, Brenda Goodman, Stephen Labaton, Matt Richtel and Katie

This article can be found at http://www.refuseandresist.org/police_state/art.php?aid=2367.

Privacy and Customer Security Policies

Telephone Company Customer Privacy

This tells you about our privacy policy for our telephone company customers. Please use the following links for additional information:

- Internet Privacy Policy
- General Privacy Principles.

For more than a century, customers have counted on Verizon's telephone companies to respect and protect the privacy of information we obtain in the normal course of providing service. While we are working hard to serve you in new and exciting ways, our commitment to protecting your privacy remains as strong as ever.

Your Privacy is Our Priority

Verizon has strict policies governing employee access to customer records. We access customer accounts, records or reports for authorized business purposes only. We educate our employees about their obligation to safeguard customer information and telephone calls, and we hold them accountable for their actions.

Privacy is a priority for Verizon when we develop new products and services. Verizon conducts a privacy review, which includes consumer input, as part of its product development process. We inform customers about any privacy implications of new products and services we introduce.

Back to Top

The Information We Obtain, and How We Use It

Verizon obtains information about customers that helps us to provide service, and we use that information for business purposes only.

For example: We need to know your name, address and the services you buy from us. When you call us, a service representative refers to your customer record to serve you better. It also may be useful for us to know about your telephone bill, your calling patterns, and whether you have special needs. We may use that kind of information to offer you the most effective services for your particular needs.

If Verizon enters into a merger, acquisition, or sale of all or a portion of its assets, a customer's personally identifiable information will, in most instances, be transferred as a part of the transaction.

Or we may use information in our records to protect customers, employees or property, for instance, to investigate fraud or harassment.

We want to make sure the information we obtain and use is accurate. Much of this information is reflected in your monthly telephone bill. If you see an inaccuracy on your Verizon bill, and you let us know, then we can correct it.

Other Privacy & Policy Links

- Internet Privacy Policy
- Letter from the CEO
- General Privacy Principles
- Telephone Company Customer Privacy
- FiOS TV Subscriber Privacy Notice
- Do Not Call Policy
- Browser Policy Statement
- Linking Policy Statement
- Terms and Conditions
- Changes to Privacy Policy
- Your California Privacy Rights

Verizon regularly provides useful information about new products and services to our residential customers, including our customers with non-published telephone numbers. However, consumers who do not wish to receive such information can "opt out" or have their names removed from direct mail and telemarketing lists that we use internally. For example, if you receive an unwanted telemarketing call from us, simply tell a Verizon representative that you do not wish to receive future calls and ask to be placed on our "Do Not Call" list. Please understand that making this type of request may mean that you will be unaware of services or discounts that you might find useful.

You should know that when you speak with us at Verizon, a supervisor might listen in on that call. Supervisors listen in only to help train employees and ensure that we provide you with accurate information and high-quality customer service.

Back to Top

Disclosure of Information Outside Verizon

As a rule, Verizon will notify you and give you the opportunity to "opt out" when we disclose telephone customer information outside of Verizon. In fact, we generally keep our records of the services you buy and the calls you make private, and will not ordinarily disclose this information to outside parties without your permission. However, we do release customer information without involving you if disclosure is required by law or to protect the safety of customers, employees or property. This is further explained below.

Examples of your control over the disclosure of information:

- You tell us the telephone listings you want to include in our directories and in directory assistance.
You also may choose to have a non-published number, or a non-listed number, or to exclude your address from your listing.
- We may compile lists of names, addresses, and telephone numbers from our published White Pages directories and provide the lists to qualified companies that are conducting product promotions. Non-published and non-listed numbers will not be included in these lists, and we will remove other customers from these lists by request.
- All customers in areas where Caller ID services are available have the ability to block the display of
their phone numbers and names. (Note that Caller ID blocking does not prevent the transmission of your phone number when you dial certain business numbers, including 911, or 800, 888, 877, and 900 numbers.)

