

United States District Court
For the Northern District of California

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:

Clayton et al v AT&T Communications
of the Southwest, Inc, et al, C 07-
1187; United States v Clayton, C
07-1242; United States v Reishus, C
07-1323; United States v Farber, C
07-1324; United States v Palermino,
et al, C 07-1326; United States v
Volz, et al, C 07-1396

In 2006, the United States filed lawsuits seeking to enjoin state officials in Maine, New Jersey, Connecticut, Vermont and Missouri 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. These cases, together with a subpoena enforcement action brought by the same Missouri officials who are defendants in the United States'

1 injunction case concerning that state,¹ were transferred to this
2 court by the Judicial Panel on Multidistrict Litigation (JPML) on
3 February 15, 2007, with cross motions for dismissal and/or summary
4 judgment pending.

5 The court denied those motions by order dated July 24,
6 2007 (Doc #334); 2007 WL 2127345. The court held that the states'
7 investigations into wiretapping activities did not violate the
8 doctrine of intergovernmental immunity, were not preempted by
9 federal statutes and did not infringe on the federal government's
10 power over foreign affairs to a constitutionally impermissible
11 degree. Doc #334 at 16-34; 2007 WL 2127345 at *8-*14. As to the
12 government's argument based on the state secrets privilege (SSP),
13 the court noted that the Ninth Circuit might well provide useful
14 guidance when it ruled on the government's appeal in Hepting v AT&T
15 Corp, 439 F Supp 2d 974 (ND Cal 2006), which was then pending
16 before it. Accordingly, the court denied the government's motion
17 based on the SSP without prejudice to its renewal following the
18 Ninth Circuit's decision in Hepting. Doc #334 at 35; 2007 WL
19 2127345 at *15.

20 In the interim, two important developments have altered
21 the posture of these cases. Congress enacted, on July 10, 2008,
22 _____

23 ¹ Clayton et al v AT&T Communications of the Southwest, Inc, et
24 al, C 07-1187, is "a subpoena enforcement action brought by the state
25 defendants in [Clayton] that * * * presents facts and issues identical
26 to those raised by [Clayton]." Doc #536 at 6 n 2. Because of the
27 different posture of Clayton, plaintiff Robert Clayton has both joined
28 in the briefs filed by the state officials in all six cases and has
filed a separate opposition and surreply on the United States' motion.
Doc ##592, 602. The telecommunications carrier defendants therein
have also filed a motion to dismiss a pending application to compel
production of documents and to compel witnesses to appear and answer
questions in Clayton. Doc #594. That motion is rendered moot by the
court's rulings on the United States' motions.

1 the FISA Amendments Act of 2008, Pub L No 110-261, 122 Stat 2436
2 (FISAAA), which contains a provision, section 803 (codified at 50
3 USC § 1885b), that the United States contends requires dismissal of
4 all six of these actions. Then, the following month, the Ninth
5 Circuit remanded Hepting v AT&T without rendering a decision "in
6 light of the FISA Amendments Act of 2008." Docket No 06-17137 (9th
7 Cir), order dated August 21, 2008.

8
9 I

10 The following summary of the six underlying state
11 proceedings sets forth certain salient procedural events specific
12 to each case as reflected in documents filed in this court.

13
14 A

15 The Maine case, United States v Adams (now Reishus),
16 C 07-1323, began after Maine citizen James Cowrie petitioned the
17 Maine Public Utilities Commission (MePUC) to investigate whether
18 Verizon had shared its customers' records with the NSA. Verizon
19 responded that it could neither admit nor deny involvement in
20 national security matters, but included seven "affirmative
21 assertions of fact," including the following representations:

- 22 1. Verizon was not asked by NSA to provide, nor did
23 Verizon provide, customer phone records from any of
24 its businesses, or any call data from those records.
25 2. None of these companies — wireless or wireline —
26 provided customer records or call data.
27 3. Verizon's wireless and wireline companies did not
28 provide to NSA customer records or call data, local
or otherwise.

