

1  
2  
3  
4  
5  
6  
7 BEFORE THE PUBLIC UTILITY COMMISSION  
8 OF OREGON  
9 UM 1265

10 AMERICAN CIVIL LIBERTIES UNION  
11 OF OREGON, INC. and AMERICAN  
12 CIVIL LIBERTIES UNION  
13 FOUNDATION OF OREGON, INC.,

14 Complainants,

15 v.

16 VERIZON NORTHWEST, INC., and  
17 QWEST CORPORATION,

18 Defendants.

COMPLAINANTS' MOTION TO LIFT  
ABEYANCE ORDER

18 The American Civil Liberties Union of Oregon and the American Civil Liberties  
19 Union Foundation of Oregon, Inc. (hereinafter referred to jointly as "ACLU") move the  
20 Oregon Public Utility Commission ("PUC") to lift the stay of proceedings dated  
21 December 11, 2006. In the year since the PUC's order, a U.S. government official  
22 has disclosed additional information about its electronic surveillance program,  
23 Verizon has revealed details about its cooperation with government investigations, a  
24 U.S. District Judge has ruled that the Supremacy Clause and the foreign affairs  
25 power of the federal government do not prohibit state or private investigations of the  
26 telecommunications companies, and most recently the Vermont Public Service

1 Board has allowed discovery of two telecommunications companies to proceed.  
2 Because of these developments, the ACLU contends that the PUC should lift its stay  
3 of proceedings to allow the ACLU to initiate discovery into non-privileged matters.

4 **I. RECENT DISCLOSURE OF ADDITIONAL INFORMATION ABOUT**  
5 **TELECOMMUNICATION COMPANIES' COOPERATION WITH THE U.S.**  
6 **GOVERNMENT'S ELECTRONIC SURVEILLANCE PROGRAM NEGATES ANY**  
7 **PLEA OF NATIONAL SECURITY**

8 As detailed in the ACLU's First Amended Complaint, in May 2006, *USA Today*  
9 revealed that since shortly after 9/11 at least two major phone companies have been  
10 voluntarily granting the NSA direct, mass access to their customers' calling records,  
11 and that the NSA had compiled a giant database of those records. Leslie Cauley,  
12 "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2006.  
13 Subsequently confirmed by 19 lawmakers, this program extends to all Americans,  
14 not just those suspected of terrorist or criminal activity. Susan Page, "Lawmakers:  
15 NSA Database Incomplete," *USA Today*, June 30, 2006.

16 A few months ago, the Director of National Intelligence, Mike McConnell,  
17 officially confirmed the substance of these allegations. In an interview with the *El*  
18 *Paso Times*, Director McConnell described the Bush Administration's rationale for  
19 changes to the Foreign Intelligence Surveillance Act ("FISA") including the difficulty  
20 in securing warrants and the need to seek immunity for telecommunications  
21 companies. He stated, "[n]ow the second part of the issue was under the president's  
22 program, the terrorist surveillance program, the private sector had assisted us.  
23 Because if you're going to get access you've got to have a partner and they were  
24 being sued." Chris Roberts, *Transcript: Debate on the foreign intelligence surveillance*  
25 *act*, EL PASO TIMES, August 23, 2007 (link:  
26 [http://www.elpasotimes.com/ci\\_6685679?source=most\\_viewed](http://www.elpasotimes.com/ci_6685679?source=most_viewed)) (emphasis added).

A full copy of the transcript of this interview is attached as Exhibit "A" to Declaration

1 of Keith S. Dubanevich.

2 Throughout the entire course of the proceedings brought by the ACLU, and  
3 investigations conducted by regulators across the country, the telecommunications  
4 companies and the National Security Agency have maintained that their program is  
5 so secret that any discussion or investigation of it would jeopardize national security  
6 and that any investigation or suit would inevitably be wiped out by the government's  
7 official privilege against revealing state secrets (the state secrets privilege).

8 With this interview Director McConnell has cast serious doubt on both of  
9 those assertions. Indeed, the limited investigation requested by the ACLU would be  
10 into whether Verizon illegally shared information with the NSA or with anyone else.  
11 Director McConnell has confirmed that cooperation, and hence the ACLU's  
12 complaint and requested investigation will cause no harm to national security,  
13 particularly given Director McConnell's apparent belief that disclosure of the  
14 program is permissible. Further, the state secrets privilege only applies to secret  
15 government activities and programs. By granting this interview Director McConnell  
16 has lifted the veil of that official secrecy and increased the likelihood that court  
17 cases, both those brought by regulators and by private parties, can and will go  
18 forward.

19 **II. JUDGE WALKER DENIED SUMMARY JUDGMENT ON SUPREMACY**  
20 **CLAUSE AND FOREIGN AFFAIRS POWERS GROUNDS**

21 As the PUC is aware, the Judicial Panel on Multidistrict Litigation has  
22 transferred numerous telecommunications civil actions to the Northern District of  
23 California. On July 26, 2006, Judge Vaughn R. Walker issued an order that denied  
24 dismissal of the cases on the basis of the state secrets privilege. More recently, on  
25 July 24, 2007, Judge Walker ruled in a careful and well written analysis that the  
26 Supremacy Clause does not require dismissal of the various civil actions. (Exhibit

1 “B” to Dubanevich Declaration). The PUC reached an identical conclusion in its  
2 December 11, 2006, Order. Judge Walker also ruled that the foreign affairs power of  
3 the federal government does not prohibit state and private litigant actions against  
4 telecommunications companies.

5 With respect to the state secrets privilege, the government has conceded that  
6 “some questions posed in these investigations fall outside the privilege’s scope” and  
7 as such are not prohibited. See Exhibit B at page 35. Thus, the state secrets  
8 privilege cannot be raised to bar discovery into matters that fall outside the  
9 privilege’s scope.

### 10 **III. VERIZON HAS PROVIDED DETAILS REGARDING ITS COOPERATION WITH** 11 **GOVERNMENT REQUESTS**

12 On October 12, 2007, Verizon responded to an inquiry from three U.S. House  
13 of Representatives committees that are investigating the telecommunications  
14 industry. (Exhibit “C” to Dubanevich Declaration). In its letter Verizon admits to  
15 having responded to hundreds of government requests that sought customer  
16 information (phone call data) prior to receiving a court order. In addition, from  
17 January 2005 to September 2007, Verizon provided data, including internet protocol  
18 addresses, to federal authorities a total of 94,000 times. Clearly, when Verizon  
19 perceives that disclosing Verizon’s cooperation with the government may be helpful  
20 to its cause Verizon has done so. But whenever the ACLU or another party has  
21 sought to inquire into Verizon’s improper and illegal disclosure of customer  
22 information, Verizon has resisted all such efforts.

23 Regardless of Verizon’s motivation for disclosing its cooperation with  
24 government investigations, what is clear is that the veil of secrecy has been lifted  
25 and it cannot be legitimately claimed that the electronic surveillance program is so  
26 secret that any discussion or investigation of it would jeopardize national security.

1 **IV. FOLLOWING JUDGE WALKER'S ORDER, THE VERMONT PUBLIC SERVICE**  
2 **BOARD ALLOWED DISCOVERY TO PROCEED ON ALL TOPICS NOT**  
3 **COVERED BY THE STATE SECRETS PRIVILEGE**

4 On October 31, 2007, the Vermont Public Service Board ("VPSB"), which had  
5 previously stayed its proceedings pending the proceedings in the Northern District of  
6 California, reconsidered the stay in light of Judge Walker's July 24, 2007, order.  
7 Just as has been argued here by the ACLU, the Vermont Department of Public  
8 Service asserted that "discovery can be crafted to allow the parties to 'determine  
9 whether Verizon has violated Vermont law regarding the privacy of its customers'  
10 information without running afoul of the state secrets privilege." (Exhibit "D" to  
11 Dubanevich Declaration at page 4). Not surprisingly Verizon opposed any discovery,  
12 even into matters the government has conceded fall outside the scope of the state  
13 secrets privilege.

14 The VPSB first recognized that the cases pending before it had been on hold  
15 for an extended period of time. Second, the VPSB recognized that a number of  
16 courts had rejected many of the claims and defenses asserted by the government  
17 and the telecommunications companies and "found that states retain significant  
18 authority for consumer protection activities." *Id.* at page 9. Indeed, the VPSB noted  
19 Judge Walker's comment that FISA "actually anticipates the application of state law  
20 remedies when a carrier discloses business records without proper authorization."  
21 *Id.* In addition, the VPSB took note of Judge Walker's conclusion that "state  
22 investigations will not inevitably conflict with federal law." *Id.* at 9-10.

23 While the VPSB recognized that the state secrets privilege issue was still  
24 pending before the Ninth Circuit Court of Appeals, "we do not understand the  
25 privilege to be so broad as to prevent general inquiries into the practices of  
26 telecommunications carriers in responding to requests from third parties for  
protected consumer information." *Id.* at 10. Thus, the VPSB allowed discovery of

1 information not covered by the state secrets privilege. In specific, the VPSB allowed  
2 discovery regarding the following issues:

- 3 (1) Current and recent written carrier policies regarding requests  
4 from the government for the release of customer records,  
5 including any policies describing when warrants, letters and  
6 certifications are prerequisite and when, if ever, they are not  
7 required and associated records.
- 8 (2) The carriers' actual practices in determining whether to comply  
9 with requests from the government for the release of customer  
10 records, including carrier record-keeping practices regarding both  
11 the government's requests and their own responses.
- 12 (3) The frequency with which the carriers have actually released  
13 customer records information to the government, the scope of  
14 those disclosures, the legal authority, if any, relied upon, and  
15 associated records, including unclassified national security letters  
16 or certifications required by statute or executive order.
- 17 (4) The accuracy and sufficiency of the carriers' existing customer  
18 privacy notices regarding release of customer record information.
- 19 (5) Whether past responses from the Carriers to the Department or  
20 statements to the public were misleading and inaccurate.

21 **V. THE PUBLIC UTILITIES COMMISSION SHOULD ALLOW DISCOVERY INTO  
22 NON-PRIVILEGED INFORMATION TO ENSURE VERIZON'S COMPLIANCE  
23 WITH APPLICABLE LAW**

24 The PUC is obligated to enforce Oregon law and should allow inquiries into  
25 phone company compliance. Just as the VPSB found, because there are legitimate  
26 areas of inquiry regarding Verizon's conduct that are not covered by the state secrets  
27 privilege, there is no good reason to further delay an inquiry into Verizon's  
28 compliance with applicable law.

29 The inquiries proposed by ACLU are narrow in scope and do not intrude into  
30 the state secrets privilege.<sup>1</sup> For example, on September 8, 2006 the ACLU sent the

---

31 <sup>1</sup> The ACLU requests that the PUC require Verizon to respond to the same  
32 inquiries allowed by the VPSB, as well as the narrow requests previously  
33 propounded by the ACLU.

1 following inquiry to Verizon:

2  
3 1. Has Verizon Northwest Inc. ever disclosed, provided or revealed to  
4 any person or entity, public or private, or enabled any person or entity, public  
5 or private, to obtain the contents of Oregon telecommunications customers'  
6 intrastate telecommunications, voice or data, other than in the following  
7 circumstances:

8 a. in strict compliance with a warrant, subpoena, or other court  
9 order; or

10 b. in strict compliance with federal law, including 18 U.S.C. §§ 2510-  
11 2522, 18 U.S.C. §§ 2701-2712, and 50 U.S.C. §§ 1801-1811?

12 If that has ever occurred, under what authority were such  
13 intrastate telecommunications contents disclosed, provided or revealed to or  
14 obtainable by any person or entity, public or private?

15 2. Has Verizon Northwest, Inc. ever disclosed, provided or revealed to  
16 any person or entity, public or private, or enabled any person or entity, public  
17 or private, to obtain information about or data describing the  
18 intrastate telecommunication activity of Oregon telecommunications  
19 customers, voice or data, other than in the following circumstances:

20 a. in strict compliance with a warrant, subpoena, or other court  
21 order; or

22 b. in strict compliance with Or. Admin. R. 860-032-0510; or

23 c. in strict compliance with federal law, including 18 U.S.C. §§ 2510-  
24 2522, 18 U.S.C. §§ 2701-2712, and 50 U.S.C. §§ 1801-1811?

25 If that has ever occurred, under what authority was information about or data  
26 describing the intrastate telecommunication activity of Oregon  
telecommunications customers disclosed, provided or revealed to or obtainable  
by any person or entity, public or private?

(Exhibit "E" to Dubanevich Declaration, emphasis added)

As the PUC will notice, the ACLU does not inquire into international  
telecommunications, nor does the ACLU inquire into Verizon's cooperation with the  
NSA. Rather, these requests are narrowly tailored to focus only on Verizon's illegal  
disclosure of intrastate telecommunications. These requests do not require Verizon

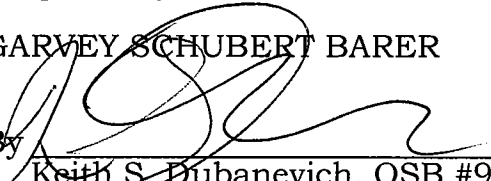
1 to disclose anything about its lawful cooperation with government authorities.  
2 Indeed, these requests specifically seek information about only whether Verizon has  
3 ever provided phone call content or data without proper legal justification.

4 There is nothing in these requests that could in any way intrude upon the  
5 state secrets privilege as that privilege presumably covers only lawful cooperation  
6 with the government pursuant to FISA or some other legal authority. Moreover,  
7 Verizon has no standing to assert the state secrets privilege so any such privilege  
8 should not be a bar to allowing discovery to go forward at this time. *U.S. v.*  
9 *Reynolds*, 345 US 1, 7 (1953). As a consequence, whatever the Ninth Circuit decides  
10 in *Hepting et al., v. AT&T Corp., et al.*, 439 FSupp 2d 974 (ND Cal 2006) will have no  
11 impact on this case because the limited inquiry posed by the ACLU here does not  
12 intrude upon the state secrets privilege which cannot be invoked by Verizon in any  
13 event.

14 DATED this 6th day of December, 2007.

15 Respectfully submitted,

16 GARVEY SCHUBERT BARER

17   
18 By Keith S. Dubanevich, OSB #975200  
19 E-Mail: kubanevich@gsblaw.com  
20 Mark E. Friedman, OSB #730947  
21 E-Mail: mfriedman@gsblaw.com  
22 Telephone: (503) 228-3939  
23 Facsimile: (503) 226-0259

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



1 **CERTIFICATE OF SERVICE**

2 I hereby certify that the foregoing **COMPLAINANTS' MOTION TO LIFT**  
3 **ABEYANCE ORDER** was served on:

4 Heather Zachary  
5 Wilmer Cutler Pickering  
6 Hale and Dorr LLP  
7 1875 Pennsylvania Avenue, NW  
8 Washington, DC 20009  
9 E-Mail: [heather.zachary@wilmerhale.com](mailto:heather.zachary@wilmerhale.com)

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

8 Gregory Romano  
9 General Counsel  
10 Verizon Corporate Services  
11 MC WA0105RA  
12 1800 41<sup>st</sup> Street  
13 Everett, WA 98201  
14 E-mail: [Gregory.m.romano@verizon.com](mailto: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](mailto:renee.willer@verizon.com)

13 Citizens' Utility Board of Oregon  
14 OPUC Dockets  
15 610 SW Broadway, Ste. 308  
16 Portland, OR 97205  
17 E-Mail: [dockets@oregoncub.org](mailto:dockets@oregoncub.org)

17 by mailing to them a copy of the original thereof, contained in sealed envelopes,  
18 addressed as above set forth, with postage prepaid, and deposited in the mail in  
19 Portland, Oregon, on December 6, 2007.

20   
21 Keith S. Dubanevich, OSB#975200  
22 Attorneys for Complainants

23 PDX\_DOCS:403370.1 [30186-00114]

1  
2  
3  
4  
5  
6  
7 BEFORE THE PUBLIC UTILITY COMMISSION  
8 OF OREGON  
9 UM 1265

10 AMERICAN CIVIL LIBERTIES UNION  
11 OF OREGON, INC. and AMERICAN  
12 CIVIL LIBERTIES UNION  
13 FOUNDATION OF OREGON, INC.,

14 Complainants,

15 v.

16 VERIZON NORTHWEST, INC., and  
17 QWEST CORPORATION,

18 Defendants.

DECLARATION OF KEITH S.  
DUBANEVICH IN SUPPORT OF  
COMPLAINANTS' MOTION TO LIFT  
ABEYANCE ORDER

19 1. My name is Keith Scott Dubanevich. I am one of the attorneys for the  
20 Complainants. I am over the age of eighteen, have personal knowledge of every  
21 statement contained herein and they are all true and correct.

22 2. Attached hereto as exhibit "A" is a true and correct copy of *Transcript:*  
23 *Debate on the foreign intelligence surveillance act*, EL PASO TIMES, August 23, 2007  
24 (link: [http://www.elpasotimes.com/ci+-6685679?source=most viewed](http://www.elpasotimes.com/ci+-6685679?source=most%20viewed)).

25 3. Attached hereto as exhibit "B" is a true and correct copy of the July 24,  
26 2007, Order in MDL Docket No 06-1791 VRM, *In re National Security Agency*

1 *Telecommunications Records Litigation.*

2 4. Attached hereto as exhibit "C" is a true and correct copy of a letter dated  
3 October 12, 2007, from Randal S. Milch, Senior Vice President, Legal & External  
4 Affairs & General Counsel, Verizon Business to The Honorable John D. Dingell, The  
5 Honorable Edward J. Markey, and The Honorable Bart Stupak.

6 5. Attached hereto as exhibit "D" is a true and correct copy of Vermont  
7 Public Service Board Order dated October 31, 2007 in Docket Nos. 7183, 7192 and  
8 7193.

9 6. Attached hereto as exhibit "E" is a true and correct copy of a letter sent  
10 by Garvey Schubert Barer to Verizon dated September 8, 2006.