Examples where disclosure is required by law or to protect the safety of customers, employees or property:

- When you dial 911, information about your location may be transmitted automatically to a public safety agency. Certain information about your long distance calls is transmitted to your long distance
company for billing purposes. Verizon also is required by law to give competitive local exchange carriers access to its customer databases for purposes of serving their customers, to exchange credit information with other carriers, and to provide listings (other than certain non-published and non-listed information) to directory publishers.
- Verizon must disclose information, as necessary, to comply with court orders or subpoenas. Verizon
also will share information to protect its rights or property and to protect users of its services and other carriers from fraudulent, abusive or unlawful use of services.
- We may, where permitted by law, provide information to credit bureaus, or provide information and/or
sell receivables to collection agencies, to obtain payment for Verizon-billed products and services.
- Verizon also occasionally uses contractors to do work for the company. These contractors have

the
same obligations as our regular employees concerning customer information.

Back to Top

Your Telephone Account Information Rights
The FCC refers to your telephone account information as Customer Proprietary Network Information or CPNI. Under Federal Law, you have the right to, and we have the duty to protect, the confidentiality of your telecommunications service information. This information includes the type, technical arrangement, quantity, destination, and amount of use of telecommunications services and related billing for these services.

We may use this information, without further authorization by you, to offer you: (i) services of the type you already purchase from us, and (ii) the full range of products and services available from Verizon and other Verizon companies that may be different from the type of services you currently buy from us. In addition to local telephone services, Verizon and other Verizon company services include long distance (where authorized), wireless, and Internet services. A more complete description of our companies and service offerings is available on this Web site. Use of your information will permit us to offer you a package of services tailored to your specific needs. Without further authorization by you, we may also share your information with other Verizon companies with whom you already have an existing service relationship.

No action by you is necessary to permit us to use your information to offer you services that may be different from the type of services you currently buy from us. However, prior to using your information for the first time, we will notify you by mail or through your account executive, and you will have 30 days to tell us, using the toll free number mentioned in our notice, if you do not want us to use your information to offer services different from the type of services you currently buy from us. After the 30 days has expired, Verizon may begin using your information to offer services different from those you currently purchase from us unless you have notified us that we may not use it for this purpose. At any time after the 30 days, however, you can change your decision by using the toll free number. Your decision will remain effective until you change it.

If you have any questions regarding the notice or would like to know how to restrict the use of your information, please call the Verizon Customer Sales & Solutions Center telephone number located on your telephone bill or visit the Customer Sales & Solutions Center to locate the telephone number for your area.

Back to Top

Providing Services to Enhance Your Privacy
Verizon considers privacy implications as new services are planned and introduced and informs customers of the privacy implications of these services.

Non-published numbers, Caller ID and Caller ID blocking services, and Anonymous Call Rejection are among the privacy-management services Verizon offers our telephone customers. We also work to develop other services that help customers to control access to information about them. We seek customer input in developing new products and conduct comprehensive customer outreach and education efforts before and after introducing privacy-sensitive products.

Back to Top

Protecting your Privacy in Cyberspace and in Other Areas of Our Business
At Verizon, we are committed to expanding the world of communications and multimedia for customers, a world of wireline and wireless solutions: voice, video, and data services, as well as information and entertainment. We will investigate the privacy implications these new services may have and build safeguards into services before they are introduced. We will inform and educate you

about the effect on customer privacy any new services may have.

For example, Verizon's commitment to maintaining high standards for the protection of customer privacy extends beyond telephone service to include our Web sites. Recognizing concern over privacy on the Internet, Verizon has developed an on-line privacy policy that clearly defines the corporation's data collection processes and the use of that data at all times. Visitors to Verizon's Web sites -- for example, www.verizon.com, www.SuperPages.com, www.verizon.net -- are apprised of the types of information obtained, how it is obtained, how it is used, and how they can restrict the use or disclosure of that data.

Verizon is committed to maintaining high standards for the protection of customer privacy. At Verizon, your privacy is our priority. For more information on how Verizon strives to protect your privacy, customers can access our World Wide Web site at www.verizon.com.

Back to Top

Updated November 2005

Customer Privacy Policy

REVISED October 10, 2001

Like you, we at Qwest are concerned about customer privacy. We have a long history of maintaining the privacy of information we obtain in the normal course of providing our services. We work hard to serve you through new and exciting products and services. In the process, we remain sensitive to privacy issues.