See Doc #536-2 (Ex A) at 38. On August 9, 2006, MePUC issued an

1 order reciting the seven representations and noting that "if [they]
2 are in fact true, such statements could satisfy the concerns raised
3 in the complaint." Id at 39. The order went on to state, however,
4 that "[i]n order to fulfill our duty to consider whether to open an
5 investigation * * * we find that we require as to each of the seven
6 representations set forth above a sworn affirmation that such
7 representation is true and not misleading in light of the
8 circumstances in which it is made." Id. MePUC has not asked for
9 any additional information from Verizon. On August 21, 2006, the
10 government sued in the United States District Court for the
11 District of Maine to enjoin the MePUC from pursuing this inquiry.
12 On February 8, 2007, Judge Woodcock preliminarily enjoined MePUC
13 from enforcing the order. See United States v Adams, 473 F Supp 2d
14 108 (D Me 2007).

15 The New Jersey case, United States v Rabner (now Farber),
16 C 07-1324, was filed in response to the New Jersey Attorney
17 General's issuance of subpoenas duces tecum to the
18 telecommunication carriers named in the complaint (Civil Docket No
19 C 07-1324, Doc #1-1 (Complaint)), of which the following document
20 requests are, according to the United States, representative:

- 21 1. All names and complete addresses of Persons including,
22 but not limited to, all affiliates, subsidiaries and
23 entities, that provided Telephone Call History Data to
the NSA. * * *
- 24 2. All Executive Orders issued by the President of the
25 United States and provided to Verizon Concerning [sic]
any demand or request to provide Telephone Call History
Data to the NSA.
- 26 3. All orders, subpoenas and warrants issued by or on
27 behalf of any unit or officer of the Executive Branch
of the Federal Government and provided to Verizon
28 Concerning [sic] any demand or request to provide
Telephone Call History Data to the NSA.

United States District Court
For the Northern District of California

1 4. All orders, subpoenas and warrants issued by or on
2 behalf of any Federal or State judicial authority and
3 provided to Verizon Concerning [sic] any demand or
request to provide Telephone Call History Data to the
NSA.

4 Doc #536-2 (Ex A) at 12.

5 United States v Palermino, C 07-1324, was filed in
6 response to an investigation by the Connecticut Department of
7 Public Utility Control (CtDPUC), prompted by a complaint filed by
8 the American Civil Liberties Union of Connecticut (ACLU), into
9 whether the local carriers violated Connecticut law. Quoted below
10 are three of the approximately thirty interrogatories the ACLU
11 propounded to AT&T in the Connecticut proceeding:

12 ACLU-5 Has AT&T at any time during the Relevant Period
13 disclosed customer information and/or records to
14 private parties, government entities and/or law
15 enforcement personnel when not compelled to do so
by subpoena, warrant, court order or a request
under 18 USC § 2709 ("National Security Letter" or
"NSL")?

16 * * *

17 ACLU-5b If your response to ACLU-5 is yes, provide full
18 details of each occasion on which AT&T disclosed
19 customer information and/or records to private
20 parties, government entities and/or law
21 enforcement personnel when not compelled to do so
by subpoena, warrant, court order or NSL,
including the date of each request, the
information sought, the information provided, and
the date on which the information was provided.

22 * * *

23 ACLU-9 Has AT&T at any time during the Relevant Period
24 disclosed customer information and/or records to
25 law enforcement or government personnel in
response to an NSL?

26 Doc #536-2 (Ex A) at 31-32.

27 United States v Volz, C 07-1396, was filed in response to
28 identical information requests propounded to AT&T and Verizon

United States District Court
For the Northern District of California

1 concerning their conduct and policies vis-à-vis the NSA by the
2 commissioner of the Vermont Department of Public Service (VtDPS).

3 Doc #536-2 (Ex A) at 15-17. The requests asked, inter alia:

4 1. Has AT&T disclosed or delivered to the [NSA] the phone
5 call records of any AT&T customers in Vermont at any time
6 since January 1, 2001? If any such disclosures occurred
7 prior to the date specified, please provide the date on
8 which the disclosures commenced.