11 DATED this 6th day of December, 2007

12  
13  
14   
15 Keith S. Dubanevich, OSB #975200  
16 E-Mail: kdubanevich@gsblaw.com  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

1 **CERTIFICATE OF SERVICE**

2 I hereby certify that the foregoing **DECLARATION OF KEITH S.**

3 **DUBANEVICH IN SUPPORT OF COMPLAINANTS' MOTION TO LIFT ABEYANCE**

4 **ORDER** was served on:

5  
6 Heather Zachary  
7 Wilmer Cutler Pickering  
8 Hale and Dorr LLP  
9 1875 Pennsylvania Avenue, NW  
10 Washington, DC 20009  
11 E-Mail: [heather.zachary@wilmerhale.com](mailto:heather.zachary@wilmerhale.com)

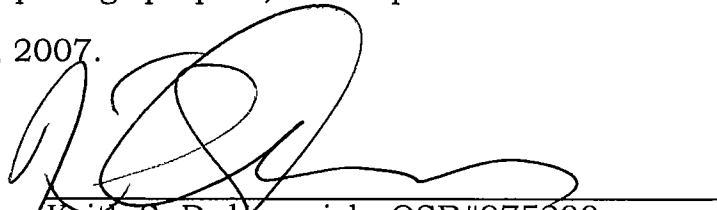
Jason Eisdorfer  
Energy Program Director  
Citizens' Utility Board of Oregon  
610 SW Broadway, Ste. 308  
Portland, OR 97205  
E-Mail: [Jason@oregoncub.org](mailto:Jason@oregoncub.org)

9  
10 Gregory Romano  
11 General Counsel  
12 Verizon Corporate Services  
13 MC WA0105RA  
14 1800 41<sup>st</sup> Street  
15 Everett, WA 98201  
16 E-mail: [Gregory.m.romano@verizon.com](mailto: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](mailto:renee.willer@verizon.com)

14 Citizens' Utility Board of Oregon  
15 OPUC Dockets  
16 610 SW Broadway, Ste. 308  
17 Portland, OR 97205  
18 E-Mail: [dockets@oregoncub.org](mailto:dockets@oregoncub.org)

18 by mailing to them a copy of the original thereof, contained in sealed envelopes,  
19 addressed as above set forth, with postage prepaid, and deposited in the mail in  
20 Portland, Oregon, on December 6, 2007.

21  
22   
23 Keith S. Dubanevich, OSB#975200  
24 Attorneys for Complainants

24 PDX\_DOCS:404240.1

Now 78°F  
High 80°F  
Low 50°F  
5 DAY FORECAST

search

Site  Web Search powered by YAHOO! SEARCH

**El Paso Times** | **Inside El Paso** | **Southwest Parent** | **Jobs** | **Cars** | **Classifieds** | **Real Estate** | **Apartments** | **Shopping**

News | New & Updated | Military | Weather | Mobile Alerts | Blogs | Forums | Letters to the Editor | Living | Obituaries | Español | Customer Service

del.icio.us | Digg | Reddit | YahooMyWeb | Google | Facebook | What's this?

### Transcript: Debate on the foreign intelligence surveillance act

By Chris Roberts / A@El Paso Times  
Article Launched: 08/22/2007 01:05:57 AM MDT

The following is the transcript of a question and answer session with National Intelligence Director Mike McConnell.

Question: How much has President Bush or members of his administration formed your response to the FISA debate?

Answer: Not at all. When I came back in, remember my previous assignment was director of the NSA, so this was an area I have known a little bit about. So I came back in. I was nominated the first week of January. The administration had made a decision to put the terrorist surveillance program into the FISA court. I think that happened the 7th of Jan. So as I come in the door and I'm prepping for the hearings, this sort of all happened. So the first thing I want to know is what's this program and what's the background and I was pretty surprised at what I learned. First off, the issue was the technology had changed and we had worked ourselves into a position that we were focusing on foreign terrorist communications, and this was a terrorist foreigner in a foreign country. The issue was international communications are on a wire so all of a sudden we were in a position because of the wording in the law that we had to have a warrant to do that. So the most important thing to capture is that it's a foreigner in a foreign country, required to get a warrant. Now if it were wireless, we would not be required to get a warrant. Plus we were limited in what we were doing to terrorism only and the last time I checked we had a mission called foreign intelligence, which should be construed to mean anything of a foreign intelligence interest, North Korea, China, Russia, Syria, weapons of mass destruction proliferation, military development and it goes on and on and on. So when I engaged with the administration, I said we've gotten ourselves into a position here where we need to clarify, so the FISA issue had been debated and legislation had been passed in the house in 2006, did not pass the Senate. Two bills were introduced in the Senate, I don't know if it was co-sponsorship

Advertisement

### More headlines

- Man stabbed to death
- Many feel Bliss expansion excuse for tax hike
- Man's trial in slaying of landlord to continue
- Voters decide if schools get \$400 million
- Vote for police chief suggested
- Study foresees \$21.7 billion for city from Bliss influx
- Reyes, others tell children importance of veterans
- County to edit 2002 Coliseum bond issuance
- Professor to train new principals in Chicago
- Progress brings hope for Bliss unit

### Most Viewed Stories

(From the last 12 hours)

1. Man stabbed to death
2. Third child of wounded Bliss soldier dies after crash
3. High schools top 10
4. L.A. Times writer takes more jobs at El Paso
5. EP toddler killed in crash near Las Cruces
6. Home sales plunge in El Paso
7. Man dies during dispute, wife taken into custody
8. Overnight stabbing sends man to hospital
9. Man's trial in slaying of landlord to continue
10. Miners will 'get back to work' after loss to Rice

Top Jobs

or two different bills, but Sen. (Dianne Feinstein, D-Calif.) had a bill and Sen. Specter had a bill and it may have been the same bill, I don't know, but the point is a lot of debate, a lot of dialogue. So, it was submitted to the FISA court and the first ruling in the FISA court was what we needed to do we could do with an approval process that was at a summary level and that was OK, we stayed in business and we're doing our mission. Well in the FISA process, you may or may not be aware ...

Q: When you say summary level, do you mean the FISA court?

A: The FISA court. The FISA court ruled presented the program to them and they said the program is what you say it is and it's appropriate and it's legitimate, it's not an issue and was had approval. But the FISA process has a renewal. It comes up every so many days and there are 11 FISA judges. So the second judge looked at the same data and said well wait a minute I interpret the law, which is the FISA law, differently. And it came down to, if it's on a wire and it's foreign in a foreign country, you have to have a warrant and so we found ourselves in a position of actually losing ground because it was the first review was less capability, we got a stay and that took us to the 31st of May. After the 31st of May we were in extremis because now we have significantly less capability. And meantime, the community, before I came back, had been working on a National Intelligence Estimate on terrorist threat to the homeland. And the key elements of the terrorist threat to the homeland, there were four key elements, a resilient determined adversary with senior leadership willing to die for the cause, requiring a place to train and develop, think of it as safe haven, they had discovered that in the border area between Pakistan and Afghanistan. Now the Pakistani government is pushing and pressing and attempting to do something about it, but by and large they have areas of safe haven. So leadership that can adapt, safe haven, intermediate leadership, these are think of them as trainers, facilitators, operational control guys. And the fourth part is recruits. They have them, they've taken them. This area is referred to as the FATA, federally administered tribal areas, they have the recruits and now the objective is to get them into the United States for mass casualties to conduct terrorist operations to achieve mass casualties. All of those four parts have been carried out except the fourth. They have em, but they haven't been successful. One of the major tools for us to keep them out is the FISA program, a significant tool and we're going the wrong direction. So, for me it was extremists to start talking not only to the administration, but to members of the hill. So from June until the bill was passed, I think I talked to probably 260 members, senators and congressmen. We submitted the bill in April, had an open hearing 1 May, we had a closed hearing in May, I don't remember the exact date. Chairman (U.S. Rep. Silvestre Reyes, D-Texas) had two hearings and I had a chance to brief the judiciary committee in the house, the intelligence committee in the house and I just mentioned the Senate, did not brief the full judiciary committee in the Senate, but I did meet with Sen. (Patrick Leahy, D-Vt.) and Sen. (Arlen Specter, R-Pa.) and I did have an opportunity on the Senate side, they have a tradition there of every quarter they invite the director of national intelligence in to talk to them update them on topics of interest. And that happened in (June 27). Well what they wanted to hear about was Iraq and Afghanistan and for whatever reason, I'm giving them my review and they ask questions in the order in which they arrive in the room. The second question was on FISA, so it gave me an opportunity to, here I am worrying about this problem and I have 41 senators and I said several things. The current threat is increasing, I'm worried about it. Our capability is decreasing and let me explain the problem.

Q: Can't you get the warrant after the fact?

A: The issue is volume and time. Think about foreign intelligence. What it presented me with an opportunity is to make the case for something current, but what I was really also trying to put a strong emphasis on is the need to do foreign intelligence in any context. My argument was

Healthcare FT Physical Therapist  
Professional The Hoover Compensation  
General Correctional Officer  
Enthusiastic & energetic person  
desired to be part of a growing  
dental team.  
Professional The Hoover Compensation  
ALL LISTINGS

CLICK TO VIEW  
**careerbuilder** TV

SELECT A CATEGORY:

POWERED BY DMC

that the intelligence community should not be restricted when we are conducting foreign surveillance against a foreigner in a foreign country, just by dint of the fact that it happened to touch a wire. We haven't done that in wireless for years.

Q: So you end up with people tied up doing paperwork?

A: It takes about 200 man hours to do one telephone number. Think about it from the judges standpoint. Well, is this foreign intelligence? Well how do you know it's foreign intelligence? Well what does Abdul calling Mohammed mean, and how do I interpret that? So, it's a very complex process, so now, I've got people speaking Urdu and Farsi and, you know, whatever, Arabic, pull them off the line have them go through this process to justify what it is they know and why and so on. And now you've got to write it all up and it goes through the signature process, take it through (the Justice Department), and take it down to the FISA court. So all that process is about 200 man hours for one number. We're going backwards, we couldn't keep up. So the issue was ...

Q: How many calls? Thousands?

A: Don't want to go there. Just think, lots. Too many. Now the second part of the issue was under the president's program, the terrorist surveillance program, the private sector had assisted us. Because if you're going to get access you've got to have a partner and they were being sued. Now if you play out the suits at the value they're claimed, it would bankrupt these companies. So my position was we have to provide liability protection to these private sector entities. So that was part of the request. So we went through that and we argued it. Some wanted to limit us to terrorism. My argument was, wait a minute, why would I want to limit it to terrorism. It may be that terrorists are achieving weapons of mass destruction, the only way I would know that is if I'm doing foreign intelligence by who might be providing a weapon of mass destruction.

Q: And this is still all foreign to foreign communication?

A: All foreign to foreign. So, in the final analysis, I was after three points, no warrant for a foreigner overseas, a foreign intelligence target located overseas, liability protection for the private sector and the third point was we must be required to have a warrant for surveillance against a U.S. person. And when I say U.S. person I want to make sure you capture what that means. That does not mean citizen. That means a foreigner, who is here, we still have to have a warrant because he's here. My view is that that's the right check and balances and it's the right protection for the country and lets us still do our mission for protection of the country. And we're trying to fend off foreign threats.

Q: So are you satisfied with it the way it is now?

A: I am. The issue that we did not address, which has to be addressed is the liability protection for the private sector now is proscriptive, meaning going forward. We've got a retroactive problem. When I went through and briefed the various senators and congressmen, the issue was alright, look, we don't want to work that right now, it's too hard because we want to find out about some issues of the past. So what I recommended to the administration is, 'Let's take that off the table for now and take it up when Congress reconvenes in September.'

Q: With an eye toward the six-month review?

A: No, the retroactive liability protection has got to be addressed.

Q: And that's not in the current law?

A: It is not. Now people have said that I negotiated in bad faith, or I did not keep my word or whatever...

Q: That you had an agenda that you weren't honest about.

A: I'll give you the facts from my point of view. When I checked on board I had my discussion with the president. I'm an apolitical figure. I'm not a Republican, I'm not a Democrat. I have voted for both. My job is as a professional to try to do this job the best way I can in terms of, from the intelligence community, protect the nation. So I made my argument that we should have the ability to do surveillance the same way we've done it for the past 50 years and not be inhibited when it's a foreigner in a foreign country. The president's guidance to me early in the process, was, 'You've got the experience. I trust your judgement. You make the right call. There's no pressure from anybody here to tell you how to do it. He did that early. He revisited with me in June. He did it again in July and he said it publicly on Friday before the bill was passed. We were at the FBI, it's an annual thing, we go to the FBI and do a homeland security kind of update. So he came out at noon and said, 'I'm requesting that Congress pass this bill. It's essential. Do it before you go on recess. I'm depending on Mike McConnell's recommendations. And that was the total sum and substance of the guidance and the involvement from the White House with regard to how I should make the call. Now, as we negotiated, we started with 66 pages, were trying to get everything cleaned up at once. When I reduced it to my three points, we went from 66 pages to 11. Now, this is a very, very complex bill. I had a team of 20 lawyers working. You can change a word in a paragraph and end up with some major catastrophe down in paragraph 27, subsection 2c, to shut yourself down, you'll be out of business. So when we send up our 11 pages, we had a lot of help in making sure we got it just right so it would come back and we'd say wait a minute we can't live with this or one of the lawyers would say, 'Wait we tried that, it won't work, here's the problem.' So we kept going back and forth, so we sent up a version like Monday, we sent up a version on Wednesday, we sent up a version on Thursday. The House leadership, or the Democratic leadership on Thursday took that bill and we talked about it. And my response was there are some things I can't live with in this bill and they said alright we're going to fix them. Now, here's the issue. I never then had a chance to read it for the fix because, again, it's so complex, if you change a word or phrase, or even a paragraph reference, you can cause unintended ...

Q: You have to make sure it's all consistent?

A: Right. So I can't agree to it until it's in writing and my 20 lawyers, who have been doing this for two years, can work through it. So in the final analysis, I was put in the position of making a call on something I hadn't read. So when it came down to crunch time, we got a copy and it had some of the offending language back in it. So I said, 'I can't support it.' And it played out in the House the way it played out in the House. Meantime on the Senate side, there were two versions being looked at. The Wednesday version and the Thursday version. And one side took one version and the other side took the other version. The Thursday version, we had some help, and I didn't get a chance to review it. So now, it's Friday night, the Senate's voting. They were having their debate and I still had not had a chance to review it. So, I walked over, I was up visiting some senators trying to explain some of the background. So I walked over to the chamber and as I walked into the office just off the chamber, it's the vice president's office, somebody gave me a copy. So I looked at the version and said, 'Can't do it. The same language was back in there.'

Q: What was it?

A: Just let me leave it, not too much detail, there were things with regard to our authorities



some language around minimization. So it put us in an untenable position. So then I had another version to take a look at, which was our Wednesday version, which basically was unchanged. So I said, well certainly, I'm going to support that Wednesday version. So that's what I said and the vote happened in the Senate and that was on Friday. So now it rolled to the House on Saturday. They took up the bill, they had a spirited debate, my name was invoked several times, not in a favorable light in some cases. (laughs) And they took a vote and it passed 226 to 182, I think. So it's law. The president signed it on Sunday and here we are.

Q: That's far from unanimous. There's obviously going to be more debate on this.

A: There are a couple of issues to just be sensitive to. There's a claim of reverse targeting. Now what that means is we would target somebody in a foreign country who is calling into the United States and our intent is to not go after the bad guy, but to listen to somebody in the United States. That's not legal, it's, it would be a breach of the Fourth Amendment. You can go to jail for that sort of thing. And if a foreign bad guy is calling into the United States, if there's a need to have a warrant, for the person in the United States, you just get a warrant. And so if a terrorist calls in and it's another terrorist, I think the American public would want us to do surveillance of that U.S. person in this case. So we would just get a warrant and do that. It's a manageable thing. On the U.S. persons side it's 100 or less. And then the foreign side, it's in the thousands. Now there's a sense that we're doing massive data mining. In fact, what we're doing is surgical. A telephone number is surgical. So, if you know what number, you can select it out. So that's, we've got a lot of territory to make up with people believing that we're doing things we're not doing.

Q: Even if it's perception, how do you deal with that? You have to do public relations, I assume.

A: Well, one of the things you do is you talk to reporters. And you give them the facts the best you can. Now part of this is a classified world. The fact we're doing it this way means that some Americans are going to die, because we do this mission unknown to the bad guys because they're using a process that we can exploit and the more we talk about it, the more they will go with an alternative means and when they go to an alternative means, remember what I said, a significant portion of what we do, this is not just threats against the United States, this is war in Afghanistan and Iraq.

Q: So you're saying that the reporting and the debate in Congress means that some Americans are going to die?

A: That's what I mean. Because we have made it so public. We used to do these things very differently, but for whatever reason, you know, it's a democratic process and sunshine's a good thing. We need to have the debate. The reason that the FISA law was passed in 1978 was an arrangement was worked out between the Congress and the administration, we did not want to allow this community to conduct surveillance, electronic surveillance, of Americans for foreign intelligence unless you had a warrant, so that was required. So there was no warrant required for a foreign target in a foreign land. And so we are trying to get back to what was the intention of '78. Now because of the claim, counterclaim, mistrust, suspicion, the only way you could make any progress was to have this debate in an open way.

Q: So you don't think there was an alternative way to do this?

A: There may have been an alternative way, but we are where are ...

Q: A better way, I should say.

A: All of my briefs initially were very classified. But it became apparent that we were not going

to be able to carry the day if we don't talk to more people.

Q: Some might say that's the price you pay for living in a free society. Do you think that this is necessary that these Americans die?

A: We could have gotten there a different way. We conducted intelligence since World War II and we've maintained a sensitivity as far as sources and methods. It's basically a sources and methods argument. If you don't protect sources and methods then those you target will choose alternative means, different paths. As it is today al-Qaida in Iraq is targeting Americans, specifically the coalition. There are activities supported by other nations to import electronic, or explosively formed projectiles, to do these roadside attacks and what we know about that is often out of very sensitive sources and methods. So the more public it is, then they take it away from us. So that's the tradeoff.

#### DIVERSITY IN THE INTELLIGENCE COMMUNITY

Q: I wanted to ask you about the diversity question. This has major ramifications here, we have this center of excellence program that's recruiting high school kids, many of whom wouldn't qualify if first generation American citizens weren't allowed.

A: So you agree with me?

Q: It does sound like something that would benefit this area that would also allow you to get people from here who are bicultural and have an openness to seeing things ...

A: You're talking about Hispanics?

Q: Yes.

A: Hispanics are probably the most under-represented group if you think of America, what the ethnic makeup of America, Hispanics are the most under-represented group in my community. Now, that said, and should increase that Hispanic population and programs like this will do that. That's why the outreach. But also we need, particularly with the current problem of terrorism, we need to have speakers of Urdu and Farsi and Arabic and people from those cultures that understand the issues of tribes and clans and all the things that go with understanding that part of the world. Varying religions and so on. Because it is, it's almost impossible, I've had the chance to live in the Middle East for years, I've studied it for years, it's impossible to understand it without having some feel for the culture and so on. So while I'm all for increasing the diversity along the lines we talked about, I'm also very much in favor of first generation Americans from the countries that are causing issues and problems.