The Information We Obtain and How We Use It

The information we obtain from you is generally necessary for us to provide your services and design new services for your future use. For example, we need to know your name, address and the services you buy from us to properly provide and bill for those services. When you call us, our representatives pull up account records and may refer to your bill, your calling patterns, and other information we have to answer questions you may have or recommend how we can best serve you.

We may also use information in our records to protect our customers, employees or property — for instance, to investigate fraud, harassment or other types of unlawful service activities involving Qwest or other carriers that we do business with. In some cases, it may be necessary to provide this information to the government or third parties who make a lawful demand for it.

We share information within our Qwest companies to enable us to better understand our customers' product and service needs, and to learn how to best design, develop, and package products and services to meet those needs. Like any large business, we may structure our company to include a number of smaller companies. Currently, our primary lines of business include local and long-distance services, wireless services, cable services, dedicated web hosting, Internet access for businesses and consumers, on-line services, and directory publishing. We also offer other products and services, for example, Frame Relay, Asynchronous Transfer Mode (ATM), telephone equipment, voice mail services, and directory advertising.

Accuracy of the Information We Hold

We want the information we obtain and use about customers to be accurate. If your service information or your personal contact information changes or you see an inaccuracy on your Qwest bill, let us know so we can correct it.

Security and Accountability

We have information systems that collect and store customer information in addition to systems that store our own business records. These systems have different types of security as appropriate for the information stored. Qwest requires employees to keep customer information confidential and we hold them accountable for their actions.

Providing Services to Enhance Your Privacy

Non-published numbers, Caller ID and Caller ID blocking services, Anonymous Call Rejection, and No Solicitation are among the privacy services Qwest offers to enhance your privacy.

Disclosure of Information Outside Qwest

As a general rule, Qwest does not release customer account information to unaffiliated third parties without your permission unless we have a business relationship with those companies where the disclosure is appropriate. For example, we may hire outside companies as contractors or agents; or we might be engaged in a joint venture or partnership with a company. Upon occasion, Qwest may decide to stop providing a service or may decide to sell or transfer parts of our business to unaffiliated companies. When this happens, we may provide confidential customer information to these companies so that they can offer you the same or similar services. In all of these situations, we provide information to these other companies only as needed to accomplish our business objectives and the companies are bound by requirements to keep Qwest customers' information confidential.

There are exceptions to the general rule. For example, we might provide information to regulatory or administrative agencies so that they can accomplish their regulatory tasks (for example, responding to a customer complaint) or to maximize the efficiencies of our own processes (such as getting mailing addresses correct, for example). Other disclosures will be driven by legal requirements imposed on Qwest. Qwest complies with "legal process," such as a subpoena or court order or other similar demand, associated with either criminal or civil proceedings.

Disclosure of Account Information

If you tell us in writing to release your account information to someone, we will honor your request and provide that information.

Your account information is released to other carriers when you give us your permission or when they advise us they have your approval to access the information. This most often occurs with respect to a sale of service they want to make or have made to you. Unless we are advised that permission from you has been granted, we do not release the information.

We may provide account information to collection agencies when customers do not pay their bills. We restrict the use that can be made of this information to collection activities only for our charges and for the charges we bill for others.

Other carriers use Qwest to bill for their charges. In this case, they provide us with information about you, including your calling patterns, and we bill you on their behalf. In turn, we provide them with non-sensitive information about your service, such as the date your service was established or disconnected; whether you have toll or 900 blocking services, whether you have a calling card or not and when it was issued, how you pay your bills and if they are paid on time.

Disclosure of Customer Telephone Numbers, Names and Addresses

Telephone number, name and sometimes address information is "released" by Qwest in different ways. It is sometimes released as "lists" to entities that are entitled by law to receive the information or which have entered into contracts with Qwest to receive it. The information is sometimes released through the network "transactionally," such as when your phone number and name are released through a Caller ID mechanism. Sometimes the information is provided in reports to those persons who are being called by you and want to know more about who is calling them and when. Whether a number is recognized as "published" or not will generally depend on

the medium by which the number is captured and released.

For example, a person can ask Qwest to include them in directories (that is "publish" their number) or not. Persons can ask to not be published in directories but included in Directory Assistance (non-listed numbers). Or persons can ask not to be either in directories or Directory Assistance (non-published). All of these terms refer to a "listing" status.