9 2. If the answer to the preceding question is yes, please
10 identify the categories of information AT&T provided to
11 the NSA, including the called and calling parties'
12 numbers; date of call; time of call; length of call; name
13 of called and calling parties; and the called and calling
14 parties' addresses.

15 * * *

16 7. Please state how many AT&T customers have had their
17 calling records disclosed or turned over to the NSA or
18 any other governmental entity, on an agency-by-agency
19 basis, since the inception of the disclosures? Please
20 separate the total into business and residential
21 customers.

22 8. State whether the disclosures of AT&T Vermont customer
23 call information to the NSA and/or any state or federal
24 agency is ongoing.

25 9. State the number of occasions that AT&T has made such
26 disclosures.

27 Doc #536-2 (Ex A) at 15-16. AT&T refused to respond initially and
28 did not do so until October 2, 2006. Doc #624-2 at 2-3. Verizon
submitted detailed responses that explicitly excluded any

information pertaining to "its cooperation, if any, with the NSA
and any similar intelligence gathering activities." Doc #596-9.

Seeking a response from AT&T and more complete responses from
Verizon in response to the May 17, 2006 requests, VtDPS petitioned
the Vermont Public Service Board (VtPSB) to open investigations of
the carriers (e g Doc #596-7 (Ex F)); in September 2006, the VtPSB
ordered the carriers to respond. Doc #596-8 (Ex G); Doc #536-2 (Ex

1 A) at 18-19. On October 2, 2006, the United States filed suit to
2 enjoin the investigation. Doc #601-2 at 2.

3 According to the factual recital in an order promulgated
4 by the VtPSB, the state proceedings then "remained largely dormant"
5 pending the outcome of the federal proceedings. Doc #601-2 at 3.
6 After this court issued its July 24, 2007 order denying the United
7 States' motion to dismiss and, in October 2007, the VtDPS provided
8 to the VtPSB letters written by Verizon and AT&T to members of
9 Congress that "acknowledged that they provided customer information
10 to law enforcement officials in a wide variety of contexts." Id.
11 After taking briefing from the parties as to whether the state
12 proceeding "should be reactivated," the VtPSB entered, on October
13 31, 2007, a "Procedural Order" which stated "[W]e have decided to
14 allow discovery and to establish a schedule for further
15 proceedings, albeit with a carefully limited scope." Id at 9.

16 The order noted, discussing this court's July 24, 2007
17 opinion, that "some questions posed in state investigations fall
18 outside the scope of the [SSP]," that "state investigations will
19 not inevitably conflict with federal law" and that it did "not
20 understand the privilege to be so broad as to prevent general
21 inquiries into the practices of telecommunications carriers in
22 responding to requests from third parties for protected consumer
23 information." Id at 9-10. It explained the purpose of its renewed
24 inquiry thusly:

25 [T]he recent carrier letters to Congress state that
26 the companies are providing information to the
27 government in a wide variety of circumstances,
28 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

1 should more accurately disclose the variety of the
2 carriers' actual practices. Also, as we have
3 previously noted, the [SSP] does not block
4 consideration of whether Verizon's responses to the
5 Department were misleading and inaccurate.

6 Id.

7 On August 8, 2008, counsel for the VtDPS wrote two letters
8 to the VtPSB — one pertaining to the Verizon proceeding, the other
9 pertaining to the AT&T proceeding. Both contained the following
10 conclusion about the impact of FISAAA section 803:

11 The Department has reviewed the recent FISA amendments
12 as well as the various discovery responses received from
13 AT&T[/Verizon] to date and has reluctantly concluded
14 that the amendments passed by Congress and signed into
15 law by President Bush appear to preclude further
16 investigation into the activities which initially gave
17 rise to this proceeding.