Q: What is the status of that program.

A: It is not in statue. It is not in policy. It has been habit. So we've stated, as a matter of policy, that we're not going to abide by those habits.

Q: And that's already the case?

A: Yes, and are we making progress? Not fast enough, but we will make progress over time.

Q: How do you measure that?

A: Very simple, you get to measure what are you and where are you trying go and are you making progress. I wrestled with this years ago when I was NSA ...

Q: You don't want quotas, though?

A: Quotas are forbidden so we set goals. My way of thinking about it is what is your end state? Now some would say that federal governments should look like America, whatever that is. OK, that sounded like a reasonable metric, so I said, 'Alright, what does America look like?' So I got a bunch of numbers. I said, 'Alright, what do we look like?' and it didn't match, and as I just told you, the one place where there's the greatest mismatch is Hispanic. It's much closer, as matter of fact, people would be surprised how close it is across, at least my community among the other minorities. Now, that said, numbers don't necessarily equal positioning in the organization. So that's another feature we have to work on, is placement of women and minorities in leadership positions.

Q: So, you're quantifying that as well?

A: Yes.

#### TERRORIST ACTIVITY ON THE NATION'S SOUTHWEST BORDER

Q: There seems to be very little terrorist-related activity on the Southwest border, which is watched very closely because of the illegal immigration issue. Can you talk about why it's important to be alert here?

A: Let me go back to my NIE, those are unclassified key judgements, pull them down and look at them. You've got committed leadership. You've got a place to train. They've got trainers and they've got recruits. The key now is getting recruits in. So if the key is getting recruits in. So, if you're key is getting recruits in, how would you do that? And so, how would you do that?

Q: I'd go to the northern border where there's nobody watching.

A: And that's a path. Flying in is a path. Taking a ship in is a path. Coming up through the Mexican border is a path. Now are they doing it in great numbers, no. Because we're finding them and we're identifying them and we've got watch lists and we're keeping them at bay. There are numerous situations where people are alive today because we caught them (terrorists). And my point earlier, we catch them or we prevent them because we've got the sources and methods that lets us identify them and do something about it. And you know the more sources and methods are compromised, we have that problem.

Q: And in many cases we don't hear about them?

A: The vast majority you don't hear about. Remember, let me give you a way to think about this. If you've got an issue, you have three potential outcomes, only three. A diplomatic success, an operational success or an intelligence failure. Because all those diplomatic successes and operations successes where there's intelligence contribution, it's not an intelligence success. It's just part of the process. But if there's an intelligence failure ...

Q: Then you hear about it.

A: So, are terrorists coming across the Southwest border? Not in great numbers.

Q: There are some cases?

A: There are some. And would they use it as a path, given it was available to them? In time they will.

Q: If they're successful at it, then they'll probably repeat it.

A: Sure. There were a significant number of Iraqis who came across last year. Smuggled across illegally.

Q: Where was that?

A: Across the Southwest border.

Q: Can you give me anymore detail?

A: I probably could if I had my notebook. It's significant numbers. I'll have somebody get it for you. I don't remember what it is. The point is it went from a number to (triple) in a single year, because they figured it out. Now some we caught, some we didn't. The ones that get in, what are they going to do? They're going to write home. So, it's not rocket science, word will move around. There's a program now in South America, where you can, once you're in South American countries, you can move around in South America and Central America without a visa. So you get a forged passport in Lebanon or where ever that gets you to South America. Now, no visa, you can move around, and with you're forged passport, as a citizen of whatever, you could come across that border. So, what I'm highlighting is that something ...

Q: Is this how it happened, the cases you're talking about?

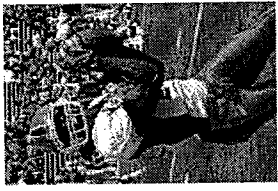
A: Yes.

Print Email Return to Top

### Miners Mania

Miners will 'get back to work' after loss to Rice

In the wake of UTEP's debacle at Rice, there really was only one question left to ponder. Full story



### Entertainment

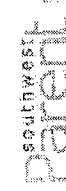
Show seeks best gospel singers

NEW YORK -- Move over, "American Idol": BET has gone talent-hunting for its next superstar in the place often considered to be the birthplace of the most-powerful singing in the world -- the church. Full story



<p><b>Refinance and Save \$1,000s</b> \$150,000 Mortgage for \$483/month. Compare up to 4 free www.pickamortgage.com</p>	<p><b>Refinance \$300,000 for Only \$965/Month</b> \$300,000 Mortgage for only \$965/month. Save \$1,000's - No www.HomeLoanHelpline.com</p>	<p><b>House Payments Fall Again</b> See Rates, No Credit Check Req. Calculate Your New Mortgage www.LowerMyBills.com</p>
--	--	--

Copyright © 20072007 by the El Paso Times and MediaNews Group and/or wire services and suppliers. None of the content on this site may be republished or reused in any way without the written permission of the copyright holder.



News Partners: Alamogordo Daily News Á Carlsbad Current-Argus Á The Deming Headlight Á Farmington Daily Times Á Las Cruces Sun-News Á Ruidoso News Á Silver City Sun-News

El Paso Times Site Map

Privacy Policy | MNG Corporate Site Map | Copyright  
Weather data Copyright 2007 CustomWeather, Inc.

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

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE:  
NATIONAL SECURITY AGENCY  
TELECOMMUNICATIONS RECORDS  
LITIGATION

MDL Docket No 06-1791 VRW

ORDER

This Document Relates To:  
07-1187, 07-1242, 07-1323,  
07-1324, 07-1326, 07-1396

The government seeks to enjoin state officials in Missouri, Maine, New Jersey, Connecticut and Vermont from investigating various telecommunication carriers concerning their alleged disclosure of customer telephone records to the National Security Agency (NSA) based on the Supremacy Clause of the United States Constitution, the foreign affairs power of the federal government and the state secrets privilege.

Before these cases were transferred to this court by the Judicial Panel on Multidistrict Litigation (JPML) on February 15, 2007, the government and various defendants filed cross motions for dismissal and summary judgment. With the exception of reply briefs in the Connecticut and Vermont cases, these motions were fully briefed prior to transfer. The court's scheduling order directed the parties to complete briefing in the Connecticut and Vermont cases and permitted the government and state officials to submit consolidated briefs addressing Ninth Circuit law and other issues not previously briefed. Doc #219.

United States District Court  
For the Northern District of California



1           Clayton v AT&T, 07-1187, arises out of investigative  
2 subpoenas issued to AT&T by two commissioners of the Missouri  
3 Public Service Commission (MoPSC) regarding information it  
4 allegedly disclosed to the NSA. Doc #1, Ex A. These subpoenas  
5 seek, for example,

- 6           (1) Any order, subpoena or directive of any court,  
7           tribunal or administrative agency or office  
8           whatsoever, directing or demanding the release of  
9           customer proprietary information relating to  
10           Missouri customers;
- 11           (2) The number of Missouri customers, if any, whose  
12           calling records have been delivered or otherwise  
13           disclosed to the [NSA]; and
- 14           (3) The nature or type of information disclosed to the  
15           NSA, including telephone number, subscriber name  
16           and address, social security numbers, calling  
17           patterns, calling history, billing information,  
18           credit card information, internet data and the  
19           like.

20           Doc #299, Ex A, tab 3.

21           Because the commissioners considered AT&T's response to  
22           be inadequate, they moved pursuant to Missouri law to compel AT&T  
23           to comply with the investigation in Missouri state court. AT&T  
24           then removed the case to the United States District Court for the  
25           Western District of Missouri. Shortly thereafter, the government  
26           initiated a separate Missouri action, United States v Gaw, 07-1242,  
27           on July 26, 2006, seeking declaratory and injunctive relief against  
28           the MoPSC and AT&T.

          The Maine case, United States v Adams, 07-1323, began  
after Maine citizens petitioned the Maine Public Utilities  
Commission (MePUC) to investigate whether Verizon had shared its  
customers' records with the NSA. Verizon submitted two press  
releases in response on May 12 and May 16, 2006, stating that (1)



1 the NSA never requested customer records and (2) if a government  
2 agency requested its customer records, Verizon would disclose them  
3 only when authorized by law. Doc #1, ¶ 40. On August 9, 2006,  
4 MePUC ordered Verizon to affirm under oath that its press releases  
5 were accurate. Id, ¶¶ 41-42; Doc #299, Ex A, tab 5. MePUC has not  
6 asked for any additional information from Verizon. See Doc #299,  
7 Ex A, tab 5. On August 21, 2006, the government sued in the United  
8 States District Court for the District of Maine to enjoin the MePUC  
9 from pursuing this inquiry. On February 8, 2007, Judge Woodcock  
10 preliminarily enjoined MePUC from enforcing the order. See United  
11 States v Adams, 473 F Supp 2d 108 (D Me 2007).

12 The New Jersey case, United States v Rabner, 07-1324,  
13 stems from the New Jersey Attorney General's investigation into  
14 whether telecommunication carriers disclosed to the NSA telephone  
15 call history data of New Jersey subscribers. Doc #1, ¶34. The New  
16 Jersey Attorney General issued *subpoenas duces tecum* pursuant to  
17 New Jersey consumer protection law to ten carriers doing business  
18 in New Jersey. These subpoenas include the following requests:

- 19 (1) All orders, subpoenas and warrants issued by or on  
20 behalf of any unit or officer of the Executive  
21 Branch of the Federal Government and provided to  
22 [the carriers] concerning any demand or request to  
23 provide telephone call history data to the NSA;
- 24 (2) All documents concerning an identification of  
25 customers \* \* \* whose telephone call history data  
26 was provided \* \* \* to the NSA; of the persons whose  
27 data was provided to the NSA; and
- 28 (3) All documents concerning any communication between  
[the carriers] and the NSA \* \* \* concerning the  
provision of telephone call history data to the  
NSA.

27 Doc #299, Ex A, tab 1. In response to these subpoenas, the  
28 government sued the New Jersey Attorney General in the United

1 States District Court for the District of New Jersey. Doc #1-1.  
2 United States v Palermino, 07-1324, arises from a  
3 complaint filed by the American Civil Liberties Union of  
4 Connecticut (ACLU) requesting that the Connecticut Department of  
5 Public Utility Control (CtDPUC) investigate whether the local  
6 carriers violated Connecticut law. In response, the CtDPUC  
7 initiated an administrative proceeding and pursued the requested  
8 investigation. After the CtDPUC denied the carriers' motions to  
9 dismiss, ACLU filed its first set of interrogatories to each of the  
10 carriers, seeking information concerning potential illegal  
11 disclosure of customer records, such as the following:

- 12 (1) Did AT&T have any published privacy policy or  
13 policies concerning customer information and/or  
14 records in effect between September 11, 2001, and  
15 August 10, 2006?
- 16 (2) To the extent that any published privacy policy  
17 referenced in your response [above] changed during  
18 the relevant period, explain the specific terms  
19 that changed, when the changes occurred, and the  
20 reasons for the change.
- 21 (3) Without providing any details about the purpose(s)  
22 or target(s) of any investigation(s) or  
23 operations(s), at any time during the relevant  
24 period has AT&T ever received [a court order or a  
25 request under 18 USC § 2709, I e, a "national  
26 security letter"] seeking disclosure of customer  
27 information and/or records?

22 Doc #299, Ex A, tab 4. On September 6, 2006, the government sued  
23 in the United States District Court for the District of  
24 Connecticut.

25 In United States v Volz, 07-1396, the commissioner of the  
26 Vermont Department of Public Service (VtDPS) propounded information  
27 requests under Vermont law, 30 VSA § 206, to AT&T and Verizon  
28 concerning their conduct and policies vis-à-vis the NSA. 07-1396,

1 Doc #1, Ex C. After AT&T and Verizon failed to comply with the  
2 request, VtDPS petitioned the Vermont Public Service Board (VtPSB)  
3 to open investigations of the carriers, Id, ¶¶ 33-34, and  
4 eventually ordered the carriers to respond. Id, ¶ 37 & Ex I. This  
5 prompted the government to bring suit to enjoin VtPSB in the  
6 District Court of Vermont.

7 The parties' cross motions for summary judgment concern  
8 three issues: whether the state officials' investigations (1)  
9 violate the Supremacy Clause by regulating directly or  
10 discriminating against the federal government or conflicting with  
11 an affirmative command of Congress; (2) impinge on the foreign  
12 affairs power of the federal government; or (3) run afoul of the  
13 state secrets privilege.

14 In reviewing a summary judgment motion, the court must  
15 determine whether genuine issues of material fact exist, resolving  
16 any doubt in favor of the party opposing the motion. "[S]ummary  
17 judgment will not lie if the dispute about a material fact is  
18 'genuine,' that is, if the evidence is such that a reasonable jury  
19 could return a verdict for the nonmoving party." Anderson v  
20 Liberty Lobby, Inc, 477 US 242, 248 (1986). "Only disputes over  
21 facts that might affect the outcome of the suit under the governing  
22 law will properly preclude the entry of summary judgment." Id.  
23 And the burden of establishing the absence of a genuine issue of  
24 material fact lies with the moving party. Celotex Corp v Catrett,  
25 477 US 317, 322-23 (1986). When the moving party has the burden of  
26 proof on an issue, the party's showing must be sufficient for the  
27 court to hold that no reasonable trier of fact could find other  
28 than for the moving party. Calderone v United States, 799 F2d 254,

1 258-59 (6th Cir 1986). Summary judgment is granted only if the  
2 moving party is entitled to judgment as a matter of law. FRCP 56©.  
3 The nonmoving party may not simply rely on the pleadings,  
4 however, but must produce significant probative evidence supporting  
5 its claim that a genuine issue of material fact exists. TW Elec  
6 Serv v Pacific Electrical Contractors Ass'n, 809 F2d 626, 630 (9th  
7 Cir 1987). The evidence presented by the nonmoving party "is to be  
8 believed, and all justifiable inferences are to be drawn in his  
9 favor." Anderson, 477 US at 255. "[T]he judge's function is not  
10 himself to weigh the evidence and determine the truth of the matter  
11 but to determine whether there is a genuine issue for trial." Id  
12 at 249.

13  
14 II

15 The court takes up jurisdictional issues first.  
16 In these suits, the government seeks both declaratory and  
17 injunctive relief, including: (1) a declaration that state  
18 investigations are invalid under and preempted by the Supremacy  
19 Clause; and (2) an order enjoining the state officials from  
20 investigating the carriers relating to their alleged disclosure of  
21 records to the NSA. These pleadings suffice to confer federal  
22 question jurisdiction under 28 USC §§ 1331 and 1345.

23 It is well-established that the federal courts have  
24 jurisdiction under 28 USC § 1331 over a preemption claim seeking  
25 injunctive and declaratory relief. See, e g, Verizon Md, Inc v Pub  
26 Serv Comm'n of Md, 535 US 635, 641-43 (2002). In Shaw v Delta Air  
27 Lines, Inc, 463 US 85, 96 & n14 (1983), the Supreme Court held:

28 //

1 A plaintiff who seeks injunctive relief from state  
2 regulation, on the ground that such regulation is  
3 preempted by a federal statute which, by virtue of  
4 the Supremacy Clause of the Constitution, must  
prevail, thus presents a federal question which the  
federal courts have jurisdiction under 28 USC §  
1331 to resolve.

5 See also Bud Antle, Inc v Barbosa, 45 F3d 1261, 1362 (9th Cir 1994)  
6 ("Even in the absence of an explicit statutory provision  
7 establishing a cause of action, a private party may ordinarily seek  
8 declaratory and injunctive relief against state action on the basis  
9 of federal preemption."); United States v Morros, 268 F3d 695, 702-  
10 03 (9th Cir 2001), citing Bell v Hood, 327 US 678, 681-82 (1946)  
11 (conferring federal question jurisdiction for claims by government  
12 that seek relief "directly under the Constitution or laws of the  
13 United States" in challenging the actions of state officials under  
14 the Supremacy Clause); Richard H Fallon, et al, Hart and Wechler's  
15 The Federal Courts and the Federal System 903 (5th ed 2003).

16 An alternative ground for federal question jurisdiction  
17 is furnished by 28 USC § 1345, which "provides the district courts  
18 with original jurisdiction of all civil actions commenced by the  
19 United States," thereby creating "independent subject matter  
20 jurisdiction." Morros, 268 F3d at 702-03. Accordingly, the court  
21 finds that jurisdiction lies in federal court under 28 USC §§ 1331  
22 and 1345.

23 A second hurdle to reaching the merits in these cases is  
24 that the government lacks an express cause of action. The  
25 government describes three means of remedying this omission, one of  
26 which the court can easily dispense with. The government errs in  
27 arguing that the existence of jurisdiction itself gives rise to a  
28 cause of action. It is firmly established by the Supreme Court

1 that the vesting of jurisdiction does not in and of itself give  
2 rise to a cause of action. Texas Industries, Inc v Radcliff  
3 Materials, Inc, 451 US 630, 640-41 (1981). Nor do the statutes  
4 relied on for jurisdiction create substantive causes of action.  
5 Hence, to secure a cause of action for these suits, the government  
6 must look elsewhere.

7 One option for establishing a cause of action lies with  
8 an obscure line of cases culminating in In re Debs, 158 US 564  
9 (1895), which permit the government to sue to vindicate its  
10 sovereign interests even when not authorized by statute. See also  
11 Dugan v United States, 16 US 172 (1818); United States v Tingey, 30  
12 US 115 (1831); Cotton v United States, 52 US 229 (1851); Jessup v  
13 United States, 106 US 147 (1882). Debs involved an attempt by the  
14 federal government to enjoin the Pullman labor strike of 1894. 158  
15 US at 577. The Court upheld the propriety of the injunction,  
16 proclaiming that

17 [e]very government, entrusted, by the very terms of  
18 its being, with powers and duties to be exercised  
19 and discharged for the general welfare, has a right  
20 to apply to its own courts for any proper assistance  
in the exercise of the one and the discharge of the  
other \* \* \*.

21 In spite of the Court's high-flying rhetoric, the Debs doctrine has  
22 seldom been invoked in the century-plus since its inception.  
23 "[R]elatively little has been made of this broad authorization to  
24 sue because in most instances, the federal government has sued  
25 pursuant to federal statutes and not based on its inherent interest  
26 in protecting its citizens." Erwin Chemerinsky, Federal  
27 Jurisdiction, § 2.3 (Aspen 2003).