However, the telephone **network** does not recognize a number as published/listed or non-listed or non-published. Thus, the network will "pass" that number to interconnecting carriers (local, long-distance, wireless) and to called parties. Only if the network (a) has the capability to block the number; and (b) you have invoked a blocking mechanism will the called party (but not the carriers in between) be unable to see the calling number. And, where both the calling number and name are "carried" as part of the network call, generally both will be displayed or both will be blocked.

In some cases, such as on some party- or coin-operated lines, as well as calls to pay-per-call (900) or toll-free numbers (such as 800/888/877 numbers), the network does not have the capability to block your underlying phone number even if you invoke Caller ID blocking. And there may be other services that rely on this type of automatic number identification (ANI) technology, such as cable companies that offer movies keyed to the automatic delivery of your phone number or pizza companies that route your calls to the closest stores based on your number. There are a variety of businesses that subscribe to these types of services. By federal regulation, however, businesses that utilize this technology can only use it to provide you the service in question or one directly related to it. And, because federal law requires phone numbers associated with facsimile transmissions to be released as part of the facsimile, these phone numbers are not blocked either.

When you order services from us to connect to an Internet Service Provider (ISP) or choose a carrier, we may need to advise them of your telephone number in order that they may provide your requested service. This includes non-listed and non-published telephone numbers.

In addition to the above types of disclosures, Qwest is required, by law, to make disclosures of customer telephone number, name and address information in certain circumstances, including those described below.

- We are required to provide **listed** customer names, addresses and telephone numbers to directory publishers - our own and others. Qwest and other directory publishers may publish this information in alphabetical or reverse directories that take the form of paper directories, electronic directories over the Internet, or on CDs. We also provide customer name and addresses for all customers (including non-listed and non-published customers) to directory publishers to allow for directory deliveries, but only for that purpose.
- We are required to provide customer names, addresses and telephone numbers to directory assistance and operator services providers. This information includes non-listed information, as well as the name and address of non-published customers. By contract, Qwest requests these companies to honor the privacy indicators that may be included in their purchased lists and such indicators are included for nonlisted and nonpublished numbers. Some of these providers offer Internet or online directory assistance services.

- In some cases, when you dial 911, your name, address and telephone number information is provided to the emergency service provider. And, by law, we are required to provide this information, including non-listed and non-published information, to emergency service providers and emergency support services providers upon request in a more comprehensive format.

- If you place a long-distance call using a provider other than the one you use on your home phone -- for example, if you place a calling card or third number billed call from a pay phone - Qwest is required by law to provide billing name and address information to the service provider. This includes names and addresses associated with non-published and non-listed information where the individual has not objected. This information cannot be used for marketing purposes. Similar information is provided with respect to the provision of services by non-Qwest carriers.

We might provide your name and address to administrative agencies where we are working with them to minimize costs and maximize accuracy. For example, we might share this information with the Post Office so that we continue to get reduced postage rates and you get your bills and other information from us in a cost-efficient, reliable and timely fashion.

We also compile lists of customer names, addresses and telephone numbers of the type printed in the White Pages directories and provide these lists to qualified companies that are conducting product promotions. Non-published and non-listed numbers are not included in these lists and we remove other customers from these lists by request.

Your Control Over the Disclosure of Information

You tell us the telephone listings you want to include in our directories and in directory assistance. You also may choose to have a non-published or non-listed number, or to exclude your address from your listing.

As we addressed above, in certain cases you can block the transmission of your telephone number (and name) to those persons you call.

Our Qwest divisions may provide you with information about new products and services or special promotions. However, Qwest does maintain an internal "Do Not Call" list in line with federal law. If you ask not to be contacted, the business or division that is calling you will put your telephone number on a list. Other Qwest business divisions will still be able to call you unless you make it clear that you do not want to be contacted by any Qwest business unit. Some states have adopted their own "Do Not Call" laws, which are usually managed by a third party database administer. Often those laws permit continued contact with persons whose numbers are on the list when there is an existing business relationship, so you might get a call from us even if you are on these kinds of lists.

It is Qwest's practice to stop sending direct mail materials to individuals that request it not be sent. There are no laws that control this accommodation but we respect the desire of individuals to be free of such communications if they wish.