18 * * *

19 [T]he Department notes that the FISA amendments are the
20 subject of a number of legal challenges. Therefore,
21 whatever disposition the Board decides is appropriate
22 for this proceeding, the Department recommends that it
23 be undertaken without prejudice to the ability of the
24 Department or any other complaining party to refile
25 should the legal landscape change in the future.

26 Doc #624-2 at 2-5. The letter recommended the assessment of
27 disciplinary fines against AT&T for its refusal to respond to the
28 "non-security related requests" between May 25 and October 2, 2006.
29 Id at 3. As to Verizon, the letter stated "the Department does not
30 believe there is any basis for continuing this matter." Id at 4.
31 The record before the court contains no documents dated after the
32 two August 8, 2008 letters pertinent to the Vermont proceedings. It
33 may be assumed from the posture of the proceedings in the federal
34 case, however, that VtPSB has not followed VtDPS's suggestion that
35 it terminate its investigations.

36 \\

United States District Court
For the Northern District of California

1 Clayton v AT&T, C 07-1187, arises out of investigative
2 subpoenas issued to AT&T by commissioners of the Missouri Public
3 Service Commission (MoPSC) regarding information AT&T allegedly
4 disclosed to the NSA. Doc #536-2 (Ex A). The subpoenas seek, for
5 example:

6 (1) The number of Missouri customers, if any, whose calling
7 records have been delivered or otherwise disclosed to
8 the [NSA] and whether or not any of those customers were
9 notified that their records would be or had been so
10 disclosed and whether or not any of those customers
11 consented to the disclosure;

* * *

12 (3) The nature or type of information disclosed to the NSA,
13 including telephone number, subscriber name and address,
14 social security numbers, calling patterns, calling
15 history, billing information, credit card information,
16 internet data and the like.

17 Id at 22.

18 Because the commissioners considered AT&T's response
19 inadequate, they moved pursuant to Missouri law to compel AT&T to
20 comply with the investigation in Missouri state court. AT&T then
21 removed the case to the United States District Court for the
22 Western District of Missouri. Shortly thereafter, the government
23 filed United States v Gaw (now Clayton), 07-1242, on July 26, 2006,
24 seeking declaratory and injunctive relief against the MoPSC and
25 AT&T. The telecommunications carrier defendants in Clayton v At&T
26 have moved to dismiss Clayton's pending application to compel
27 production of documents and to compel witnesses to appear and
28 answer questions. Doc #594. The United States moves for summary
judgment in both Clayton cases.

\\

\\

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

B

Section 803, part of FISAAA's Title II under the headings "Protections for Electronic Communication Service Providers" and "procedures for implementing statutory defenses under [FISA],"² provides as follows:

SEC 803. PREEMPTION.

(a) IN GENERAL. —

No State shall have authority to —

(1) conduct an investigation into an electronic communication service provider's alleged assistance to an element of the intelligence community;

(2) require through regulation or any other means the disclosure of information about an electronic communication service provider's alleged assistance to an element of the intelligence community;

(3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or

(4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.

(b) SUITS BY THE UNITED STATES. —

The United States may bring suit to enforce the provisions of this section.

(c) JURISDICTION. —

The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this section.

(d) APPLICATION. —

This section shall apply to any investigation, action, or proceeding that is pending on or commenced

² This provision is codified at 50 USC § 1885 (definitions), 50 USC § 1885a (procedures for implementing statutory defenses), 50 USC § 1885b (preemption) and 50 USC § 1885c (reporting).

1 after the date of the enactment of the FISA Amendments
2 Act of 2008.

3 Section 703 (50 USC § 1881) defines "intelligence community" to
4 have the meaning given the term in section 3(4) of the National
5 Security Act of 1947 (50 USC § 401a(4)). That section defines
6 "intelligence community" to include fifteen enumerated federal
7 agencies and offices including the NSA and to provide for certain
8 officials including the president to designate additional
9 departments or agencies as "element[s] of the intelligence
10 community."