28 //

1           The contours of the doctrine enunciated in Debs remain  
2 unclear, not least due to the vague guidance offered by the Debs  
3 Court.

4           [It is not the province of the government to  
5 interfere in any mere matter of private controversy  
6 between individuals, or to use its great powers to  
7 enforce the rights of one against another, yet,  
8 whenever the wrongs complained of are such as affect  
9 the public at large, and are in respect of matters  
10 which by the Constitution are entrusted to the care  
11 of the Nation, and concerning which the Nation owes  
12 the duty to all the citizens of securing to them  
13 their common rights, then the mere fact that the  
14 government has no pecuniary interest in the  
15 controversy is not sufficient to exclude it from the  
16 courts, or prevent it from taking measures therein  
17 to fully discharge those constitutional duties.

18 Debs, 158 US at 586.

19           Under its most expansive reading, Debs authorizes the  
20 government to sue without statutory authorization whenever the  
21 alleged violations "affect the public at large." 158 US at 586.  
22 Such a broad mandate has led the government to invoke Debs in  
23 varied circumstances, including in suits to enforce immunity of the  
24 armed forces from certain state taxes, see United States v  
25 Arlington County, 326 F2d 929 (4th Cir 1964), to enforce civil  
26 rights under the Commerce Clause, see United States v Jackson, 318  
27 F2d 1 (5th Cir 1963), and to enjoin sellers from obtaining default  
28 judgments without proper service of process, see United States v  
Brand Jewelers, Inc, 318 F Supp 1293 (SDNY 1970). Most relevant  
here, the government has succeeded in invoking this doctrine in  
disputes over interference with national security. United States v  
Marchetti, 466 F2d 1309 (4th Cir 1972) (protection of contractual  
rights in addition to national security interest). See also United  
States v Mattson, 600 F2d 1295, 1298 (9th Cir 1979) ("Where

1 interference with national security has been at issue, courts have  
2 also relied on the doctrine to reach the merits of the  
3 controversy.")

4 The state officials draw the court's attention to Justice  
5 Black's concurring opinion in New York Times Co v United States,  
6 403 US 713, 718 (1971), which gives reason for restraint in  
7 applying Debs. Justice Black cautioned that invocation of Debs  
8 invites the government - that is, the executive branch - to exceed  
9 its constitutional grant to ensure that the laws are faithfully  
10 executed.

11 It would, however, be utterly inconsistent with the  
12 concept of separation of powers for this Court to  
13 use its power of contempt to prevent behavior that  
14 Congress has specifically declined to prohibit. \* \*  
15 \* The Constitution provides that Congress shall make  
16 laws, the President execute laws, and courts  
17 interpret laws. It did not provide for government  
18 by injunction in which the courts and the Executive  
19 branch can 'make laws' without regard to the action  
20 of Congress. It may be more convenient for the  
21 Executive Branch if it need only convince a judge to  
22 prohibit conduct rather than ask the Congress to  
23 pass a law, and it may be more convenient to enforce  
24 a contempt order than to seek a criminal conviction  
25 in a jury trial. Moreover, it may be considered  
26 politically wise to get a court to share the  
27 responsibility for arresting those who the Executive  
28 Branch has probable cause to believe are violating  
the law. But convenience and political  
considerations of the moment do not justify a basic  
departure from the principles of our system of  
government.

403 US 713, 718 (1971) (citations omitted).

In view of these separation of powers concerns, the court  
agrees with the state officials that mere incantation of "sovereign  
interests" does not suffice under Debs to generate a cause of  
action. But even a narrow construction of Debs cannot prevent the  
doctrine's application here. Although the state officials insist



1 on casting these investigations as garden variety  
2 telecommunications regulation, it cannot be gainsaid that the  
3 officials' efforts bear particularly on the government's national  
4 security interests. Whatever the boundaries of the Debs, the court  
5 is confident that these suits fall well within its borders. See  
6 Mattson, 600 F2d at 1298 ("Where interference with national  
7 security has been at issue, courts have also relied on the doctrine  
8 to reach the merits of the controversy."). Debs is thus properly  
9 invoked by the government in these cases.

10 As an alternative to relying on Debs, the government  
11 asserts that the Supremacy Clause of the Constitution creates an  
12 implied right of action to enjoin state regulations that are  
13 preempted by a federal statutory or constitutional provision. The  
14 Supreme Court implicitly supported such a right in Pharmaceutical  
15 Research and Manufacturers of America v Walsh, 538 US 644 (2003).  
16 Plaintiffs in that case argued - without a cause of action - that a  
17 state regulation was preempted by Medicaid, a federal Spending  
18 Clause statute. Only two Justices declined to reach the merits of  
19 plaintiff's claim for reason that no claim was stated. The  
20 remaining Justices - a plurality of four and three in dissent -  
21 proceeded to the merits without pause, tacitly deciding that an  
22 implied claim was stated for preemption.

23 The DC Circuit relied on Walsh in rejecting a state  
24 agency's contention that plaintiffs "have no private right of  
25 action for injunctive relief against the state" based on the  
26 preemptive force of a federal statute. Pharmaceutical Research and  
27 Manufacturers of America v Thompson, 362 F3d 819 (DC Cir 2004).  
28 "By addressing the merits of the parties' arguments without mention

1 of any jurisdictional flaw," the court explained, "seven Justices  
2 appear to have *sub silentio* found no flaw." 362 F3d at 819 n3. See  
3 also Planned Parenthood v Sanchez, 403 F3d 324 (5th Cir 2005).

4 The court concurs with the DC Circuit's reasoning. By  
5 entertaining federal preemption suits, see e g, Walsh, 538 US 644,  
6 Verizon Maryland, Inc, 535 US 635 (2002), the Supreme Court has  
7 cleared the path for parties to seek declaratory and injunctive  
8 relief against state action on the basis of federal preemption  
9 alone. This implied cause of action, in conjunction with the  
10 proper invocation of Debs, provides two grounds for the government  
11 to proceed in these cases.

12 Even if the government has jurisdiction and a cause of  
13 action, several state officials urge this court to abstain from  
14 exercising jurisdiction over these suits pursuant to the Younger v  
15 Harris, 401 US 37 27 (1971), line of cases, which hold that  
16 principles of comity and federalism require federal courts to  
17 abstain from enjoining pending state proceedings. See also Ohio  
18 Civil Rights Comm'n v Dayton Christian Schools, Inc, 477 US 619,  
19 627 (1986) (extending the Younger doctrine to certain state  
20 administrative proceedings, so long as those proceedings are  
21 "judicial in nature").

22 In the Ninth Circuit, however, the federal government  
23 may bypass the Younger hurdle when it acts as a litigant. See  
24 United States v Morros, 268 F3d 695 (9th Cir 2001). According to  
25 the Morros court, if the federal government seeks relief against a  
26 state or its officers, it makes little sense to hew to the  
27 principles of comity and federalism that animate Younger because  
28 "the state and federal governments are in direct conflict before

1 they arrive at the federal courthouse," rendering futile "any  
2 attempt to avoid a federal-state conflict." Id (citing United  
3 States v Composite State Bd of Medical Examiners, 656 F2d 131, 136  
4 (5th Cir 1981). The Ninth Circuit's reasoning in Morros  
5 undoubtedly applies here. The possibility of avoiding "unnecessary  
6 conflict between state and federal governments," Composite State,  
7 656 F2d at 136, faded long before these cases arrived to this  
8 court. Because such a conflict inheres in these cases, Younger  
9 abstention is inapplicable.

10 The court finally turns to the argument advanced in three  
11 of these cases that no case or controversy exists because the state  
12 officials have not attempted to enforce its statutes and  
13 regulations against the carriers. Ripeness is one of the four  
14 justiciability doctrines that stem from the Article III limitation  
15 of the federal judicial power to cases or controversies.  
16 Accordingly, "whether a claim is ripe for adjudication goes to a  
17 court's subject matter jurisdiction \* \* \*." St Clair v City of  
18 Chico, 880 F2d 199, 201 (9th Cir 1989), quoted in Schwarzer et al,  
19 Federal Civil Procedure Before Trial § 2:178 (1997). The standard  
20 to be applied in determining if there is a case or controversy ripe  
21 for resolution is whether there is "a reasonable threat of  
22 prosecution for conduct allegedly protected by the Constitution."  
23 Ohio Civil Rights Comm'n v Dayton Christian Schools, 477 US 619,  
24 626 n1 (1986).

25 Because the state officials have made plain their  
26 intention to subject the carriers to investigation, the court  
27 agrees with the government that the carriers face a reasonable  
28 threat of prosecution and thus there is before the court a ripe

United States District Court  
For the Northern District of California

1 case or controversy. Cf Public Utilities Comm'n v United States,  
2 355 US 534, 538 (1958) (allowing preenforcement review of a state  
3 regulation that required common carriers to receive state  
4 pre-approval before offering reduced shipping rates to the United  
5 States where the state had "plainly indicated an intent to enforce  
6 the Act"); see also Mobil Oil Corp v Virginia, 940 F2d 73, 76 (4th  
7 Cir 1991) (allowing preenforcement review of amendments to the  
8 Virginia Petroleum Products Franchise Act, which an oil company  
9 claimed were preempted, even though Virginia had not specifically  
10 indicated that it intended to enforce that statute against  
11 plaintiffs, because the Virginia "Attorney General [had] not \* \* \*  
12 disclaimed any intention of exercising her enforcement authority").  
13

14 III

15 Turning to the merits, these cases concern whether the  
16 state laws underlying the investigations run afoul of the Supremacy  
17 Clause, the federal foreign affairs power or state secrets  
18 privilege. State law may violate the Supremacy Clause in two ways:  
19 the law may regulate directly or discriminate against the  
20 government, see McCulloch v Maryland, 4 Wheat 316, 425-437 (1819),  
21 or the law may conflict with an affirmative command of Congress,  
22 see Gibbons v Ogden, 9 Wheat 1, 211 (1824); see also Hillsborough  
23 County v Automated Medical Laboratories, Inc, 471 US 707, 712-713  
24 (1985). The government's attack on the investigations relies on  
25 both grounds of invalidity.

26 //  
27 //  
28 //

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

A

It is a fundamental principle of our law "that the constitution and the laws made in pursuance thereof are supreme; that they control the constitution and laws of the respective States, and cannot be controlled by them." McCulloch v Maryland, 4 Wheat 316, 426 (1819). From this principle is derived the corollary that "the activities of the Federal Government are free from regulation by any state." Hancock v Train, 426 US 167, 178 (1976). As Justice Holmes observed in Johnson v Maryland, 254 US 51, 57 (1920):

[T]he immunity of the instruments of the United States from state control in the performance of their duties extends to a requirement that they desist from performance until they satisfy a state officer upon examination that they are competent for a necessary part of them.

The doctrine that embodies these principles - termed intergovernmental immunity - prevents state laws from regulating directly or discriminating against the federal government.

The Supreme Court's modern-day treatment of the intergovernmental immunity doctrine has been marked by restraint, making plain the doctrine has no application here. Although the pertinent state disclosure orders, Doc #299, Ex A, relate to federal government activities, they do not regulate the government directly; indeed, they impose no duty on the government. See United States v New Mexico, 455 US 720 (1982). The Court upheld analogous regulations in North Dakota v United States, 495 US 423, 437 (1990), which involved laws requiring out-of-state shippers of alcohol to file monthly reports and to affix a label to each bottle of liquor sold to federal military enclaves. Id at 426. The Court

1 reasoned that because the laws operated on suppliers, not the  
2 government, "[t]here is no claim \* \* \*, nor could there be, that  
3 North Dakota regulates the Federal Government directly." *Id* at  
4 436-37. That conclusion leaves no doubt that the state  
5 investigations operate on the carriers alone.

6 Nor can it be said that the investigations "discriminate  
7 against the federal government or those with whom it deals." North  
8 Dakota v United States, 495 US 423, 437 (1990). The  
9 nondiscrimination rule prevents states from meddling with federal  
10 government activities indirectly by singling out for regulation  
11 those who deal with the government. This rule does not, however,  
12 oblige special treatment. A "[s]tate does not discriminate against  
13 the Federal Government and those with whom it deals unless it  
14 treats someone else better than it treats them." Washington v  
15 United States, 460 US 536, 544-45 n10 (1983). Applying these  
16 principles, the Court has required that regulations be imposed  
17 equally on all similarly situated constituents of a state and not  
18 based on a constituent's status as a government contractor or  
19 supplier. See United States v County of Fresno, 429 US 452,  
20 462-464 (1977).

21 The nondiscrimination analysis should not "look to the  
22 most narrow provision addressing the Government or those with whom  
23 it deals. A state provision that appears to treat the Government  
24 differently on the most specific level of analysis may, in its  
25 broader regulatory context, not be discriminatory." North Dakota,  
26 495 US at 438. The asserted laws at issue here regulate equally  
27 all public utilities, making no distinction based on the  
28 government's involvement. Although the present investigation, in

United States District Court  
For the Northern District of California

1 targeting alleged disclosure of call records to the NSA, may  
2 "appear[] to treat the government differently," the regulatory  
3 regime as whole treats any unauthorized disclosure the same. These  
4 neutral state laws regulating the carriers "are but normal  
5 incidents of the organization within the same territory of two  
6 governments." North Dakota, 495 US at 435, citing Helvering v  
7 Gerhardt, 304 US 405, 422 (1938).

8           The government presents an impressive patchwork of dicta  
9 in support of its theory, but none of the cases it cites pertains  
10 to the present facts. Hancock v Train, 426 US 167, 174 (1976), for  
11 example, concerns a state attorney general's efforts to require the  
12 United States Army, the Tennessee Valley Authority and the Atomic  
13 Energy Commission to obtain state air pollution permits for  
14 facilities on federal installations. The Hancock Court found  
15 decisive the fact that the regulations "place[d] a prohibition on  
16 the federal government" - a feature absent here. Both Mayo v  
17 United States, 319 US 441, 447 (1943), and City of Los Angeles v  
18 United States, 355 F Supp 461, 464 (CF Cal 1972), prove equally  
19 unavailing for the government. In both cases, plaintiffs sought to  
20 exact fees directly from a government entity. Again, no equivalent  
21 interplay between the public utilities and the federal government  
22 exists here.

23           In sum, because the investigations neither regulate  
24 directly nor discriminate against the federal government, the  
25 investigations do not violate the doctrine of intergovernmental  
26 immunity.

27 //

28 //

B

The court turns to the government's preemption argument. By virtue of the Supremacy Clause, it is a "fundamental principle of the Constitution \* \* \* that Congress has the power to preempt state law." Crosby v Nat'l Foreign Trade Council, 530 US 363, 372 (2000) (citing US Const, Art VI, cl 2). The Supreme Court cautions, however, that "despite the variety of these opportunities for federal preeminence, we have never assumed lightly that Congress has derogated state regulation, but instead have addressed claims of preemption with the starting presumption that Congress does not intend to supplant state law." New York State Conference of Blue Cross & Blue Shield Plans v Travelers Insurance Co, 514 US 645, 654 (1995). Accordingly, "the purpose of Congress is the ultimate touchstone" of any preemption analysis. Cipollone v Liggett Group, 505 US 504, 516 (1992) (citation omitted).

State law must yield to federal law in three situations. First, state law may be preempted if Congress has expressly so provided. Gade v National Solid Wastes Mgm't Ass'n, 505 US 88 (1992). Second, under field preemption, "[i]f Congress evidences an intent to occupy a given field, any state law falling within that field is preempted." Silkwood v Kerr-McGee Corp, 464 US 238, 248 (1984) (citing Fidelity Federal Savings & Loan Ass'n v de la Cuesta, 458 US 141, 153 (1982)). Finally, under conflict preemption, "[i]f Congress has not entirely displaced state regulation over the matter in question, state law is still preempted to the extent it actually conflicts with federal law, that is, when it is impossible to comply with both state and federal law \* \* \* or where the state law stands as an obstacle to



1 the accomplishment of the full purposes and objectives of  
2 Congress." Id (citing Florida Lime & Avocado Growers, Inc v Paul,  
3 373 US 132, 142-43 (1963) and Hines v Davidowitz, 312 US 52, 67  
4 (1941)). The government contends that express, field and conflict  
5 preemption apply to the state investigations.

6  
7 1

8 State law is preempted insofar as Congress has expressly  
9 stated its intent to supersede state law. Shaw v Delta Air Lines,  
10 Inc, 463 US 85, 95-98 (1983). The task of statutory construction  
11 of an expressed preemption clause "must in the first instance focus  
12 on the plain wording of the clause, which necessarily contains the  
13 best evidence of Congress' preemptive intent." CSX Transportation,  
14 Inc v Easterwood, 507 US 658, 664 (1993). If Congress intends to  
15 alter the usual constitutional balance between the states and the  
16 federal government, it must make its intention to do so  
17 unmistakably clear in the language of the statute. Rice v Santa Fe  
18 Elevator Corp, 331 US 218, 230 (1947). The plain statement rule,  
19 as applied to expressed preemption, "is nothing more than an  
20 acknowledgment that the states retain substantial sovereign powers  
21 under our constitutional scheme, powers with which Congress does  
22 not readily interfere." Gregory v Ashcroft, 501 US 452, 461.

23 Little more than a paragraph in the briefing is devoted  
24 to the contention that federal law - namely, the Stored  
25 Communications Act ("SCA"), 18 USC § 2701 et seq - preempts  
26 expressly the state laws at issue here. The SCA, which was enacted  
27 as part of the Electronic Communications Privacy Act of 1986  
28 ("ECPA"), Pub L No 99-508, 100 Stat 1848 (1986), regulates

1 disclosure of non-content "record[s] or other information  
2 pertaining to a subscriber." 18 USC § 2702©. Relevant to the  
3 issue of preemption, the SCA specifies that "[t]he remedies and  
4 sanctions described in this chapter are the only judicial remedies  
5 and sanctions for nonconstitutional violations of this chapter."  
6 Id § 2708.

7 As the court concluded in its order denying remand in  
8 Riordan, 06-3574, and Campbell, 06-3596, section 2708 of the SCA  
9 serves a limited purpose: to prevent criminal defendants from  
10 suppressing evidence based on electronic communications or customer  
11 records obtained in violation of ECPA's provisions. Doc #130 at 6.  
12 The government gives no reason to revisit this issue. Accordingly,  
13 the court concludes that federal law does not expressly preempt the  
14 states laws at issue here.

