BEFORE THE WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

IN RE: ACLU REQUEST FOR AN INVESTIGATION OF UNLAWFUL DISCLOSURE OF PRIVATE TELECOMMUNICATION CUSTOMER INFORMATION (CPNI)	**DOCKET NO. UT-060856**

INITIAL COMMENTS OF PUBLIC COUNSEL

June 30, 2006

I. INTRODUCTION

1. The Public Counsel Section of the Washington State Attorney General's Office (Public Counsel) files these comments with the Washington Utilities and Transportation Commission (WUTC or Commission) in response to the June 2, 2006, Notice of Comment Opportunity in the above captioned docket. Public Counsel appreciates the attention the Commission has given to this very important issue and we hope these comments will assist the Commission in its deliberations.

2. Prior to addressing the specific questions contained in the June 2 Notice, this memorandum will review WUTC rulemaking on telecommunications privacy issues, public information available about the National Security Agency (NSA) program, and significant legal issues raised by this matter.

II. BACKGROUND

A. Procedural History.

1. ACLU Request for Investigation.

3. On May 25, 2006, the American Civil Liberties Union of Washington Foundation (ACLU) asked the WUTC to open an investigation into possible violations of law or rule stemming from the then recently-publicized allegations that a number of telephone companies released certain customer calling information to the United States Government, at the government's request.

2. Open Meeting.

4. In response to the ACLU's request, the Commission docketed the matter as Docket No. UT-060856 and scheduled the request for preliminary consideration at the Commission's May

ATTORNEY GENERAL OF WASHINGTON
Public Counsel
900 4th Ave., Suite 2000
Seattle, WA 98164-1012

31, 2006, Open Meeting. The WUTC received a number of comments, including those of Public Counsel, the ACLU, and AT&T.

3. Opportunity to Comment.

5. On June 2, 2006, the Commission issued a Notice of Comment Opportunity allowing for initial comments by June 30, 2006, and answering comments by July 17, 2006. The Notice asked five questions related to the "threshold legal and jurisdictional issues relevant to the request for investigation." Interested parties were asked to address these questions. These are Public Counsel's initial comments.

B. History of WUTC Activity Related to Customer Proprietary Network Information.

6. The WUTC first protected Customer Proprietary Network Information (CPNI)[1] in 1997, by prohibiting its use for marketing purposes.[2] In 1999, the Commission replaced that rule with rules identical in substance to those adopted by the FCC in 1998.[3] After the rules were partly invalidated in *U. S. West, Inc. v. Federal Communications Comm'n*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied sub nom. Competition Policy Inst. v. U. S. West*, 530 U.S. 1213 (2000), the FCC revised its rules to comply with the court decision. Significantly, the FCC left open to state public utility commissions the option of imposing more stringent rules based on their "particular expertise" with regard to "competitive conditions and consumer protection issues in their jurisdictions, and privacy regulation, as part of general consumer protection," noting that such issues are not a uniquely federal matter.[4]

---

[1] What constitutes CPNI is defined by 47 USC § 222(h)(1), in essence: "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and any "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier," not related to subscriber list information (e.g., telephone directories) as defined by the statute.

[2] General Order No. R-442, Docket No. UT-960942.

[3] General Order No. R-459, Docket No. UT-971514.

[4] In the Matter of Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of the Non-

7. On November 7, 2002, the WUTC adopted new regulations more stringent than the federal rules, limiting a telecommunications carrier's ability to use or disclose certain CPNI without affirmative prior customer consent ("opt-in"). General Order No. R-505, Docket UT-990146 [hereinafter R-505]. Verizon and other carriers challenged those rules and they were ultimately struck down on First Amendment grounds. *See, Verizon Northwest v. Showalter, et. al.*, 282 F.Supp.2d 1187 (W.D. Wash. 2003). While the federal district court struck down the "opt-in" rules, however, the court affirmed the substantial state interest in the protection of privacy. 282 F. Supp. 2d at 1192.

8. After the more stringent rules were vacated by the federal district court ruling, the Commission adopted its current CPNI rules, WAC 480-120-202. These rules incorporate the FCC's CPNI rules by reference.[5]

9. The Commission's order in UT-990146 adopting the strict CPNI rules is instructive since it offers insight into the privacy policy concerns expressed by the Commission in this area and recognized by the federal district court as constituting a substantial state interest.[6] These same concerns remain relevant for the instant docket.

Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking (Released: July 25, 2002). 17 F.C.C.R. 14820 (July 2002), at ¶ 71.

[5] 47 CFR §§ 64.2003 through 64.2009. The FCC is currently conducting a rulemaking to determine if the CPNI rules need amendment to address the issue of "electronic audit tracking." In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Consumer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, RM-11277.

[6] Among the substantial harms to privacy envisioned by the Commission were: (1) People wish to remain anonymous for their own safety; (2) People could be screened by prospective employers or fired from their jobs based on perfectly lawful communications with people or organizations to which their prospective or current employers object; (3); Candidates for political office could face unfair scrutiny based on associations with organizations and people with whom telephone records indicate they or their family members have communicated; (4) People wishing to intimidate or harass members of particular political causes, lifestyles or practices, or religions, could obtain organizations' calling records and with the help of a reverse telephone directory, determine the names and addresses of people connected with such causes, practices, religions, etc.; (5) Reporters could have sources compromised, despite assurances that the sources would remain anonymous; (6) Firms could gain insights into their competitors' trade secrets such as the identity of suppliers, call volumes, and, with the aid of a reverse directory, the identity of a competitor's customers and (7) With data about answered/unanswered calls, thieves could find out when an individual is likely or unlikely to be home, making that person vulnerable. *Id*., at ¶ 52.

10. In adopting the rules, the Commission observed that the business of providing telecommunications services requires companies to engage in full-time monitoring of their subscribers' private communications. To be precise, call detail "includes any information about particular telephone calls, including the number from which a call is made, any part of the number to which it was made, when it was made, and for how long. It also includes aggregated information about telephone calls made to or from identifiable individuals or entities, and information about unanswered calls that is specific to a particular period of time." R-505, ¶ 95.

11. Without restrictions on its use, the Commission expressed concern about potential abuse of the information for marketing or other purposes where it could be bought and sold "like any other valuable commodity. *Id*., at ¶¶ 38, 44-45.[7] The Commission felt it "imperative to clarify" company practices and ensure that certain customer calling information is "off-limits to marketing use and disclosure to third parties, at least without the customers' express approval." *Id*., at ¶ 47

12. Moreover, the Commission was concerned about the potential for call information to result in customer "profiling." *Id*., at ¶ 46. "By compiling layer upon layer of information about specific individuals, they are able to produce a profile based on income, lifestyle, and an enormous variety of other factors." *Id*. The Commission quoted a report published by the Washington State Attorney General and the University of Washington School of Law on this point:

> Using these databases, it is possible to identify people by what many would consider private aspects of their lives, including their medical conditions, their SAT scores, and their ethnicities. Those selected by their personal characteristics can be targeted not only by direct marketers, but also by lawyers, insurance companies, financial institutions, and anyone else who has the funds to pay for the information.

Id., at ¶ 46.

[7] In support of this point, the Commission noted no less than one thousand companies compiling comprehensive databases about individual consumers. *Id*., at ¶ 46.

13. In one passage of that order, the Commission expressly discussed CPNI in relation to law enforcement activity, observing that the ready commercial availability of CPNI would undermine the "protection of that same information from use by the government." *Id*., at ¶ 48. Specifically, "individual law enforcement agents and agencies of government could obtain the information not only by presentation of a search warrant authorized by a judge but also merely by purchasing it from the company or from any of a number of other commercial database suppliers." *Id*.

14. The Commission made this statement in November 2002 - after the attacks of September 11, 2001. Nonetheless, the Commission expressed deep concern about the privacy of CPNI, including the government's unfettered access to it.

C. The Alleged NSA Program and Telephone Company Involvement.

1. Summary of press reports.

15. On May 10, 2006, *USA Today* reported that the National Security Agency (NSA) had secretly amassed a database containing the domestic calls of millions of Americans.[8] The scope of the alleged domestic program, as reported by *USA Today*, went far beyond the previously identified NSA program to wiretap certain international calls without a warrant. *USA Today* reported that the three largest telephone companies – AT&T, Verizon, and BellSouth – had been providing customer "call detail records" since shortly after September 11, 2001. *Id*. The story reported that the "government is collecting 'external' data on domestic phone calls but is not intercepting 'internals,' a term for the actual content of the communication, according to a U.S. intelligence official familiar with the program."[9] While customers' names, street addresses and other personal information are not being shared with the NSA, according to *USA Today*, "…the

[8] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 10, 2006. The article was subsequently updated on May 11, 2006.