11 The United States submitted with its reply brief the
12 October 26, 2007 report of the Senate Select Committee on
13 Intelligence to accompany Senate Bill 2248 (SSCI Report), S Rep No
14 110-209, 110th Cong, 1st Sess (2007). Doc # 596-2 (Ex A). Senate
15 Bill 2248 was the original Senate bill that, together with the
16 House bill (H 3773), resulted in the compromise legislation that
17 ultimately passed both houses on July 8, 2008 (H 6304). See FISA
18 Amendments of 2008, HR 6304, Section-by-section Analysis and
19 Explanation by Senator John D Rockefeller IV, Chairman of the
20 Select Committee on Intelligence. Doc #469-2 at 51.

21 The SSCI Report listed among the committee's
22 recommendations for legislation amending FISA, "narrowly
23 circumscribed civil immunity should be afforded to companies that
24 may have participated in the President's program based on written
25 requests or directives that asserted the program was determined to
26 be lawful." Doc #596-2 at 3. The SSCI Report included a lengthy
27 summary of the instant MDL cases, of which the following excerpt
28 concerns the cases that are the subject of the instant motions:

United States District Court
For the Northern District of California

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

BACKGROUND ON PENDING LITIGATION

* * *

STATE REGULATORY INVESTIGATIONS

In addition to the civil declaratory judgment and damages suits, a number of state public utilities commissions have opened investigations of electronic communication service providers for their alleged provision of assistance to the intelligence community. These public utilities commissions are seeking to investigate whether the companies violated state privacy rights by providing customer records to agencies of the federal government.

The federal government filed suit seeking to enjoin state officials in five states from further investigation of electronic communication service providers for their alleged disclosure of customer telephone records to the National Security Agency. These cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California in February 2007. In July 2007, the district court found that these state investigations were not preempted by either the Supremacy Clause or the foreign affairs power of the federal government.

The Government may yet prevail in preventing state regulatory investigations of whether particular providers furnished customer records to the intelligence community. But, like the civil suits filed against providers, the outcome of this litigation is uncertain and will likely involve further protracted proceedings.

Doc #569-2 at 7-8.

PREEMPTION

Section 204 of the bill preempts state investigations or required disclosure of information about the relationship between individual electronic communication service providers and the intelligence community. The provision reflects the Committee's view that, although states play an important role in regulating electronic communication service providers, they should not be involved in regulating the relationship between electronic communication service providers and the intelligence community.

Doc #569-2 at 12.

[S]ection 204 provides for the protection, by way of preemption, of the federal government's ability to conduct intelligence activities without interference by state investigations.

1 Doc #569-2 at 13.

2 Section 204. Preemption of state investigations

3 Section 204 adds a Section 803 to the new Title VIII.
4 It addresses investigations that a number of state
5 regulatory commissions have or might begin to
6 investigate cooperation by state regulated carriers
7 with US intelligence agencies. Section 803 preempts
8 these state investigations by prohibiting them and
9 authorizing the United States to bring suit to enforce
10 the prohibition.

11 Doc #569-2 at 23-24.

12 II

13 The United States moves for summary judgment in all six
14 cases on the single ground that section 803 expressly preempts the
15 state investigations that the United States has sought to enjoin by
16 means of these actions. Doc #536. The United States asserts that
17 section 803 is a valid exercise of the federal government's power
18 under the Supremacy Clause and that "state laws or activities are
19 expressly preempted when there is an explicit federal statutory
20 command that they be displaced." Id at 7-8.

21 The United States contends that all of the state
22 proceedings, including the various subpoenas, administrative orders
23 and interrogatories issued by the five states at issue in these
24 motions, are "investigation[s] into an electronic service
25 provider's alleged assistance to an element of the intelligence
26 community" barred by the new section 803(a)(1) and/or attempts to
27 "require through regulation or any other means the disclosure of
28 information about an electronic communication service provider's
alleged assistance to an element of the intelligence community"
prohibited by section 803(a)(2). Doc #536 at 10. On this basis,
the United States seeks a declaration that section 803 preempts the

1 state investigations at issue, a permanent injunction against the
2 state investigations and summary judgment in its favor. Id at 11.