15  
16 2

17 Even if a federal statute does not expressly preempt  
18 state law, it may do so by implication. Field preemption is found  
19 if the federal so thoroughly regulates a legislative field that  
20 Congress intended it to be occupied exclusively by the federal  
21 government. Freightliner Corp v Myrick, 514 US 280, 287 (1995).  
22 If a "scheme of federal regulation \* \* \* [is] so pervasive as to  
23 make reasonable the inference that Congress left no room for the  
24 States to supplement it," or if an Act of Congress "touches a field  
25 in which the federal interest is so dominant that the federal  
26 system will be assumed to preclude enforcement of state laws on the  
27 same subject," field preemption exists. English v General Electric  
28 Co, 496 US 72, 79 (1990); Rice, 331 US at 230. Because Congress

21

1 left room for state regulation of public utilities and their  
2 consumers' privacy, field preemption fails.

3           As discussed in the court's remand order, see Doc #130 at  
4 7, the preemptive force of the Foreign Intelligence Surveillance  
5 Act ("FISA") is undercut by the statute's language that  
6 contemplates state court litigation concerning illegal  
7 surveillance. For example, section 1806(f), in pertinent part,  
8 provides procedures for consideration of the propriety of FISA  
9 orders "[w]herever \* \* \* any motion or request is made by an  
10 aggrieved person pursuant to any other statute or rule of \* \* \* any  
11 state before any court or other authority of \* \* \* any state to  
12 discover or obtain applications or orders of other materials  
13 relating to electronic surveillance \* \* \* ." 50 USC 1806(f). The  
14 statutory exemption in 1861(e) also implies the availability of  
15 civil claims with respect to the production of records. It  
16 provides that a "person who, in good faith, produces tangible  
17 things under an order pursuant to this section shall not be liable  
18 to any other person for such production." 50 USC 1861(e). FISA  
19 thus contemplates that, in the absence of a government order for  
20 the business records under 50 USC 1861(a)(1), injured parties will  
21 have causes of action and remedies under other provisions of state  
22 and federal law.

23           These provisions in FISA suggest that Congress did not  
24 intend to foreclose state involvement in the area of surveillance  
25 regulation. As such, it cannot be said that the scheme of federal  
26 regulation here is "so pervasive as to make reasonable the  
27 inference that Congress left no room for the States to supplement  
28 it." English, 496 US at 79.

1  
2 Finally, state action is preempted to the extent it  
3 actually conflicts with federal statutes, regulations or the  
4 Constitution. Barnett Bank of Marion County, NA v Nelson, 517 US  
5 25, 31 (1996). Conflict preemption is found if it is "impossible  
6 for a private party to comply with both state and federal  
7 requirements" or if state law "stands as an obstacle to the  
8 accomplishment and execution of the full purposes and objectives of  
9 Congress." Freightliner Corp v Myrick 514 US 280, 287 (1995);  
10 Geier v American Honda Motor Co, 529 US 861, 873 (2000).

11 In support of conflict preemption, the government relies  
12 chiefly on two statutory privileges, first citing to section 6 of  
13 the National Security Agency Act of 1959, 50 USC § 402 note 6,  
14 which provides:

15 [N]othing in this act or any other law \* \* \* shall be  
16 construed to require the disclosure of the organization  
17 or any function of the National Security Agency, of any  
18 information with respect to the activities thereof, or of  
the names, titles, salaries, or number of persons  
employed by such agency. 50 USC § 402, n6, sec 6(a)  
(emphasis added).

19 The government also relies on 50 USC § 403-1(i)(1), which states,  
20 "[t]he Director of National Intelligence shall protect intelligence  
21 sources and methods from unauthorized disclosure." The overarching  
22 issue is whether compliance with both federal and state regulations  
23 is a physical impossibility or whether the state investigations  
24 "stand[] as an obstacle to the accomplishment of the full purposes  
25 and objectives of Congress." Silkwood, 464 US at 248. For reasons  
26 discussed below, the court finds that neither of these provisions  
27 compels preemption.

28 //

United States District Court  
For the Northern District of California

1 Compliance with both federal and state regulations is not  
2 a physical impossibility, at least in view of "the circumstances of  
3 [the] particular case." Florida Lime & Avocado Growers, Inc v  
4 Paul, 373 US 132, 142-43 (1963). "What is a sufficient obstacle is  
5 a matter of judgment, to be informed by examining the federal  
6 statute as a whole and identifying its purpose and intended  
7 effects." Crosby v National Foreign Trade Council, 530 US 363, 373  
8 (2000)

9 For when the question is whether a Federal act  
10 overrides a state law, the entire scheme of the  
11 statute must of course be considered and that which  
12 needs must be implied is of no less force than that  
13 which is expressed. If the purpose of the act  
14 cannot otherwise be accomplished -- if its  
operation within its chosen field else must be  
frustrated and its provisions be refused their  
natural effect -- the state law must yield to the  
regulation of Congress within the sphere of its  
delegated power.

15 Crosby, 530 US at 373 (citing Savage v Jones, 225 US 501, 533  
16 (1912)).

17 Applying this standard, the court cannot conclude that  
18 the state investigations will inevitably conflict with federal law.  
19 In Hepting, 06-672, the government argued that the information  
20 covered by the section 6 statutory privilege is "at least co-  
21 extensive with the assertion of the state secrets privilege by the  
22 DNI." 06-672, Doc #124 at 14. Insofar as section 6 proscribes  
23 disclosure that would otherwise fall within the state secrets  
24 privilege, no conflict exists, as the government may intervene and  
25 assert the state secrets privilege in any of these proceedings. A  
26 conflict may arise, however, to the extent the state officials seek  
27 information covered by section 6 that lies outside the scope of the  
28 state secrets privilege. The court doubts whether any of the these

1 investigations would engender such a conflict, especially given the  
2 government's insistence that all information sought by the state  
3 officials implicates the state secrets privilege. Regardless, it  
4 would be inappropriate for the court to rule on the scope of this  
5 possible conflict in the abstract. See Time Warner Entm't Co, LP v  
6 FCC, 56 F3d 151, 195 (DC Cir 1995) ("[W]hether a state regulation  
7 unavoidably conflicts with national interests is an issue incapable  
8 of resolution in the abstract.").

9 Under the obstruction strand of conflict preemption,  
10 state law is preempted to the extent it actually interferes with  
11 the "methods by which the federal statute was designed to reach  
12 [its] goal." Int'l Paper Co v Ouellette, 479 US 481, 494 (1987);  
13 Verizon North, Inc v Strand, 309 F3d 935, 940 (6th Cir 2002). In  
14 making this determination, courts "consider the relationship  
15 between state and federal laws as they are interpreted and applied,  
16 not merely as they are written." Jones v Rath Packing Co, 430 US  
17 519, 526 (1977); Time Warner, 56 F3d at 195 ("[W]hether a state  
18 regulation unavoidably conflicts with national interests is an  
19 issue incapable of resolution in the abstract.") (quoting Alascom,  
20 Inc v FCC, 727 F2d 1212, 1220 (DC Cir 1984)). Hence, obstruction  
21 preemption focuses on both the objective of the federal law and the  
22 method chosen by Congress to effectuate that objective, taking into  
23 account the law's text, application, history and interpretation.

24 To support obstruction, the government avers that any  
25 litigation touching upon the statutory privileges must *ipso facto*  
26 obstruct Congress' purpose. But such a view misapprehends the  
27 federal law's purpose by ignoring the bulk of Congress's activity  
28 in this realm. For example, inquiry into activity not sanctioned

United States District Court  
For the Northern District of California

1 by the Pen Register Act, 18 USC § 3121, or FISA, falls outside of  
2 section 6's ambit. The Pen Register Act provides that "no person  
3 may install or use a pen register or a trap and trace device  
4 without first obtaining a court order under section 3123 of this  
5 title [18 USCS § 3123] or under the [FISA]." 18 USC § 3121(a).  
6 Similarly, FISA requires an application under oath attesting to  
7 eleven qualifying conditions, including the purpose of the  
8 investigation, and the persons to be investigated, as well as that  
9 the information likely to be obtained is foreign intelligence  
10 information not concerning a "United States person." 50 USC §  
11 1804(a)(1) to (11). Both of these statutes counter the  
12 government's myopic view of federal law in this area.

13 In further support of its conflict-preemption argument,  
14 the government points to 18 USC § 798(a), a statute that makes it a  
15 crime to divulge improperly any classified information "concerning  
16 the communication intelligence activities of the United States."  
17 18 USC § 798(a). Because the disclosure under the subpoenas is not  
18 "authorized," such disclosures may violate federal law. Yet the  
19 term "classified information" for purposes of 18 USC 798(a) means  
20 "information which, at the time of a violation of this section, is,  
21 for reasons of national security, specifically designated by a  
22 United States Government Agency for limited or restricted  
23 dissemination or distribution." 18 USC § 798(b). And the  
24 government does not purport to have designated as classified the  
25 records at issue here; indeed, it has not acknowledged that the  
26 carriers even divulged records to the NSA. As such, no conflict  
27 exists with 18 USC §798(a) until the government "specifically  
28 designate[s]" the records pertinent to the cases at bar. Even if

1 the pertinent records fall under 18 USC § 798(a), the  
2 aforementioned statutory privileges – not to mention the state  
3 secrets privilege – furnish the government with more than enough  
4 protection against any conflict.

5 Finally, the government contends that presidential  
6 executive orders aimed at protecting national security information  
7 conflict with the state investigations. Executive orders, in and  
8 of themselves, do not preempt state law. Congress has the  
9 exclusive power to make laws necessary and proper to carry out the  
10 powers vested by the United States Constitution in the federal  
11 government. Youngstown Sheet & Tube Co v Sawyer, 343 US 579  
12 (1952). Only when executive orders are necessary as a means of  
13 carrying out federal laws do they preempt state law. Cf Fidelity  
14 Federal Sav & Loans Ass'n, 458 US at 154 (administrative  
15 regulations may preempt state law when Congress has delegated that  
16 rule-making power).

17 Executive order 12,958 directs agencies to control  
18 strictly the classified information in their possession and to  
19 ensure that information is disclosed only when doing so is "clearly  
20 consistent with the interests of national security." 60 Fed Reg  
21 19825. Similarly, executive order number 12,968 (60 Fed Reg 40245)  
22 establishes a security program for access to information by non-  
23 government employees and 36 CFR § 1222.42(b) requires that when  
24 "nonrecord material containing classified information is removed  
25 from the executive branch, it is protected under conditions  
26 equivalent to those required of executive branch agencies \* \* \*."

27 The government attempted to explain why these orders are  
28 necessary as a means of carrying out federal laws, as required for



1 preemption, for the first time at oral argument. Without the  
2 benefit of briefing, however, it remains uncertain whether these  
3 executive orders amount to anything more than mere expressions of  
4 executive will. But even supported by an act of Congress, these  
5 orders cannot carry the day for the government. Again, no conflict  
6 inheres because for any information sought in violation of these  
7 orders the government may exercise its privileges, statutory or  
8 otherwise.

9 Accordingly, the government cannot show the requisite  
10 conflict because, based on the present record, the investigations  
11 do not require an act by the carriers that federal law or policy  
12 deems unlawful. Nor do the investigations pose an obstacle to the  
13 purposes and objectives of Congress. Should it occur that  
14 information sought by the states implicates the aforementioned  
15 executive orders but falls outside the state secrets privilege, the  
16 court will entertain a renewed motion from the government based on  
17 conflict preemption.

18  
19 C

20 Even if no federal activity preempts the state laws at  
21 issue here, the state investigations are said to infringe on the  
22 foreign affairs power of the federal government under Zschernig v  
23 Miller, 389 US 429 (1968). The national government's exclusive  
24 authority to regulate the foreign affairs of the United States has  
25 long been recognized as a constitutional principle of broad scope.  
26 See United States v Pink, 315 US 203, 233 (1942) ("Power over  
27 external affairs is not shared by the States; it is vested in the  
28 national government exclusively."); Hines v Davidowitz, 312 US 52,

1 63 (1941). "It follows that all state action, whether or not  
2 consistent with current foreign policy, that distorts the  
3 allocation of responsibility to the national government for the  
4 conduct of American diplomacy is void as an unconstitutional  
5 infringement on an exclusively federal sphere of responsibility."  
6 Laurence H Tribe, American Constitutional Law § 4-5 at 656 (3d ed  
7 2000).

8 This principle, which prohibits state action that unduly  
9 interferes with the federal government's authority over foreign  
10 affairs, derives from both the text and structure of the  
11 Constitution. The Constitution allocates power for external  
12 affairs to the legislative and executive branches of the national  
13 government and simultaneously prohibits the states from engaging in  
14 activities that might interfere with the national government's  
15 exercise of these powers. To be sure, no clause in the  
16 Constitution explicitly bestows a "foreign affairs power" to the  
17 federal government. See L Henkin, Foreign Affairs and the United  
18 States Constitution 14-15 (2d ed 1996). But a number of  
19 provisions, when read together, strongly imply that such authority  
20 was intended. See Harold G Maier, Preemption of State Law: A  
21 Recommended Analysis, 83 Am J Int'l L 832, 832 (1989) ("[N]either  
22 the Articles of Confederation nor the Constitution provided for a  
23 general foreign affairs power. Nonetheless, there was never any  
24 real question that the United States would act as a single nation  
25 in the world community.").

26 Specifically, the Constitution provides that Congress  
27 possesses the authority "to lay and collect Taxes, Duties, Imposts  
28 and Excises, to pay the Debts and provide for the common Defense

1 and general Welfare of the United States," US Const art I, § 8, cl  
2 1, "to regulate Commerce with foreign Nations," id, cl 3, and "to  
3 define and punish Piracies and Felonies committed on the high Seas,  
4 and Offences against the Law of Nations," id, cl 10. Additionally  
5 Congress is granted the power "to declare War, grant Letters of  
6 Marque and Reprisal, and make Rules concerning Captures on Land and  
7 Water," id, cl 11, and the President is designated the "Commander  
8 in Chief of the Army and Navy of the United States," id, art II, §  
9 2, cl 1.

10 With respect to the states, the Constitution directs that  
11 "no State shall enter into any Treaty, Alliance, or Confederation;  
12 grant Letters of Marque and Reprisal" or, without the consent of  
13 Congress, "lay any Imposts or Duties on Imports or Exports" or  
14 "enter into any Agreement or Compact \* \* \* with a foreign Power,"  
15 or "engage in War, unless actually invaded, or in such imminent  
16 Danger as will not admit of delay." Id, § 1, cl 10.

17 These and other constitutional provisions evidence an  
18 intent on the part of the framers to grant paramount authority for  
19 foreign affairs to the political branches of the federal  
20 government, thereby necessitating the exclusion of intrusive  
21 efforts on the part of the states in foreign relations. The  
22 Supreme Court enshrined these principles in Zschernig v Miller, 389  
23 US 429 (1968), in which the Court announced the foreign affairs  
24 doctrine that governs the cases at bar.

25 Zschernig involved an Oregon probate statute that  
26 conditioned the inheritance rights of an alien not residing in the  
27 United States on his ability to prove that American heirs would  
28 have a reciprocal right to inherit estates in the foreign country

1 and that he would receive payments from the Oregon estate "without  
2 confiscation, in whole or in part, by the governments of such  
3 foreign countries." Id at 430. The Supreme Court noted that it  
4 had earlier refused to invalidate a similar statute enacted by  
5 California "on its face" because that statute would have only "some  
6 incidental or indirect effect in foreign countries." Id at 432-33  
7 (quoting Clark v Allen, 331 US 503, 517 (1947)). In Zschernig,  
8 however, the Court assessed "the manner of [the Oregon statute's]  
9 application" and observed that the law had compelled state courts  
10 to "launch[] inquiries into the type of governments that obtain in  
11 particular foreign nations." 389 US at 433. The Court noted, for  
12 example, that the statute triggered assessments of "the actual  
13 administration of foreign law" and "the credibility of foreign  
14 diplomatic statements." Id at 435. In short, the statute "seemed  
15 to make unavoidable judicial criticism of nations established on a  
16 more authoritarian basis than our own." Id at 440. Looking at these  
17 effects of the Oregon statute, the Court concluded that it was  
18 unconstitutional because it "affected international relations in a  
19 persistent and subtle way," had a "great potential for disruption  
20 or embarrassment" and triggered "more than 'some incidental or  
21 indirect effect in foreign countries.'" Id at 434-35, 440.

22 Zschernig thus stands for the proposition that states may  
23 legislate with respect to traditional state concerns, such as  
24 inheritance and property rights, even if the legislation has  
25 international implications, but such conduct is unconstitutional  
26 when it has more than an "incidental or indirect effect in foreign  
27 countries." Id at 440. As the First Circuit recently observed,  
28 under Zschernig, "there is a threshold level of involvement in and

1 impact on foreign affairs which the states may not exceed."  
2 National Foreign Trade Council v Natsios, 181 F3d 38, 49-57 (1st  
3 Cir 1999), aff'd on other grounds sub nom, Crosby v National  
4 Foreign Trade Council, 530 US 363 (2000).

5 But Zschernig, and the foreign affairs power it  
6 announced, has its limits. Only a handful of state or local laws  
7 have been struck down under Zschernig, and these laws have  
8 typically singled out foreign nations for regulation. See, e g,  
9 Natsios, 181 F3d 38, 53 (finding that the Massachusetts Burma Law,  
10 which restricted the ability of Massachusetts and its agencies from  
11 purchasing goods or services from companies that did business with  
12 Burma (Myanmar), was unconstitutional, in part, as a "threat to  
13 [the] federal foreign affairs power"); Tayyari v New Mexico State  
14 University, 495 F Supp 1365, 1376-79 (D NM 1980) (striking down a  
15 university's policy designed to "rid the campus of Iranian  
16 students" because it conflicted with a federal regulation and  
17 "frustrated the exercise of the federal government's authority to  
18 conduct the foreign relations of the United States"); Springfield  
19 Rare Coin Galleries, Inc v Johnson, 115 Ill 2d 221 (Ill 1986)  
20 (invalidating an Illinois statute that excluded South Africa from a  
21 tax exemption as more than an "incidental" intrusion on the federal  
22 government's foreign affairs power); Bethlehem Steel Corp v Board  
23 of Commissions, 276 Cal App 2d 221 (1969) (invalidating a  
24 California Buy American statute because it had "more than 'some  
25 incidental or indirect effect in foreign countries' and \* \* \* great  
26 potential for disruption \* \* \* .").