Qwest or its business partners may use e-mail to communicate with customers about events or new products and services or to respond to visitor's e-mails. Our residential local telephone service customers may visit our qwest.com web site, E-mail Contact Preferences page to add or remove themselves from our email list. If you receive unwanted email from us you may also remove yourself from our email list by simply following the "unsubscribe" instructions in the email. We will not send commercial solicitations to customers who request it not be sent. Please note that if

you do go through this process, some e-mail messages may still come to you, although not those dealing with commercial solicitations. For example, we may e-mail you about viruses, or changes to your service, or other types of product advisories.

We honor customer requests to have their names removed from lists that Qwest might provide to firms desiring to do product promotions. Customers with non-listed and non-published numbers are not included on the lists. For individuals with listed information, if you do not wish to have your name included on such lists, just tell us and we will remove your name at no charge.

Qwest Choice TV & OnLine Services™

For more information on our Customer Privacy Policy related to Qwest Choice TV & OnLine Services click here.

To improve the services it can offer you, Qwest may opt to expand its capabilities for obtaining information about users in the future. Qwest will update this privacy policy continually to ensure that you are aware of developments in this area.

Should you have any questions or comments relating to this Privacy Policy or Qwest privacy practices, please contact Qwest at Privacy@qwest.com.

Back to Top

ABOUT QWEST | CAREERS AT QWEST

Gregory M. Romano
General Counsel
Northwest Region

WA0105GC
1800 41st Street
Everett, WA 98201

Phone 425 261-5460
Fax 425 261-5262

Email address:
Gregory.M.Romano@verizon.com

September 18, 2006

VIA ELECTRONIC AND OVERNIGHT MAIL

Mark E. Friedman, Esq.
Keith S. Dubanevich, Esq.
Garvey Schubert Barer
121 SW Morrison Street, 11th Floor
Portland, OR 97204-3141

Re: Letter from ACLU of Oregon dated September 8, 2006

Dear Messrs. Friedman and Dubanevich:

Thank you for your letter dated September 8, 2006, on behalf of the ACLU of Oregon ("ACLU"). You note that responses by Verizon Northwest Inc. ("Verizon NW") to the two questions posed in the letter "may be helpful ... in determining whether it is necessary for the [ACLU] to proceed before the PUC." For all the reasons set forth in Verizon NW's July 5th response to the ACLU's original filing to the Oregon Public Utilities Commission ("Commission"), the ACLU should not continue attempts to convince the Commission to hear or investigate this matter. The Commission would be unable to adduce any facts relating to, and thus unable to resolve, the issues raised in the ACLU's filings. As you know, the Oregon Attorney General recognized the difficulties in attempting to collect relevant information while national security issues are being resolved at the federal level, and elected on August 4th not to pursue a similar ACLU investigation request into these matters at this time.

As you know, Verizon NW can neither confirm nor deny whether it has any relationship to the counter-terrorism program aimed at al Qaeda involving the National Security Agency. However, as Verizon has previously stated, it (including Verizon NW) has not knowingly disclosed, provided or revealed to another person or entity (or enabled another person or entity to obtain) the contents or phone records of Oregon telecommunications customers other than in compliance with applicable law.

I hope this answer to your questions is helpful, and that the ACLU now recognizes that it should not seek Commission involvement in this matter.

Sincerely,

Gregory M. Romano

GMR:pl

Qwest
Spirit of Service™

Qwest
421 Southwest Oak Street
Suite 810
Portland, Oregon 97204
Telephone: 503-242-5623
Facsimile: 503-242-8589
e-mail: alex.duarte@qwest.com

Alex M. Duarte
Corporate Counsel

September 18, 2006

Mark E. Friedman
Keith S. Dubanevich
Garvey Schubert Barer
121 SW Morrison St., 11th Floor
Portland, OR 97204-3141

Gentlemen:

Thank you for your September 8, 2006 letter in which you ask Qwest to respond in writing to certain questions raised in the letter.

On June 14, 2006, Qwest filed its response with the Oregon Public Utility Commission in docket UM 1265, in which Qwest stated it had "no comment or other response to Complainant's Complaint at this time." Qwest continues to have no comment on these issues, and thus declines to comment on your letter or answer any questions raised in your letter.

Thank you.

Very truly yours,

Alex M. Duarte

AMD:cmb