3 Defendant state officials (and plaintiff Clayton) oppose
4 the United States' motion (Doc #590), as do intervenors "James
5 Cowie et al," a number of Maine telephone customers represented by
6 the Maine Civil Liberties Union (Doc #591). The state officials
7 make two major contentions in opposition. First, they contend that
8 section 803 is unconstitutional and therefore unenforceable because
9 it infringes on states' sovereign powers, "including those embodied
10 in the Tenth Amendment." Doc # 590 at 6. Second, they contend
11 that section 803's plain language does not purport to preempt all
12 aspects of the states' "investigations" (this term is in
13 quotation marks in the states' joint brief). Id. They contend
14 that many of the challenged actions are not "investigations" of the
15 type prohibited by section 803 but are either attempts to determine
16 whether an investigation is warranted or inquiries pertaining to
17 the telecommunications companies' policies regarding the treatment
18 of customer information, such as privacy policies and policies
19 regarding the disclosure of such information to law enforcement
20 agencies. Id at 19-22.

21 Whereas the United States' previous motion for summary
22 judgment in these cases was concerned in large part with
23 unsuccessfully attempting to establish federal preemption in the
24 absence of an express statute (see order of July 24, 2007, Doc #334
25 at 19-34; 2007 WL 2127345 at *8-15, the United States now has in its
26 corner a statute that purports to preempt state laws expressly in
27 regards to the matters it concerns. The states contend, however,
28 \\

1 that section 803 is "an unconstitutional encroachment on state
2 sovereignty." Doc #590 at 9.

3 The states rely on Printz v United States, 521 US 898
4 (1997), in which the Supreme Court struck down provisions of the
5 Brady Handgun Violence Prevention Act that required state law
6 enforcement officials to conduct background checks on handgun
7 purchasers (portions of 18 USC § 922). The Printz opinion examined
8 the Constitution's structure with reference to historical sources
9 such as the Federalist Papers in determining that under the United
10 States' system of "dual sovereignty," the states retained "a
11 residuary and inviolable sovereignty." Id at 918-19. The Printz
12 court also relied on more recent Supreme Court jurisprudence
13 examining federal laws that impose requirements on state
14 governments, especially New York v United States, 505 US 144 (1992)
15 (also cited by state defendants here), holding that federal
16 legislation exceeded the federal government's powers when it
17 required states either to enact legislation providing for the
18 disposal of radioactive waste generated within their borders or to
19 take title to, and possession of, the waste because "the Federal
20 Government may not compel the States to enact or administer a
21 federal regulatory program." 505 US at 188, cited at 521 US at 926.

22 While acknowledging that this case is unlike Printz in
23 that the federal law at issue is not mandatory on state officials
24 but rather prohibitory (Doc #590 at 13), state defendants argue that
25 "the regulation of utilities is one of the most important of the
26 functions traditionally associated with the police power of the
27 States," quoting Arkansas Electric Cooperative Corp v Arkansas
28 Public Service Comm'n, 461 US 375, 377 (1983) as is protecting the

1 privacy of states' citizens, citing this court's July 24, 2007 order
2 (at 33, 2007 WL 2127345 at 14). Doc #590 at 12. On this basis,
3 they argue, federal interference is especially problematic.

4 State defendants' constitutional challenge to section 803
5 rests on three major arguments: (1) section 803, by prohibiting
6 states from acting to protect the interests of their own citizens,
7 erodes state sovereignty and "confuses the paths of political
8 accountability" (doc #590 at 12, 14); (2) section 803 is especially
9 problematic because of its "sweeping, indeterminate language"
10 barring "any" state investigation into even "alleged assistance" by
11 telecommunications companies to intelligence agencies and preventing
12 states from requiring disclosure through "any means" (id at 15); and
13 (3) section 803 suffers in comparison to section 802 because it
14 lacks the "procedural safeguards" and "balancing of interests"
15 embedded in section 802 such as the requirement of a certification
16 of facts by the Attorney General, judicial review by means of the
17 substantial evidence standard and provisions allowing parties to
18 participate in the judicial process (Doc #590 at 17).