27 The Ninth Circuit's decision in Deutsch v Turner Corp,  
28 324 F3d 692 (9th Cir 2003), sheds light on the present issues.

United States District Court  
For the Northern District of California

1 Deutsch affirmed this court's decision in In re World War II Era  
2 Japanese Forced Labor Litig, 164 F Supp 2d 1160 (ND Cal 2001),  
3 finding preemption of a California law that created a cause of  
4 action for victims of World War II slave labor. The Ninth Circuit  
5 stated that California had "sought to create its own resolution to  
6 a major issue arising out of the war - a remedy for wartime acts  
7 California's legislature believed had never been fairly resolved."  
8 Id at 712. Because the power to make and resolve war included the  
9 authority to resolve war claims, the California scheme was  
10 preempted by the federal scheme. Id at 714. As this court  
11 observed, the statute's terms and legislative history "demonstrate  
12 a purpose to influence foreign affairs directly" and "target[]  
13 particular countries," as "California intended the statute to send  
14 an explicit foreign relations message, rather than simply to  
15 address some local concern. In re WWII, 164 F Supp 2d at 1173,  
16 1174.

17 In contrast to the law in Deutsch, none of the state laws  
18 the government seeks to preempt was enacted to influence foreign  
19 affairs. Nor can it be said that any state has attempted to  
20 "establish its own foreign policy." 389 US at 441. Instead, the  
21 laws underlying the state investigations are directed at more  
22 mundane, local concerns such as utility regulation and privacy,  
23 traditional realms of state power.

24 Nor is there a basis for concluding that the  
25 investigations of the carriers will have significant impact on the  
26 government's relations with any foreign nation. In this regard,  
27 Int'l Ass'n of Indep Tanker Owners v Locke, 148 F3d 1053, 1068 (9th  
28 Cir 1998), is instructive. The Ninth Circuit in Locke rejected out

1 of hand the argument that onerous regulations on oil tankers  
2 promulgated by the state of Washington were unconstitutional under  
3 Zschernig because the litigant "failed to demonstrate that, even if  
4 [those] regulations [had] some extraterritorial impact, that impact  
5 [was] more than 'incidental or indirect.'" Locke, 148 F3d at 1069  
6 (quoting Zschernig, 389 US at 434). Akin to the regulations in  
7 Locke, the state investigations may have an effect on foreign  
8 affairs, but that effect is only incidental and indirect. See  
9 Zschernig, 389 US at 433.

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

D

Finally, the court takes up how the state secrets  
privilege bears on the state officials' investigations. The  
Director of the NSA, General Keith B Alexander, has concluded that  
permitting the investigations to proceed would interfere with the  
national security operations of the government. Doc #265, Ex A.  
Alexander's declaration explains that each of the "five of the  
state proceedings \* \* \* seek, at a minimum, information regarding:  
(1) whether specific telecommunication carriers assisted the NSA  
with an alleged foreign intelligence program involving the  
disclosure of large quantities of records pertaining to customer  
communications; and (2) if such a program exists, the precise  
nature of the carriers' alleged involvement and details concerning  
the alleged NSA activities." Doc #265, Ex A, ¶ 16. According to  
Alexander, confirming or denying "allegations concerning  
intelligence activities, sources, methods, relationships, or  
targets" would harm national security in various ways. Id, ¶ 17.  
//

1 In view of this court's analysis in Hepting v AT&T Corp.,  
2 439 F Supp 2d 974 (ND Cal 2006), the court notes – and the state  
3 officials acknowledge – that some of the information sought in  
4 these investigations may implicate the state secrets privilege.  
5 Conversely, some questions posed in these investigations fall  
6 outside the privilege's scope, a point the government conceded at  
7 oral argument. With further guidance from the Ninth Circuit, the  
8 court will be able to decide whether and to what extent the state  
9 investigations may proceed. Accordingly, the court declines to  
10 rule on the state secrets issue pending the Ninth Circuit's  
11 decision in Hepting v AT&T Corp.

12  
13 IV

14 In sum, the government's summary judgment motion is  
15 DENIED WITHOUT PREJUDICE to its renewal following the Ninth  
16 Circuit's decision in Hepting v AT&T. The court also DENIES AS  
17 MOOT the state officials' motions for summary judgment. After the  
18 Ninth Circuit issues an order in Hepting, the parties may renotece  
19 their cross motions.

20  
21 IT IS SO ORDERED.

22 

23  
24 VAUGHN R WALKER  
25 United States District Chief Judge  
26  
27  
28



**Randal S. Milch**  
Senior Vice President, Legal & External Affairs &  
General Counsel  
Verizon Business



One Verizon Way  
VC43E043  
Basking Ridge, NJ 07920

Phone: 908-559-1752  
Fax: 908-696-2136  
[randal.s.milch@verizonbusiness.com](mailto:randal.s.milch@verizonbusiness.com)

October 12, 2007

The Honorable John D. Dingell  
Chairman, Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

The Honorable Edward J. Markey  
Chairman, Subcommittee on Telecommunications and  
the Internet  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

The Honorable Bart Stupak  
Chairman, Subcommittee on Oversight and  
Investigations  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear Chairmen Dingell, Markey and Stupak:

Ivan Seidenberg has asked me to respond to your letter to him dated October 2, 2007. I am pleased to be able to provide you with information in response to your questions.

As set out in greater detail below, Verizon has a longstanding and vigorous commitment to protecting its customers' privacy and takes comprehensive steps to protect that privacy. Verizon has safeguards and procedures in place to guard against the improper disclosure or theft of customer information. We review and modify those procedures and policies on a regular basis. Verizon's goal is to minimize the possibility of the improper disclosure of customer information, while at the same time to provide quality service to its customers.

Federal and state laws recognize, however, that criminals and terrorists may use our network to discuss or implement their schemes and explicitly authorize Verizon – through the provisions of the Foreign Intelligence Surveillance Act (FISA) and other statutory provisions – to provide assistance to government entities in their law enforcement and counter-terrorism efforts. Similarly, our business records may be of vital importance in investigations and in emergency situations to protect lives, and existing law authorizes our assistance to government entities in these situations as well.

As you are no doubt aware, as a result of news reports in May 2006, Verizon and other carriers have been the object of numerous class-action lawsuits and a number of state public utility commission investigations relating to alleged assistance with classified counter-terrorism programs allegedly instituted in the wake of the September 11 attacks. In the context of this litigation, we have been informed by the Department of Justice that we cannot confirm or deny Verizon's role (if any) in the alleged programs. See, e.g., Letter from Peter D. Keisler, Asst. Attorney General to John A. Rogovin, Counsel for Verizon, *et al.* at 2 (June 14, 2006). Similarly, the United States has brought suit against Verizon and other carriers, seeking to enjoin Verizon from responding to state public utility commission inquiries prompted by these news reports, because to do so would be "inconsistent with and would violate federal law including, but not limited to, Executive Order 12958, 18 U.S.C. § 798, and 50 U.S.C. § 402 note, as well as other applicable federal laws, regulations, and orders." See Complaint, *United States v. Zulima Farber, et. al* at 13 (D.N.J. filed on June 14, 2006).

In light of the Government's position, as most recently reiterated in Ms. Kathleen Turner's letter to Chairman Dingell of today's date, Verizon's responses to your questions herein necessarily exclude any information, discussion, reference to or representations concerning its cooperation, if any, with classified intelligence gathering activities. All of the responses to the numbered questions below are subject to this proviso and must be read consistently with it. I regret that there is any such limitation on our response.

Verizon Wireless was never named in any of the news reports as having allegedly participated in the purported programs (and indeed was dismissed from the litigation mentioned above); these responses are therefore made on behalf of the various wireline operating subsidiaries of Verizon Communications.

**1. Please describe the typical process by which your company receives requests for customer records consistent with the FISA process and how such records are disclosed to requesting entities, including how such requests are made, what documents are required, and the timeframe in which your company typically responds.**

FISA orders seeking business records are authorized by 50 U.S.C. § 1861. FISA orders are classified documents and as such would be delivered by the government to Verizon personnel holding appropriate security clearances. Pursuant to 50 U.S.C. § 1805(c), FISA orders contain detailed and specific directions relating to the actions

sought and their duration. Given their critical importance to national security, we would comply with such orders as expeditiously as possible.

**2. The FISA process permits governmental entities to obtain records, in certain compelling or time-sensitive circumstances, prior to obtaining authorization from the FISA court. In such situations, the government must subsequently seek such authorization within 72 hours of commencing a wiretap or requesting such records. What is the process by which your company complies with such requests? What is the process by which your company assures itself that the requesting entity has subsequently fulfilled its obligation to seek FISA court authorization? How often has your company been requested to commence a wiretap or search for records without an NSL, where the entity seeking such information has subsequently received authorization?**

50 U.S.C. § 1805(f) provides for emergency electronic surveillance. In such a situation, and pursuant to those statutory procedures, Verizon would receive a classified written notification that the Attorney General has authorized the emergency surveillance, stating the time of such authorization. We would provide the assistance requested as expeditiously as possible. If we do not receive a FISA order to continue the surveillance within 72 hours of the Attorney General's authorization, the surveillance would be terminated.

A similar procedure is provided for emergency pen register or trap and trace ("pen/trap") requests in 50 U.S.C. § 1843. In these situations Verizon would receive a classified written notification that the Attorney General has authorized the emergency pen/trap, again including the time of such authorization. If a FISA pen/trap order is not received in 48 hours of the emergency authorization, the pen/trap would be terminated.

18 U.S.C. § 2709 authorizes the FBI to issue National Security Letters ("NSLs") for specified customer information or records. That provision does not address wiretaps, and Verizon has not provided assistance to the government to conduct a wiretap based on an NSL.

18 U.S.C. §§ 2702(b)(8) and (c)(4) authorize Verizon to provide the content of stored communications and business records relating to customers to government entities in emergencies, absent a court order or an NSL. Our ability to provide certain information to government entities on an emergency basis is critical to the public safety. Here are some examples:

- Verizon's security teams were able to identify through an IP address the location of a child predator who had abducted a 13 year old girl. Verizon provided the location information to a waiting SWAT team who found the young girl, tied to a bed, but otherwise relatively unharmed. The predator is now serving a 20 year prison term.

- Verizon security working with US Immigration and Customs Enforcement (ICE) agents identified through an IP address the location of a man who was using a webcam to broadcast the sexual abuse of a 6 year old boy. Through Verizon's help law enforcement agents were able to locate and arrest the predator and he is now serving a 30 year prison sentence.
- In April 2007 a New York City Detective sought Verizon's help on an emergency basis in a case involving a gunman holding five hostages. We identified the last working phone service to the address and assisted the NYPD in establishing communications with the hostage taker. The hostages were released uninjured and the gunman was arrested.
- In March 2007, the U.S. Marshals Service was seeking a fugitive charged with holding a gun to the head of a pregnant woman during a home invasion while her child watched. The Marshals learned that the fugitive was armed and using a Verizon DSL line to communicate with associates, and sought Verizon's help on an emergency basis to locate him, using IP subscriber records. His location in Albany N.Y. was established and the Marshals were able to apprehend him without incident.
- In September 2007 the Wood County Schools in Parkersburg, West Virginia were plagued by a series of bomb threats. On September 26, a bomb threat was made to Parkersburg South High School via telephone. Local authorities sought Verizon's help in finding the source of the call on an emergency basis, and two teenagers were arrested the same day.

**3. Has your company been asked to produce or provide information relating to your customers without an NSL or FISA authorization? If so, please provide the date or dates such request(s) were made and the form in which such request came. Who or what entity or entities has asked your company to produce or provide information relating to your customers outside of the FISA process?**

We have been asked to provide information pertaining to a customer pursuant to federal and state laws other than 18 U.S.C. § 2709 and FISA. There are several federal statutes authorizing the interception of wire and electronic communications (18 U.S.C. § 2510 et seq.); the use of pen/traps (18 U.S.C. § 3121 et seq.); the compulsory production of stored customer communications and records (18 U.S.C. § 2703); and their voluntary disclosure by service providers (18 U.S.C. § 2702). There are similar provisions in various state statutes. We receive thousands of such lawful demands and requests each month.

Because of their volume, I provide here round numbers relating to such requests and demands for the Verizon operating companies for 2005, and for Verizon and the former MCI (jointly) from January 2006 until September 2007. In 2005, Verizon received 90,000 lawful requests and demands for customer information from federal, state and local officials, with approximately 36,000 coming from federal officials, and

54,000 coming from state and local officials. In 2006, Verizon received 88,000 such requests and demands (approximately 34,000 from federal officials and 54,000 from state and local officials), and through September 2007, 61,000 such requests and demands (approximately 24,000 from federal officials and 37,000 from state and local officials). Verizon also received lawful requests for customer information from civil litigants numbering 57,000 in 2005, 69,000 in 2006 and 66,000 through September 2007.

Of the requests and demands coming from federal, state and local officials, requests for emergency assistance were approximately 23,700 in 2005 (240 of which were from federal officials), 25,000 in 2006 (300 of which were from federal officials) and 15,000 through September 2007 (180 of which were from federal officials). Some examples of these emergency responses are set out in my response to Question 2.

Verizon received in 2005 over 1,300 pen/trap court orders, as well as over 250 wiretap court orders requested by federal and state law enforcement authorities. In 2006, we received over 800 pen/trap court orders and nearly 200 wiretap court orders. Through September 2007, these numbers are over 500 and over 130, respectively. These numbers include instances in which wiretap or pen/trap orders were renewed.

**4. Did your company raise the lack of FISA process or the lack of an NSL with any entity requesting customer information? If so, what was the governmental entity's response?**

In the situations described in response to Question 3, Verizon provided customer information to government entities in reliance on legal authorizations under applicable federal and state laws.

**5. What has been the stated legal justification provided by governmental entities for producing or providing information relating to your customers, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request for customer information? If so, please provide that analysis.**

Governmental entities have cited statutory provisions, including those noted in response to Questions 2 and 3, as authorization for production of such information. Because of the complexity of the laws authorizing government requests, however, Verizon on occasion receives requests with incorrect authorizations. For instance, Verizon has received an 18 U.S.C. § 2703(b) subpoena seeking stored voice mail, while 18 U.S.C. § 2703(a) requires a search warrant for that information. Verizon would bring such an error to the attention of the relevant government official and would not respond until an appropriate authorization is received. We do not keep track of these instances; our focus is on having the right authorization for the assistance requested.

**6. Do you believe it is proper for the onus to be on a company to determine whether the Government is acting within the scope of its authority when it requests customer information?**

No, for a number of important reasons.

Congress has properly enacted a number of protections for telecommunications providers that assist the government. For example, current law states that a telecommunications provider may not be sued for providing assistance to the government, in accordance with the terms of a subpoena, government certification, court order or warrant, among other things. *E.g.*, 18 U.S.C. §§ 2703(e), 2511(2)(a)(ii); 50 U.S.C. § 1805(i). Current law also provides a complete defense to any provider who in good faith relies on a statutory authorization (such as in emergency situations). *E.g.*, 18 U.S.C. §§ 2520(d), 2707(e)(1). If the government advises a private company that a disclosure is authorized by statute, a presumption of regularity attaches. *See Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 174 (2004). Federal statutes also give a provider a complete defense for good faith reliance on other forms of authorization or certain government requests for information. *E.g.*, 18 U.S.C. §§ 2707(e), 2520(d).

These statutory provisions are consistent with longstanding common law principles, which allow citizens to rely on the government's judgment when it asks for assistance. *See, e.g.*, Restatement (Second) of Torts § 139, cmt. d ("To require a person whom a peace officer calls upon to assist in making an arrest to take the risk for being liable in the event that the officer is not himself privileged to make it, unless such person exercises such judgment and makes such investigations as he would be required to make were he acting on his own initiative, would seriously deter such persons from giving the prompt aid necessary to effect arrests which, save in an insignificant minority of cases, the officer is privileged to make.") The person providing assistance is not obligated to second guess the government's stated need for help. *Id.*, cmt. e ("It is for the peace officer and not the actor to determine the necessity for assistance.")

One of the reasons for this rule is that private parties do not have all the information necessary to completely assess the propriety of the government's actions and that such information is uniquely in the control of the government – as for example, how grave and imminent the threat is, how necessary the government's actions are, or whether there are alternative ways of meeting the danger that would be equally effective.

Such an approach is vital to ensuring that providers are able to respond quickly to requests for assistance. Placing the onus on the provider to determine whether the government is acting within the scope of its authority would inevitably slow lawful efforts to protect the public. When an emergency situation arises, prompt assistance is often needed. If the provider were to face legal liability in the event the government is later deemed to have acted outside its authority, the provider would have to meet every request for assistance with extensive questions about the need and justification for the request. The provider would also have to seek legal advice about the merits of the

government's justification. Each of these steps would delay the government's receipt of assistance it might need to save lives.

Moreover, such delays would be unjustified because legal restraints on the government can be used to limit the potential for government abuse. For example, any evidence obtained in violation of the law may be suppressed in any subsequent criminal prosecution. The government also may face legal liability for acting outside its authority. *E.g.*, 18 U.S.C. § 2712.

**7. Specifically what information relating to your customers have you been asked to produce or provide outside of the FISA process? What information relating to your customers have you produced or provided to any governmental entities outside of the FISA process?**

As stated in response to Questions 2 and 3 above, there are various state and federal laws that govern what types of information and assistance Verizon is required and permitted to provide government entities and private attorneys in civil, criminal and administrative proceedings in addition to the FISA process that cover wiretaps, pen/traps and customer information requests.

Verizon has been asked to provide to government entities "a record or other information," 18 U.S.C. § 2703(c)(1), relating to our customers, including the six categories of information specified in 18 U.S.C. § 2703(c)(2):

1. Subscriber Name;
2. Subscriber Address;
3. Local and long distance telephone connection records, or records of session times and durations;
4. Length of service and type of service utilized;
5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. Means and source of payment for such service, including credit card or bank account number of a subscriber to such service.

We provide records in these categories in response to lawful requests to the extent we maintain them and they are available.

**8. Are you currently producing or providing any information to governmental entities outside of the FISA process? If so, specifically what information relating to your customers are you producing or providing outside of the FISA process?**

Please see my responses to Questions 3 and 7.

**9. Have you at any time sought consent from your customers to produce or provide personally identifiable information to any governmental entities outside of the FISA process?**

Verizon has informed its customers that it will respond to authorized government requests for information and will provide information to government entities in public safety situations, so our customers are on notice that we will do so. For example, Verizon's Telephone Company Customer Privacy policy, available on Verizon's website, explains that "we do release customer information without involving you if disclosure is required by law or to protect the safety of customers, employees or property." It further states that "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."