[9] *Id.*

phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information."[10]

16. Other major publications soon confirmed the existence of the NSA domestic calling database. On May 12, 2006, for example, the *New York Times* reported that a senior government official, granted anonymity because of the classified nature of the program, "confirmed that the NSA had access to records of most telephone calls in the United States."[11] The press reports contend that the NSA is using the domestic calling database to conduct "data mining" or "social network analysis," an effort to identify calling patterns and study how networks are tied together and contact each other.

17. A *Newsweek* article, written by Stephen Levy, explained the theory and practice behind this type of intelligence gathering as well as its drawbacks:

> By mapping the connections between Nawaf Alhazmi and Khalid Almihdar, two men the CIA had suspected as Quada members back in 2000, [Valdis] Krebs [a "social network" expert] established not only that they were dangerous – they had direct links to two people involved in the USS Cole bombing – but that someone named Muhammad Atta was at the center of their social web.
>
> Unfortunately, Krebs did his work well after Alhazmi and Almihdar, along with Atta, completed their deadly attack on the United States on September 11, 2001. But certainly the NSA – whose job it is to use vast computer power to protect us – would like to use such techniques to identify the next Atta. The spy agency thinks that having massive amounts of data on hand – like the phone records of millions of Americans it requested from Verizon, BellSouth and AT&T – will help it do so. The big question is whether this privacy tradeoff can actually pay off.
>
> The NSA's historic request for the nation's phone logs signals a desire to perform massive "traffic analysis" of calls within the U.S. – an examination of who calls whom, when they call and for how long – to identify potential threats. This in turn is expected to be used for the kind of analysis that Krebs performed.

---

[10] *Id.*

[11] Eric Lichtblau and Scott Shane, *Bush Is Pressed Over New Report on Surveillance*, New York Times, May 12, 2006.

But Krebs says you don't need the indiscriminate volume of phone records requested by NSA in order to perform effective social network analysis…

…Though we are officially in the dark on what the NSA will actually do with the phone records, experts figure that the agency also wants to "data mine" for leads on as-yet-unidentified terrorists. That's no slam-dunk. Data mining involves a computational extraction of huge amounts of information in order to extract nuggets that could never be unearthed solely by human efforts. While that practice works wonders in detecting credit-card fraud and targeting direct-marketing prospects, it's yet to be proved that the techniques of data mining can zoom in on terrorist behavior from billions of phone records…[12]

2. Summary of statements by Bush Administration officials and members of Congress.

18. On May 11, 2006, in response to *USA Today's* article about the NSA's domestic program, President Bush issued a public statement. We reprint that statement in its entirety:[13]

After September the 11th, I vowed to the American people that our government would do everything within the law to protect them against another terrorist attack. As part of this effort, I authorized the National Security Agency to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. In other words, if al Qaeda or their associates are making calls into the United States or out of the United States, we want to know what they're saying.

Today there are new claims about other ways we are tracking down al Qaeda to prevent attacks on America. I want to make some important points about what the government is doing and what the government is not doing.

First, our international activities strictly target al Qaeda and their known affiliates. Al Qaeda is our enemy, and we want to know their plans. Second, the government does not listen to domestic phone calls without court approval. Third, the intelligence activities I authorized are lawful and have been briefed to appropriate members of Congress, both Republican and Democrat. Fourth, the privacy of ordinary Americans is fiercely protected in all our activities.

---

[12] Stephen Levy, *Only the Beginning?*, Newsweek, May 22, 2006, p. 33.

[13] President Bush Discusses NSA Surveillance Program, May 11, 2006, statement available at: http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html.

> We're not mining or trolling through the personal lives of millions of innocent Americans. Our efforts are focused on links to al Qaeda and their known affiliates. So far we've been very successful in preventing another attack on our soil.
>
> As a general matter, every time sensitive intelligence is leaked, it hurts our ability to defeat this enemy. Our most important job is to protect the American people from another attack, and we will do so within the laws of our country. Thank you.