19 The states also contend that at least some of the state
20 investigations or actions have been reconfigured in light of the
21 suits by the United States threatening injunctive relief and the
22 enactment of FISAAA to avoid directly inquiring about NSA
23 wiretapping activities. For example, they assert that in the
24 Vermont proceeding, the VtPSB "explicitly excluded from the scope of
25 the docket any inquiry into assistance provided by the carriers to
26 the NSA involving disclosure of customer records." Doc #601 at 3.
27 They assert that in its briefing on the instant motion, the United
28 States ignores the states' attempts to avoid trenching on areas of

1 federal authority and instead "fixat[es] on the original information
2 requests, several of which did explicitly reference the NSA," thus
3 creating "a straw man, which it then attacks by arguing that the
4 States have refused to 'limit their inquiries to matters that
5 clearly do not implicate national security activities.'" Id at 4-5.
6 At oral argument, they asserted that the proper approach for the
7 court to take in applying section 803 to the pending state
8 investigations is to "parse through the individual inquiries and
9 decided which * * * are covered by 803 and which aren't." RT (Doc
10 #621) at 41:7-9; see also 47:24-48:3.

11 The United States argues, by contrast, that section 803
12 presents no constitutional problem because: (1) the Tenth Amendment
13 is inapplicable because no power is reserved to the states in
14 connection with powers "delegated to the United States by the
15 Constitution" including national security and foreign affairs;
16 (2) nothing prevents the United States from preempting state
17 authority to regulate utilities, with or without a national security
18 justification; (3) the concepts discussed in Printz are not relevant
19 because there is no federal "commandeering" of state officials here
20 and it is constitutionally permissible for the federal government to
21 "impose preconditions to continued state regulation of an otherwise
22 pre-empted field" (citing FERC v Mississippi, 456 US 742 (1982)).
23 Doc #596 at 6-10. As for the states' critiques of section 803 such
24 as overbreadth and lack of procedural safeguards, the United States
25 merely asserts that these are not legally relevant to the court's
26 analysis. Id at 10-11. In essence, the United States contends that
27 even a clumsily-drafted federal statute may constitutionally preempt
28 state regulation.

1 As for the scope of section 803's preemptive reach in
2 these proceedings, the United States argues that it is broad,
3 encompassing the investigations in their entirety. The United
4 States accuses the states of "cherry picking" aspects of their
5 inquiries that do not directly concern national security in arguing
6 against dismissal. Doc #596 at 12. The United States invokes the
7 concepts of field and conflict preemption in arguing that Congress
8 intended to "cover the field," leaving no supplemental role for the
9 states. Id at 17 n 7. The United States argues that section 803
10 does not allow the "parsing" of interrogatories advocated by the
11 states because the very investigations at issue are prohibited, RT
12 (Doc #12) at 12: 10-17, but that, "if in the future there is an
13 inquiry that the states wish to make that does not concern an
14 alleged federal intelligence activity, there is nothing that would
15 be an obstacle to that." Id at 12:24-13:2.

16 The court agrees with the United States: section 803 does
17 not violate the Tenth Amendment because it does not "commandeer"
18 state officials; rather, it prohibits them from investigating
19 certain activities initiated by federal agencies that are
20 "element[s] of the intelligence community." Because intelligence
21 activities in furtherance of national security goals are primarily
22 the province of the federal government, Congressional action
23 preempting state activities in this context is especially
24 uncontroversial from the standpoint of federalism.