**10. What safeguards did you and do you currently have in place to ensure that you do not disclose information relating to your customers in violation of 47 U.S.C. § 222 or any other provision of the Communications Act?**

We recognize the importance of protecting our customers' privacy, and customer privacy is a priority for Verizon. Thus, Verizon permits access to Customer Proprietary Network Information (CPNI) to those parties lawfully permitted to have such access, such as Verizon employees acting within the scope of normal business, customers requesting access to their own information, persons designated by the customers, government entities, or Verizon's affiliates or agents, if lawfully permitted. Such access is limited to legitimate business purposes and in compliance with applicable law.

Verizon has a robust security organization and extensive procedures to detect inappropriate access to confidential information. These technical, procedural and organizational measures are designed to safeguard computer systems and detect and thwart unauthorized access to Verizon's databases. Verizon has rigorous measures in place to prevent disclosure of confidential information to any unauthorized party, including "data brokers," private investigators, and Verizon's own employees. Verizon is continually reviewing and updating its security procedures to respond to changes in technology and the evolving tactics of criminals seeking access to CPNI. Because we are concerned that data dealers and others seeking to gain improper access to CPNI could use a detailed technical response to this question as a roadmap for further misconduct, we limit our response here to a summary of some of those safeguards, set forth below.

Employees are trained regarding the privacy protections they are required to undertake to protect sensitive personal information. For example, Verizon employees are trained to follow a strict "Code of Business Conduct," including specific requirements regarding the protection and use of CPNI. Employees who violate company standards and policies may be disciplined up to and including dismissal. Verizon employees' responsibility to safeguard CPNI is also reinforced in the company's methods,



procedures, and refresher training, and compliance is enforced through regular service quality observation. Verizon employees who regularly come into contact with CPNI as a part of their duties are provided additional, specialized training on protecting CPNI. Moreover, Verizon requires responsible senior executives to certify annually that their operations have internal controls in place to comply with Verizon's policies and the statutory and FCC requirements to protect CPNI.

Verizon corporate policy also imposes requirements regarding the proper collection, use and disclosure of sensitive customer information. For example, our policy instructs employees to refrain from displaying sensitive personal information within applications, systems, or databases to individuals who are not authorized to access or view the information and to avoid storing sensitive personal information on removable electronic media unless that media is encrypted. To limit the risk of unauthorized access or fraudulent use of sensitive personal information, all Verizon employees must immediately report any discovery of vulnerability, exposure, loss or unauthorized access to sensitive personal information to Verizon Security.

Each Verizon business unit has a Departmental Compliance Manager who is responsible for developing, implementing, and overseeing CPNI compliance within his or her respective organization. The Departmental Compliance Managers participate in monthly calls to discuss recent developments, legislation, regulatory trends, and business procedures involving CPNI. Members of Verizon's regulatory compliance and legal department also participate in these monthly calls and work with the Departmental Compliance Managers on a regular basis to review issues that may arise and to provide advice and guidance.

Specific caller identity validation procedures are followed prior to discussing account information. In particular, Verizon has procedures in place requiring employees to authenticate customer identity before discussing subscriber account information. These procedures address both employee interactions with residential and business customers over the telephone as well as customer authentication requirements for on-line account management. Verizon consistently evaluates its policies and procedures and changes them as appropriate. For example, as required by new FCC rules, Verizon is changing its policies and procedures to ensure that customers are notified of significant account changes such as a change of address or passwords to give them an opportunity to verify the changes or be made aware of unauthorized access to their accounts. In addition, Verizon has determined that it will no longer discuss call detail information with customers who call in unless the customer provides the specific call to be discussed. General requests to provide call detail information over the phone will be handled by either sending requested information to the address of record or calling the customer back at the account number of record.

Verizon also protects financial information such as customer credit card data in accordance with industry standards, and Verizon's existing operational safeguards are regularly monitored. These include encryption of credit card data while in transit; access controls or masking of data in applications that display credit card information; firewall and intrusion detection systems to protect our internal network and servers; and no

retention of credit card magnetic stripe data, the CVV2 codes (the 3 or 4 digit code on the back of the card), or pin numbers.

**11. Have you at any time been offered indemnification for producing or providing information relating to your customers to governmental entities, either within or outside of the FISA process? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing information relating to your customers to governmental entities, either within or outside of the FISA process? If so, who or what entity made such offer?**

Verizon has not been offered indemnification for the provision of any information to government entities. Congress has, however, consistently required that communications providers be compensated for their costs of responding to lawful requests for information from government entities. For example, Verizon has received compensation for reasonable costs incurred in complying with interception orders pursuant to 18 U.S.C. § 2518(4)(e); for effecting pen/traps pursuant to 18 USC § 3124 (c); for providing stored communications and customer records under 18 U.S.C. § 2706; for providing assistance in effecting electronic surveillance under 50 U.S.C. § 1805(c)(2)(D); and for effecting pen/traps under 50 U.S.C. § 1842(d)(2)(B)(iii).

**12. Have you ever been asked to install or permit the installation of equipment on your network to intercept Internet traffic? Have you ever been asked to install or permit the installation of equipment on your network to send copies of Internet traffic to any third parties? If so, who asked you to install such equipment and on what dates? Have you ever installed or permitted the installation of equipment on your network to send copies of Internet traffic to any third parties?**

**a. Have you at any time been presented with a subpoena or other court or administrative order directing you to install or permit the installation of such equipment? If so, what type(s) of court or administrative order did you receive? On what dates did you receive such subpoenas or other court or administrative orders?**

**b. If you have ever installed or permitted the installation of equipment on your network to send copies of Internet traffic to any third parties, please identify the third parties to whom copies of Internet traffic were sent.**

**c. Who asked you to install or permit the installation of such equipment? On what dates did you receive such requests? On what dates did you comply with such requests?**

**d. What has been the stated legal justification provided by governmental entities for installing or permitting the installation of such equipment and producing or providing such information relating to your customers, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request to install or**

**permit the installation of such equipment? If so, please provide that analysis.**

**e. Have you at any time been offered indemnification for installing or permitting the installation of such equipment and producing or providing such information? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing Internet traffic information relating to your customers? If so, who or what entity made such offer?**

**f. Are you currently producing or providing any Internet traffic information to governmental entities? If so, specifically what information relating to Internet traffic are you producing or providing?**

**g. Have you at any time sought consent from your customers to produce or provide this Internet traffic information?**

The Communications Assistance for Law Enforcement Act ("CALEA") requires telecommunications carriers to ensure that their networks have specified capabilities and capacity related to electronic surveillance. The FCC has determined that CALEA applies to broadband Internet access service. Verizon accordingly has installed equipment and software on its networks to effect CALEA compliance for the interception of broadband Internet traffic.

The various statutes discussed in response to Question 3 each authorize government entities to demand and receive "Internet traffic information." For example, 18 U.S.C. §§ 2510 et seq. and similar state laws permit a demand for Internet traffic including content. 18 U.S.C. § 2703(a) authorizes disclosure of stored email. 18 U.S.C. §§ 2703(c)(1)(B), (2)(C) and (2)(E) permit a lawful demand for information relating to Internet traffic ("session times and durations," "any temporarily assigned network address"), and 18 U.S.C. § 2702(c) authorizes the provision of such information in other defined circumstances, including emergencies. Similarly, 18 U.S.C. § 3127 was modified by the U.S. PATRIOT Act to include "routing" and "addressing" information in the definitions of "pen register" and "trap and trace device." FISA also covers the interception of Internet traffic including content in 50 U.S.C. § 1805 and the use of pen/traps to obtain Internet traffic data in 50 U.S.C. § 1842. Under 50 U.S.C. § 1841, the definitions of pen register and trap and trace device in 18 U.S.C. § 3127 are incorporated into FISA.

Verizon has not been indemnified for meeting its CALEA obligations or in responding to demands under the statutes set out above. As set out in my response to Question 11, however, Verizon has received compensation for its costs consistent with federal law for responding to lawful requests.

The privacy policies discussed in response to Question 9 also cover Verizon's consumer broadband services. In addition, the Verizon Online Privacy Policy informs Verizon Online customers that Verizon discloses information when such "disclosure is

required by law, or deemed necessary by Verizon in its sole discretion to protect the safety, rights or property of Verizon or any other person or entity."

**13. On September 9, 2007, the *New York Times* reported that the FBI used NSLs to request not only the call records of particular phone company customers, but also details on those customers' "communities of interest," or the network of people with whom the customers were in contact.**

**a. Have you at any time been presented with a subpoena or other court or administrative order directing you to produce or provide information about any customer's community of interest? If so, what type(s) of court or administrative order did you receive? On what dates did you receive such subpoenas or other court or administrative orders?**

**b. Has your company been asked to produce or provide information relating to any customer's community of interest without an NSL or FISA authorization? If so, please provide the date or dates such request(s) were made and the form in which such request came.**

**c. What has been the stated legal justification provided by governmental entities for producing or providing such information relating to your customers' communities of interest, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request for information about your customers' communities of interest? If so, please provide that analysis.**

**d. Specifically what information relating to your customers' communities of interest have you been asked to produce or provide? What information relating to your customers' communities of interest have you produced or provided to any governmental entities?**

**e. Have you at any time been offered indemnification for producing or providing information about your customers' communities of interest? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing information about your customers' communities of interest? If so, who or what entity made such offer?**

**f. Are you currently producing or providing any information to governmental entities concerning your customers' communities of interest? If so, specifically what information relating to your customers' communities of interest are you producing or providing?**

**g. Have you at any time sought consent from your customers to produce or provide information about their communities of interest?**

Pursuant 18 U.S.C. § 2703(c)(1), Verizon has received and responded to legal process which asks for information related designated telephone numbers and specific additional information relating to telephone numbers which may have called or been called by the designated numbers.

Verizon has also received subpoenas and NSLs containing "boilerplate" language directing us, for instance, to "Identify a 'calling circle' for the foregoing telephone numbers based on a two-generation community of interest; provide related subscriber information."

Because Verizon does not maintain such "calling circle" records, we have not provided this information in response to these requests; we have not analyzed the legal justification for any such requests, been offered indemnification for any such requests, or sought our customers' consent to respond to such any such requests.

I trust the foregoing information will be helpful to the Committee.

Sincerely,

A handwritten signature in cursive script that reads "Randal S. Milch".

Randal S. Milch

STATE OF VERMONT  
PUBLIC SERVICE BOARD

Docket No. 7183

Petition of Eight Ratepayers for an investigation )  
of possible disclosure of private telephone )  
records without customers' knowledge or )  
consent by Verizon New England Inc., d/b/a )  
Verizon Vermont )

Docket No. 7192

Petition of Vermont Department of Public )  
Service for an investigation into alleged )  
unlawful customer records disclosure by )  
Verizon New England Inc., d/b/a Verizon )  
Vermont )

Docket No. 7193

Petition of Vermont Department of Public )  
Service for an investigation into alleged )  
unlawful customer records disclosure by AT&T )  
Communications of New England, Inc. )

Order entered: 10/31/2007

**PROCEDURAL ORDER**

**I. SUMMARY**

These proceedings involve the alleged practice of two Vermont telecommunications carriers in providing customer record information to the National Security Agency. In today's Order the Vermont Public Service Board reactivates the dockets and establishes a schedule for discovery. Since the federal courts are considering the merits of the government's claims regarding the state secrets doctrine, we also limit the scope of the current proceedings to avoid conflict with that doctrine, allowing for subsequent examination of those issues if the doctrine should ultimately be held to be inapplicable.

### PROCEDURAL HISTORY

Dockets 7183 and 7192 were opened to examine whether Verizon New England Inc., d/b/a Verizon Vermont ("Verizon"), had violated a variety of Vermont utility standards by directly or indirectly providing customer record information to the National Security Agency ("NSA") or other federal or state agencies ("NSA Customer Records Program"). Docket 7183 was initiated by a petition filed on May 24, 2006, by the American Civil Liberties Union of Vermont ("ACLU") and by eight Vermont ratepayers. Docket 7192 was initiated by petition of the Vermont Department of Public Service ("Department" or "DPS") filed on June 21, 2006.

Docket 7193 was opened to examine whether AT&T Communications of New England, Inc. ("AT&T") violated Vermont utility standards by disclosing customer record information to the National Security Agency or other federal or state agencies. It was initiated by petition of the Department filed on June 21, 2006. The two proceedings were joined for the purposes of discovery, hearing and briefing.<sup>1</sup>

On October 2, 2006, the federal government filed *United States v. Volz*, a suit in the Federal District Court for the District of Vermont against the Chair and Members of the Public Service Board and the Commissioner of the Department of Public Service in their official capacities.<sup>2</sup> In *Volz*, the government sought to halt these investigations, asserting that:

[c]ompliance with the ordered production or similar discovery, issued by those officers under state law, would . . . place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing exceptionally grave harm to national security.<sup>3</sup>

The government asserted several bases in support of its complaint, including its exclusive authority over foreign affairs, the Supremacy Clause of the United States Constitution, preemption and the "state secrets" privilege.

Subsequently, *Volz* was transferred by the federal Judicial Panel on Multidistrict Litigation to the United States District Court for the Northern District of California and

---

1. Order of 7/12/06.

2. Case No. 2:06-cv-188 (D. Vt. Oct. 2, 2006) ("*Volz*"). AT&T and Verizon were also named defendants in the suit.

3. *Id.* at 1-2.

consolidated with four similar cases against state utility commissions. The cases were assigned to Judge Walker, and dispositive motions were argued.

Awaiting an outcome of the federal proceedings, these dockets have remained largely dormant. In March of 2007, this Board issued an Order anticipating a federal decision in the summer of 2007 that would assist in clarifying the allowable breadth of our inquiry. The Order stated that the Board had no immediate plans for hearings.<sup>4</sup>

On July 24, 2007, Judge Walker did issue a decision in *NSA Telecommunications Records Litigation*.<sup>5</sup> He denied the government's motion for summary judgment with respect to its claims under the Supremacy Clause and the federal government's powers over foreign affairs. However, with respect to the state secrets privilege, Judge Walker denied the government's motion without prejudice to its renewal following an anticipated Ninth Circuit decision in a related case that also raised the state secrets privilege.<sup>6</sup>

On October 18, 2007, the Department provided copies of letters sent by respondents Verizon and AT&T to three members of the United States House of Representatives ("October letters"). In those letters the carriers discussed their compliance with several laws, including the Foreign Intelligence Surveillance Act ("FISA") and the emergency pen register or trap and trace requests statute. Significantly, however, Verizon noted that its responses excluded "any information, discussion, reference to or representations concerning its cooperation, if any, with classified intelligence gathering activities."<sup>7</sup> Both carriers acknowledged that they provided customer information to law enforcement officials in a wide variety of contexts. As AT&T stated it, "telecommunications carriers are authorized to assist government agencies in a wide variety of circumstances, only some of which require judicial process."<sup>8</sup>

Accordingly, the issue before the Board is whether, in light of Judge Walker's ruling and the October Letters, the Board should proceed with its investigation or should await further

---

4. See Orders dated 3/29/07.

5. *In re Nat'l Sec. Agency Telecomm. Records Litig.*, MDL Dkt. No. 06-1791, 2007 WL 2127345 (N.D. Cal. July 24, 2007) ("*NSA Telecommunications Records Litigation*").

6. See *Hepting v. AT&T Corp.*, Docket No. C-06-672 VRW (N.D. Cal.).

7. Verizon letter at 2; see also, AT&T letter at 2.

8. AT&T letter at 2; see also, Verizon letter at 3-4.



developments in the federal proceeding regarding the state secrets privilege. A status conference was held in all three dockets on September 18, 2007. Thereafter the parties submitted briefs and reply briefs on whether this docket should be reactivated and, if so, what schedule should be followed.

## II. POSITIONS OF THE PARTIES

### A. Department of Public Service

The Department recommends establishing a schedule now, and that discovery can be crafted to allow the parties to "determine whether Verizon has violated Vermont law regarding the privacy of its customers' information without running afoul of the state secrets privilege."<sup>9</sup>

The DPS contends that *NSA Telecommunications Records Litigation* has now provided guidance sufficient to determine the company's compliance or non-compliance with state laws regarding protection of customer records.<sup>10</sup> In sum, the DPS maintains that the scope of these dockets is general, and grounds for relief can be demonstrated without inquiry into the existence or operation of any specific program of intelligence gathering conducted by the federal government.<sup>11</sup> The DPS argues that Judge Walker's decision suggested that a state proceeding can avoid these prohibited federal issues.<sup>12</sup>

Therefore, the DPS contends that at least some of the issues in these dockets are outside the state secrets privilege. These include, the DPS asserts, whether the recent and current content of Verizon's customer privacy policy complies with Vermont law; the nature of Verizon's understanding of what constitutes legal authorization for disclosure of customer records without seeking details regarding reliance on any specific authorizations in any particular instance; and, whether Verizon has ever turned over customer records to any entity absent one of the authorizations the company believes it is entitled to rely on, without seeking details regarding the

---

9. DPS Comments at 8.

10. DPS Comments at 1.

11. DPS Reply Comments at 5-6.

12. DPS Comments at 4.

identity of the third party receiving the information, the identity of the impacted customer, or details about the content of the information disclosed.<sup>13</sup>

The DPS also asserts that Verizon, in particular, has ended the secrecy surrounding certain factual issues.<sup>14</sup> Although only the government can waive the privilege, disclosures by non-governmental parties can reduce the scope of matters that are actually secret.<sup>15</sup>

The DPS reports that it is willing to withdraw its initial letter inquiries to Verizon and AT&T, dated May 17, 2006. The Department states that it currently intends to craft new information requests that follow the guidance from the recent federal court decisions to avoid conflict with the state secrets privilege.<sup>16</sup>

### **B. Intervenors**

The ACLU asks that the Board set a schedule and proceed with discovery, including depositions.<sup>17</sup> It claims added urgency based on a published interview with the Director of National Intelligence ("DNI") in the *El Paso Times*. That article acknowledged that the government has received cooperation from some telephone companies in a "Terrorist Surveillance Program" and that the government is seeking Congressional legislation immunizing carriers from liability.<sup>18</sup>

The ACLU asserts that it has been about a year since the Department of Justice ("DOJ") sued the Board, and although DOJ has "vigorously pursued those cases, it has lost at every step of the way." ACLU concludes that while delay might have made sense initially, action is needed now so that

neither the telecommunications companies nor the government can continue to hide behind a claim that disclosure of these insidious activities [involving communications content and records] will compromise national security.<sup>19</sup>

---

13. DPS Reply Briefs at 7.

14. DPS Comments in 7183 at 7.

15. See Docket 7183 Order of 9/18/06 at 21.

16. DPS 7183/7192 Reply at 4-5; DPS 7193 Reply at 4-5.

17. ACLU Brief at 1, 3.

18. ACLU Brief at 1-2.

19. ACLU Brief at 2.

Intervenor Michael Bandler argued to reactivate these dockets, in part based on the October Letters and in part based on his expectation that the federal litigation regarding state secrets is unlikely soon to be concluded. Mr. Bandler also proposed a schedule for discovery.