19. That same day, Senator Christopher Bond (R-MO), a Senate intelligence subcommittee member, told the *News Hour with Jim Lehrer* that he had been "thoroughly briefed on this program and other programs."[14] Among Senator Bond's comments was the observation that "business records are not protected by the Fourth Amendment."[15] In particular, he cited the 1979 case, *Smith v. Maryland* in which, said Senator Bond, "the U.S. Supreme Court said that the government could continue to use phone records, who called from where to where, at what time, for what length, for intelligence and criminal investigations without a warrant."[16] Similarly, according to the Senator, the President's program "uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number."[17] Senator Bond was careful, however, to explain that while the "government has, in the past, and could look at all of the records of purely domestic phone calls; that's not the purpose of this program."[18]

20. Despite Senator Bond's conflicting statements to the *News Hour,* Senator Wayne Allard (R-CO) told the Washington Post that, consistent with the *USA Today* story, the White House

---

[14] *News Hour with Jim Lehrer*, (National Public Radio broadcast, May 11, 2006), "The President Speaks Out."

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

had told him the NSA was probing calling patterns to "detect and track suspected terrorist activity."[19]

21. At a press conference on May 16, 2006, President Bush was asked whether, after the existence of the NSA database surfaced, Americans should feel that their privacy had been invaded. The President replied: "We got accused of not connecting dots prior to September the 11th, and we're going to connect dots to protect the American people, within the law," Mr. Bush said. "The program he's asking about is one that has been fully briefed to members of the United States Congress, in both political parties. They are very aware of what is taking place."[20]

22. The president's security advisor, Stephen Hadley, confirmed the program's existence, saying "It's really about calling records, if you read the [*USA Today*] story -- who was called when and how long did they talk. And these are business records that have been held by the courts not to be protected by a right of privacy. And there are a variety of ways in which these records lawfully can be provided to the government. So again, I can't confirm or deny the claims made, but if you just look at the claims, it's a very limited question and … it's hard to find the privacy issue."[21]

3. Summary of company statements.

23. AT&T, Inc. (AT&T)[22] was the first company to issue a statement in response to the *USA Today* story.[23] That statement, issued on May 11, 2006, cited AT&T's "long history of vigorously protecting customer privacy" and noted "customers expect, deserve, and receive

---

[19] Brian Bergstein, *Skepticism Surrounds NSA Mining Records*, The Washington Post, May 24, 2006.

[20] *All Things Considered* (National Public Radio broadcast, May 18, 2006), David Folkenflik, "Paper Defends Story on NSA Program."

[21] *Face The Nation* (CBS News broadcast, May 14, 2006).

[22] In response to the ACLU's request for an investigation at issue here, AT&T also submitted a written statement to the WUTC on May 26, 2006, and an oral statement to the Commission at its May 31, 2006, Open Metting.

[23] AT&T, Inc., "Statement on Privacy and Legal/Security Issues," Press Release, May 11, 2006, available online at: http://att.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22285.

nothing less than our fullest commitment to their privacy."[24] That said, AT&T explained that it also has "an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare, whether it be an individual or the security interests of the entire nation."[25] Thus, "if and when AT&T is asked to help" the company does so "strictly within the law and under the most stringent conditions."[26]

24. BellSouth Corp (BellSouth) also issued a response to the allegations in the *USA Today* article, saying, "the Company conducted an internal review to determine the facts," that review "confirmed no such contract [to provide records to NSA] exists" and that the Company "had not provided bulk customer calling records to the NSA." [27]

25. Verizon Communications Inc. (Verizon) issued two separate statements in reply to the *USA Today* story; one on May 11, 2006 and the other on May 16, 2006. In its May 11, 2006, statement, Verizon acknowledged[28] that "the President has referred to an NSA program, which he authorized, directed against al-Qaeda." [29] However, the Company did not specifically identify the NSA program or the Company's role since the "program is highly classified."[30] Indeed, Verizon took the position that it could not "confirm or deny" whether it had any "relationship" to NSA program.[31]

26. With regard to its general policy of providing customer information to a government agency, Verizon said it would do so "where authorized by law for appropriately-defined and

---

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] BellSouth Corporation, "BellSouth Statement on Governmental Data Collection," Press Release, May 15, 2006, available online at: http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860.