25 The court also agrees with the United States that the
26 appropriate remedy is to enjoin all of the investigations at issue
27 in these cases. The documents submitted to the court leave no doubt
28 that all of the investigations were initiated for the purpose of

1 delving into alleged electronic surveillance activities initiated by
2 the NSA. While it is true that some of the individual questions
3 propounded in each inquiry do not directly concern national
4 security, the remedy proposed by the states — suppressing only
5 those that make mention of national security topics while allowing
6 the rest to go forward — would be a pointless exercise that is not
7 without substantial cost both to the telecommunications companies
8 affected and to the states themselves. More importantly, the
9 “parsing” of interrogatories requested by the states does not appear
10 to be the role for the federal courts that Congress envisioned in
11 enacting section 803. Section 803(a)’s prohibition on “conduct[ing]
12 an investigation into an electronic communication service provider’s
13 alleged assistance to an element of the intelligence community,” is
14 broader than barring certain questions. There is simply no getting
15 around the fact that the purpose of each of the state proceedings at
16 issue in these cases was and is to find out about the
17 telecommunications companies’ cooperation with an “element of the
18 intelligence community.”

19 As the United States has stated herein, should any state
20 launch a new investigation not prompted by events or allegations
21 prohibited by section 803 to which the facially innocuous
22 interrogatories and information requests herein are relevant,
23 nothing bars the state from propounding those very questions in that
24 new inquiry. In this context, however, even the “innocuous”
25 interrogatories and information requests must be enjoined.

26 Turning at last to the separate issues presented by
27 Clayton v AT&T, C 07-1187, plaintiff Clayton opposes the United
28 States’ motion on the additional ground that the United States has

1 never intervened in, and is not otherwise a party to, that action
2 and therefore is not in a position to move for summary judgment.
3 Doc #592 at 2-3. He also argues that: even if given leave to
4 intervene, the United States' role would be limited, under 28 USC §
5 2403(a), to presenting arguments and evidence regarding the
6 constitutionality of FISAAA (id at 3-5); section 803 is inapplicable
7 because it provides for enforcement by the United States only by
8 "bring[ing] suit" (id at 5-6); and while section 802 (codified at 50
9 USC § 1885a) appears to be the proper vehicle under which the United
10 States could seek dismissal, the United States has not invoked
11 section 802. Id at 6-9.

12 The United States brushes off as "insubstantial"
13 Missouri's argument that the United States must intervene in order
14 to seek the dismissal of Clayton v AT&T, contending that the entry
15 of judgment in United States v Clayton would moot the state
16 officials' attempts to enforce their subpoenas in Clayton v AT&T.
17 Doc # 596 at 17-18. Alternatively, the United States argues that
18 the court "can and should treat the Government's motion as one for
19 intervention" under FRCP 24 because the case is in its early stages,
20 section 803 confers the enforcement role on the United States and
21 there is no prejudice to the Clayton v AT&T plaintiffs as they are
22 the defendants in the related action. Id at 18.

23 The court agrees with the United States that requiring a
24 separate motion for intervention is unwarranted and that section 803
25 bars the underlying proceeding at issue. Because plaintiff Clayton
26 has brought the action in question in his capacity as a state
27 official, the action is barred by section 803(a)(4) ("No state shall
28 have authority to * * * commence or maintain a civil action or other

United States District Court
For the Northern District of California

1 proceeding to enforce a requirement that an electronic communication
2 service provider disclose information concerning alleged assistance
3 to an element of the intelligence community"), section 802 does not
4 apply. The United States is authorized to bring suit to enforce
5 section 803 and has already done so in United States v Clayton.
6 Under section 803(a)(4), Clayton v AT&T cannot be maintained and is
7 hereby DISMISSED.

8
9 III

10 The United States' motion for summary judgment in United
11 States v Clayton, C 07-1242; United States v Reishus, C 07-1323;
12 United States v Farber, C 07-1324; United States v Palermino, et al,
13 C 07-1326; United States v Volz, et al, C 07-1396 is GRANTED. The
14 state proceedings at issue in each of those cases are prohibited by
15 section 803 (50 USC § 1885b) and are hereby enjoined pursuant to
16 this court's authority under that statute. Clayton et al v AT&T
17 Communications of the Southwest, Inc, et al, C 07-1187 is DISMISSED
18 with prejudice.

19 The United States is directed to submit a proposed form of
20 judgment in accordance with this order.

21
22 IT IS SO ORDERED.

23
24 

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