### **C. The Carriers**

AT&T and Verizon both oppose reactivation of these dockets. Primarily they contend that the *NSA Telecommunications Records Litigation* court has not resolved the state secrets issue and is awaiting guidance from the Ninth Circuit. Until that guidance arrives, the carriers contend that these dockets should remain inactive, consistent with the Board's Order of March 29, 2007.<sup>20</sup>

Both carriers maintain that allowing discovery concerning their alleged cooperation with the NSA would likely, or even certainly, lead to the issuance by the federal court of a prohibitive injunction.<sup>21</sup> They claim that three federal court decisions have held "that information related to the alleged NSA call records program is shielded by the privilege"<sup>22</sup> and that Judge Walker, the presiding judge in *NSA Telecommunications Records Litigation*, has held that there can be no discovery where the state secrets doctrine has been invoked.<sup>23</sup> They also note that a federal district court recently enjoined the Maine Public Utilities Commission from proceeding in a similar state regulatory docket.<sup>24</sup> Verizon argues that an injunction is more likely because reactivating these dockets would disturb the *status quo* and disproportionately harm the federal interest.<sup>25</sup> AT&T also complains about the unnecessary expense of participating in litigation over

---

20. Verizon opposition at 1, 7; AT&T comments at 3.

21. AT&T comments at 2 ("[I]t appears certain that the United States would seek a preliminary injunction to bar the disclosures and preserve the status quo until there is a final ruling on its motion for summary judgment and that the District Court would grant this injunction."); see Verizon opposition at 11 ("federal government likely would have no choice but to seek preliminary injunctive relief from the district court"; injunction would be "inevitable").

22. Verizon opposition at 11; see also AT&T comments at 3; Verizon reply at 5 (every court that has considered the call records program "has concluded that inquiry into even the existence or nonexistence of such a program is precluded by the state-secrets privilege").

23. AT&T comments at 3, 9.

24. *Id.*, citing *United States v. Adams*, 473 F.Supp.2d 108 (D. Me. 2007) (enjoining the Maine PUC).

25. Verizon opposition at 12.

this issue,<sup>26</sup> which it claims places it "in the middle between the competing demands of two sovereigns."<sup>27</sup>

As to events subsequent to last March's procedural orders postponing action, both carriers contend that these events should counsel against reactivation.<sup>28</sup> Notably, they assert that the current NSA director, General Alexander, has filed a declaration in federal court stating that these proceedings "cannot be disclosed, confirmed, or denied, without causing exceptionally grave damage to the national security of the United States."<sup>29</sup>

Although the government has acknowledged a *contents* surveillance program involving some foreign communications, the carriers contend that the government has never acknowledged the existence of a program that involves release of customer calling *records*.<sup>30</sup> The carriers contend that the *El Paso Times* interview with the DNI disclosed no new information<sup>31</sup> and merely reiterated prior disclosures concerning content surveillance.<sup>32</sup>

The carriers also argue that discovery cannot be narrowed sufficiently to avoid conflict with state secrets. AT&T contends that the privilege covers "any factual disclosure that would assist the Department in determining whether there is any relationship between AT&T and a NSA

---

26. AT&T comments at 2 (activating these dockets would "serve only to create an unnecessary emergency for Judge Walker and to impose wholly unnecessary expenses on AT&T").

27. AT&T comments at 2.

28. AT&T comments at 1-2; *see* Verizon opposition at 5.

29. Verizon opposition at 9; Verizon reply at 3; *see also* AT&T comments at 4. The declaration was filed after the Board denied Verizon's motion to dismiss in September, 2006, in part on the grounds that the state secrets privilege had not been properly claimed by government action. The motion was also denied because the state secrets privilege did not apply to all of petitioners' claims and because some of the matters involved in these dockets are not secret. Order of 9/20/06.

30. Verizon opposition at 11.

31. AT&T comments at 9.

32. AT&T comments at 2; Verizon opposition at 10-11.

calling records program - much less an 'inappropriate' one."<sup>33</sup> AT&T specifically rejects several possibilities for limiting the scope of these dockets.<sup>34</sup>

In sum, the carriers argue that this docket is no more urgent than last March, when the Board issued an Order saying that it had no immediate plans for hearings. The carriers urge the Board to "wait during the period of time that is required for a final appellate resolution of [the Ninth Circuit case on state secrets] and for Judge Walker to decide the issue on the merits" of whether the state secrets privilege applies.<sup>35</sup>

If the Board decides to reactivate the proceedings, AT&T asks for a schedule that would spare carriers the unnecessary expense and frustration of dealing with information requests that might be enjoined.<sup>36</sup>

#### **D. The Department of Justice**

The DOJ<sup>37</sup> filed a letter on September 26 making many of the same arguments as the carriers.<sup>38</sup> The DOJ contends that Judge Walker has made clear that his court will decide when and whether state investigations may proceed and will do so only after receiving guidance regarding the state secrets doctrine from the Ninth Circuit. The DOJ also asserted that nothing has occurred in the past year that warrants resuming these dockets. The DOJ warned that it would seek immediate injunctive relief if the Board should authorize discovery as to whether and to what extent carriers may have any relationship with the National Security Agency or whether the

---

33. AT&T comments at 7.

34. AT&T comments at 7. These include:

- examining whether disclosures of bulk call records are being made without determining the specific authority under which they have been made or the particular agency to which they are (suggestion made at recent status conference);
- asking carriers a 'hypothetical question' about what they would do if they were asked to make bulk disclosures to NSA in the absence of a warrant (suggestion from previous Board Order);
- examining whether the carriers should amend their privacy policies because "no evidence can be presented that they have violated their existing policies without violating the privilege."

35. AT&T comments at 10; *see* Verizon opposition at 2.

36. AT&T proposes that if a schedule is adopted, it provide that answers to information requests not be due until the later of 60 days after they are served or 30 days following the entry of a final and non-reviewable order denying a motion for a preliminary injunction. AT&T comments at 10.

37. Although the DOJ was invited to intervene, it has not done so and is not a party.

38. Nothing on the DOJ letter suggested that it had sent copies to the parties. On September 27, the Clerk of the Board sent a copy of the letter to all the parties.

carriers participated in an alleged call records program. Finally, if the Board decides to proceed, the DOJ requested adequate opportunity to seek injunctive relief and sufficient time for Judge Walker to consider such a request.

### **III. DISCUSSION**

Given the significant past delays in this proceeding, we have decided to allow discovery and to establish a schedule for further proceedings, albeit with a carefully limited scope.

#### **A. Scope**

These dockets were commenced many months ago. Since we have put these dockets on hold in deference to asserted federal claims, we have not exercised our authority under state law to determine whether the carriers have complied with Vermont law. Because these dockets have been on hold, this Board has declined or been unable to use its authority under state law to protect customer calling records from improper disclosure. This Board's supervisory authority extends to the customer privacy policies and practices employed by Vermont's regulated telecommunications companies.<sup>39</sup> Moreover, the Department of Public Service has been unable to obtain information about carrier practices, a function critical to its ability to adequately perform its responsibilities.<sup>40</sup>

Over the past year the federal courts have better defined the permissible scope of these state utility commission investigations. They have rejected a number of the government's claims, and they have found that states retain significant authority for consumer protection activities. For example, Judge Walker observed in *NSA Telecommunications Records Litigation* that FISA actually anticipates the application of state law remedies when a carrier discloses business records without proper authorization.<sup>41</sup> In the same opinion, Judge Walker noted that some questions posed in state investigations fall outside the scope of the state secrets privilege,<sup>42</sup> and, at least in

---

39. See PSB Rule 7.608 (effective 7/21/06) (setting forth privacy protections for customers of telecommunications companies providing service in Vermont).

40. See Order of 6/27/06 at 1.

41. *NSA Telecommunications Records Litigation*, slip op. at 11.

42. *Id.* at 18.

the context of conflict preemption analysis, state investigations will not inevitably conflict with federal law.<sup>43</sup>

Moreover, the recent carrier letters to Congress state that the companies are providing information to the government in a wide variety of circumstances, including some without judicial oversight. We seek to understand more about the nature of these practices, in large part so that we can determine whether the companies' privacy policies and practices should more accurately disclose the variety of the carriers' actual practices. Also, as we have previously noted, the state secrets privilege does not block consideration of whether Verizon's responses to the Department were misleading and inaccurate.<sup>44</sup>

The state secrets privilege issue is still pending in the Ninth Circuit Court of Appeals. We understand that all federal courts have previously disallowed discovery into matters allegedly protected by that privilege.<sup>45</sup> However, we do not understand the privilege to be so broad as to prevent general inquiries into the practices of telecommunications carriers in responding to requests from third parties for protected consumer information.

For these reasons, we define a narrow scope of issues for the current phase of these dockets, intending thereby to exclude all matters lying within the current claims of state secrecy.<sup>46</sup> Moreover, since this Board has all the powers of a court of public record for all matters within its jurisdiction,<sup>47</sup> we intend to exercise strict oversight of discovery.<sup>48</sup>

This phase of the docket may examine the following topics:

- (1) Current and recent written carrier policies regarding requests from the government for the release of customer records, including any policies describing when warrants, letters and certifications are prerequisite and when, if ever, they are not required, and associated records.

---

43. *Id.* at 13.

44. Order of 9/18/06 at 19-20.

45. *E.g.*, *ACLU v. NSA*, 493 F.3d 644, 687 (6th Cir. 2007).

46. If the state secrets claim is later invalidated, we will broaden the scope, and we will conduct a second phase of discovery and hearings if needed.

47. 30 V.S.A. § 9.

48. *See* PSB Rule 2.103 and 2.214 (adopting the Vermont Rules of Civil Procedure generally and discovery rules in particular for proceedings before the Board).

- (2) The carriers' actual practices in determining whether to comply with requests from the government for the release of customer records, including carrier record-keeping practices regarding both the government's requests and their own responses.<sup>49</sup>
- (3) The frequency with which the carriers have actually released customer records information to the government, the scope of those disclosures, the legal authority, if any, relied upon, and associated records, including unclassified national security letters or certifications required by statute or executive order.
- (4) The accuracy and sufficiency of the carriers' existing customer privacy notices regarding release of customer record information.
- (5) Whether past responses from the carriers to the Department or statements to the public were misleading and inaccurate.

We also want to ensure that nothing in these dockets encroaches on matters privileged by the state secrets doctrine, until the federal courts have ruled on that issue. Therefore, notwithstanding the preceding list, all of the following material is excluded from the current scope of these dockets:

- (A) Whether specific telecommunications carriers assisted the NSA with an alleged foreign intelligence program involving the disclosure of large quantities of records pertaining to customer communications;
- (B) If such a program exists, the precise nature of the carriers' alleged involvement and details concerning the NSA activities.<sup>50</sup>

If the federal courts should later invalidate the government's state secrets claim, we intend to expand the scope of these dockets to cover those matters as well.

---

49. Conceivably, a carrier might have multiple tracking and recording systems. For example, it may have one system for ordinary criminal and civil subpoenas, a second for disclosures made under the Pen Register Act, FISA and other similar statutes where the prerequisites to disclosure are public knowledge, and yet a third for "state secrets" matters that allegedly cannot even be discussed.

50. The description of the excluded items is intended to be identical to General Alexander's declaration defining the scope of state secrecy. See *NSA Telecommunications Records Litigation*, slip op. at 18.



We also emphasize that our inquiry in this phase will be limited to examining the practices of the carriers that are subject to our supervision. It is beyond the scope of this docket to examine in any respect the practices of the federal government, including how it may process information received from the carriers.

### **B. Bandler Discovery in Docket 7183**

On March 15, 2007, Docket 7183 Intervenor Michael Bandler, issued 27 interrogatories to Verizon. Those interrogatories generally covered two areas. The first set of questions concerned previous Verizon news releases, asking whether those news releases were true and reasonably complete and asking Verizon to define certain terms. Second, the interrogatories asked more general questions regarding how Verizon complies with the law. For example, they asked whether and when Verizon considers release of information to be "authorized by law absent an appropriate Court Order," and they asked how Verizon reaches such decisions. They asked what Verizon believes its obligations are when and if it releases information to a government agency that is not authorized by law. They asked whether and how Verizon might be prevented from truthfully denying participation in a "classified program." They asked specifically whether Verizon has within the last five years released information to a government agency that was not authorized by law. Finally, they asked Verizon how it safeguards customers' privacy when the legality of a governmental program is fairly debatable.

Verizon filed nine general objections, including preemption and overbreadth. Bandler filed a Motion to Compel on May 18, 2007, and Verizon filed its opposition on June 4, 2007, recommending denial. Verizon restated its earlier substantive objections, which in summary are that "federal law bars Verizon from disclosing" the information sought by Bandler, and it also "preempts the Board from requiring such disclosures."

After Verizon's response was filed, Judge Walker issued *NSA Telecommunications Records Litigation*, a significant decision that rejected some of the grounds asserted by Verizon, such as preemption. Moreover, Verizon's subsequent letter to Congress may have answered some of the factual questions propounded by Bandler, possibly eliminating the secrecy of some previously alleged state secrets. On or before November 14, 2007, Verizon shall file a revised

opposition statement to the pending motion updating its arguments in light of *NSA Telecommunications Records Litigation* and in light of Verizon's recent disclosures. Verizon shall, in particular, address whether it is possible for it to answer any or all of Mr. Bandler's second group of questions (involving Verizon's practices and policies) without violating the state secrets privilege.

#### **IV. ORDER**

IT IS HEREBY ORDERED, ADJUDGED AND DECREED by the Public Service Board of the State of Vermont that: the following schedule is established for the next phase of these dockets:

November 9, 2007	First round of discovery on carriers, copies served on all parties and DOJ <sup>51</sup>
November 23	Responses due
December 7	Second round of discovery, copies served on all parties and DOJ
December 21	Responses due
January 11, 2008	Petitioners file testimony
January 25	First round of discovery on petitioners
February 8	Responses due
February 22	Second round of discovery on petitioners
March 7	Responses due
March 21	Carriers file rebuttal testimony
March 28	Third round of discovery on petitioners
April 11	Responses due

Technical hearings and briefing schedules will be determined at a later time.

---

51. Copies of discovery requests shall be filed with Carl J. Nichols, Deputy Assistant Attorney General, Civil Division, United States Department of Justice, Washington D.C. 20530.



**CONCURRENCE OF JOHN D. BURKE**

While I am willing to concur today in the decision of my colleagues as to the extent of discovery in this docket, I would have gone further. Specifically, I would have allowed discovery as to whether specific telecommunications carriers assisted the NSA with an alleged foreign intelligence program involving the disclosure of large quantities of records pertaining to customer communications. I agree with my colleagues' decision, however, to limit, for the time being, inquiry as to the precise nature of the carriers' alleged involvement and details concerning the NSA activities.

Our Constitution should be viewed in its historic context. When the Constitution was drafted its authors were mindful of what they perceived as an abrogation of individual rights foisted on their immediate forefathers. Many of them had knowledge of their fathers or grandfathers being jailed as a result of body writs, sometimes for years, without charges being brought, and even when they were charged, it was often the result of an ex post facto enactment. Thus the authors' bias was for strong protection of individual rights and liberties. The right to privacy is such an individual right which is entitled to the same protection. It is not the alleged request by a government agency for such information that is at issue here. Rather, it is the companies' alleged compliance with that request for such material that would be problematic.

If these allegations are proven true, the citizens and ratepayers of our state should have the right to attempt to obtain redress from those who provided such information.

There has been so much publication of the possibility of such activity, it is hard to believe that the "evildoers" aren't aware of the potential peril of using this voice communication system. Thus there is no "secret" for the states secret doctrine to protect. If this activity occurred, there are only the interests of Verizon and AT&T to protect in this docket. I would let our citizens and ratepayers know what happened, if anything, and let them pursue any remedies they might find appropriate if this activity did occur.

Dated at Montpelier, Vermont, this 31<sup>st</sup> day of October, 2007.

s/John D. Burke

John D. Burke, Board Member

PORTLAND OFFICE  
eleventh floor  
121 sw morrison street  
portland, oregon 97204-3141  
TEL 503 228 3939 FAX 503 226 0259

OTHER OFFICES  
beijing, china  
new york, new york  
seattle, washington  
washington, d.c.  
GSBLAW.COM

G A R V E Y S C H U B E R T B A R E R

Please reply to MARK E. FRIEDMAN  
mfriedman@gsblaw.com TEL EXT 3126

September 8, 2006

Gregory M. Romano  
Verizon Northwest Inc.  
1800 41st Street  
Everett, WA 98201

Dear Mr. Romano:

The ACLU of Oregon appreciates your cooperation in agreeing to an extension of time for its response to Administrative Law Judge Arlow's July 31, 2006 ruling. As we stated in our motion for extension of time, as an alternative to immediately proceeding before the PUC, we are suggesting an informal approach. Kindly respond in writing to the questions we are raise in this letter. Your clear responses may be helpful for us in determining whether it is necessary for our client to proceed before the PUC.

The questions in this letter address some of our client's principal concerns related to activities of certain telecommunications companies in Oregon, including your client/employer. We were granted an extension to September 22, 2006. Therefore, we would appreciate having your letter response by no later than September 18.

1. Has Verizon Northwest Inc. 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?

If that has ever occurred, under what authority were such intrastate telecommunications contents disclosed, provided or revealed to or obtainable by any person or entity, public or private?

2. Has Verizon Northwest Inc. 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?


If that has ever occurred, under what authority was information about or data describing the intrastate telecommunication activity of Oregon telecommunications customers disclosed, provided or revealed to or obtainable by any person or entity, public or private?

Thank you very much for your considered responses to these questions.

Sincerely,

GARVEY SCHUBERT BARER

By

  
Mark E. Friedman  
Keith S. Dubanevich

MEF:mkf

cc: ACLU of Oregon

PDX\_DOCS:378856.6  
09/8/06 2:48 PM