[28] *Id.*

[29] Verizon Communications Inc., "Verizon Issues Statement on NSA and Privacy Protection," May 11, 2006, Press Release, available online at: http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93446&PROACTIVE_ID=cecdc6cbc7c8cacecc5cecfcfcfc5cecdcecbcec7cdccc6c7c5cf

[30] *Id.*

[31] *Id.*

focused purposes" and that the company "does not, and will not, provide any government agency unfettered access to its customer records or provide information to the government under circumstances that would allow a fishing expedition."[32]

27. In its May 16, 2006, statement, Verizon again said it could not and would not comment on the "NSA program acknowledged by the President."[33] However, the Company then repudiated some of what had been reported in the press. Specifically, it denied reports asserting "that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls."[34] The Company countered that after the 9/11 attacks until "just four months ago" Verizon had "three major businesses," including "its own Internet Service Provider and long-distance businesses."[35] Contrary "to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records…or any call data" related to its wireless or wireline businesses.[36]

28. Qwest Communications International, Inc. (Qwest), reported in the *USA Today* story to have refused to provide information to the NSA, did not issue a statement or comment after the story emerged. When asked for a comment for the *USA Today* article, the spokesman for Qwest said, "We can't talk about this. It's a classified situation."[37]

---

[32] *Id*. Verizon, however, pointed out "factual errors" in press coverage about the way it handles customer information in general, saying, Verizon "puts the interests of customers first and has a longstanding commitment to vigorously safeguard customers' privacy." *Id*.

[33] Verizon Communications Inc., "Verizon Issues Statement on NSA Media Coverage," May 16, 2006, Press Release, available online at: http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450&PROACTIVE_ID=cecdc6cbc7c8cacecc5cecfcfcfc5cecdcecbcec7cdccc6c7c5cf

[34] *Id*.

[35] *Id*.

[36] *Id*. The statement is somewhat unclear but appears to allude to the possibility that MCI participated in the program and so Verizon's participation was a result of its merger with MCI four months earlier. In fact, on February 5, 2006, *USA Today* reported that MCI participated in the NSA wiretapping program. Leslie Cauley and John Diamond, *Telecoms let NSA spy on calls*, USA Today, February 5, 2006.

[37] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 10, 2006. The article was subsequently updated on May 11, 2006.

29. While Qwest did not respond to the news stories, former CEO, Joseph Nacchio, did. He reportedly confirmed that the government approached Qwest in the fall of 2001 requesting phone records without a warrant or special approval from the FISA Court.[38] Speaking through his attorney, Nacchio said that he concluded that the government's request violated the privacy requirements of the Telecommunications Act.[39]

30. On June 8, 2006, the Washington Independent Telephone Association (WITA) asked the Commission to exclude it from any investigation stemming from the NSA program, saying "none of the WITA members has engaged in a practice of sharing CPNI with national or other security agencies on a *general* basis." Letter from Terrence Stapleton (June 8, 2006), p. 1 (emphasis added). WITA, however, conditioned this statement by saying that because of regular personnel changes and the long history of the WITA companies, "WITA cannot represent that sharing of CPNI with security agencies in the absence of a subpoena, court order or other compulsory process has never occurred in the past." *Id*. Public Counsel believes it would premature to exclude WITA from these proceedings.

31. Sprint Nextel has not escaped this issue either.[40] On February 5, 2006, *USA Today* reported that Sprint, AT&T and MCI cooperated with the government's program of monitoring international calls and e-mails of a domestic target without first obtaining court orders.[41] With regard to the releasing of CPNI to the NSA, Sprint has refused to disavow participation in the NSA program: "Due to the sensitive nature of the topics currently being reported in the press related to the National Security Agency and their intelligence gathering program, Sprint Nextel is not discussing these matters."[42]

---

[38] David G. Savage, *Phone Firms Questioned,* Los Angeles Times, May 13, 2006.

[39] Shrader, Katherine, *Lawyer: Ex-Qwest Exec Ignored NSA Request,* Los Angeles Times, May 13, 2006.

[40] Sprint owned United Telephone of the Northwest until May 19, 2006, when Sprint spun United off as an independent entity and the new local telephone company became Embarq.

[41] Leslie Cauley and John Diamond, *Telecoms let NSA spy on calls,* USA Today, February 5, 2006.

[42] Sprint's comments were added to its privacy policy and are available at: http://www.sprint.com/legal/privacy.html.

D. Relevant Pending Federal and State Court Cases and the Status of Those Cases.

32. Prior to the May 10, 2006, *USA Today* story regarding the existence of an NSA database containing domestic calling records, numerous lawsuits were brought challenging the NSA program involving wiretapping of calls originating domestically and terminating internationally. Other cases were filed after the May 10 story and relate only to the domestic database program. At least two dozen lawsuits have been filed in both state and federal courts against the government and one or more telecommunications companies, particularly Verizon, AT&T and Bell South. We identify some of these cases and their current status where known.[43]

- *ACLU et. al. v. NSA*, Case 2:06-cv-10204-ADT-RSW (S.D. Mich., filed January 17, 2006), was filed in the Southern District of Michigan against the NSA. Plaintiffs Motion for Partial Summary Judgment was filed on March 9, 2006 and set for oral arguments on June 12, 2006. Defendants' response to plaintiffs' Motion was due on or before May 26, 2006 but the defendants did not file a response and instead, moved to stay consideration of plaintiffs' motion as well as a motion to dismiss or, in the alternative for summary judgment. Defendants' motions were filed with two supporting declarations and a Notice of Lodging, at the U.S. Department of Justice, of materials to be examined Ex Parte by the court. The court denied the stay, and affirmed the June 12, 2006, hearing date as scheduled. After the hearing, the Judge Taylor deferred ruling until after a second hearing scheduled for July 10.

- *Hepting, et. al. v. AT&T*, C-06-0672-VRW (N.D. CA, January 30, 2006), was filed in the federal district court for the Northern District of California. This is a nationwide lawsuit that was brought against AT&T in the United States District Court for the Northern District of California. On March 9, 2006, the plaintiffs moved for partial summary judgment and that motion was noted for June 23. On May 12, 2006, the United States, as a non-party, moved to dismiss, or in the alternative, for summary judgment based on immunity grounds. Prior to the hearing the Judge requested the parties prepare responses to eleven questions, including questions related to the government's invocation of the state secrets privilege.

- *United States v. Farber, et. al*., 3:06CV02683, (D.N.J., June 14, 2005), was filed in the federal district court for New Jersey, moving to quash administrative subpoenas issued by

[43] Reuters News Service, *US wants telecom surveillance lawsuits in DC Court*, Washington Post, June 20, 2006.

the New Jersey Attorney General to Verizon for information related to the NSA program.[44] The Government relied on affidavits it produced in the *Hepting* case.

- *Bissitt v. Verizon Communications. Inc*., No. 1:06-cv-OO220-T-LDA (D.R.I., filed May 15, 2006), was filed in the District of Rhode Island against Verizon and BellSouth.

- *Driscoll v. Verizon Communications. Inc.,* No. 1:06-cv-00916-RBW (D.D.C., filed May 15, 2006), was filed in the District of Columbia against Verizon.

- *Fuller v. Verizon Communications. Inc*., No. 9:06-cv-00077-DWM (D. Mont., filed May 12,2006), was filed in the District of Montana against Verizon and Verizon Wireless.

- *Herron v. Verizon Global Networks, Inc.,* No. 2:06-cv-02491-JCZ-KWR (E.D. La., filed May 12,2006), was filed in the Eastern District of Louisiana against Verizon Global Networks Inc., AT&T Corp., American Telephone and Telegraph Company, BellSouth Communication Systems, LLC, and BellSouth Telecommunications, Inc.

- *Hines v. Verizon Northwest, Inc*., No. 9:06-cv-00694 (D. Or. filed May 12, 2006), was filed in the District of Oregon against Verizon.

- *Mahoney v. Verizon Communications, Inc*., No. 1:06-cv-00224-S-LDA (D.R.I.) filed May 15, 2006), was filed in the District of Rhode Island against Verizon communications.

- *Marck v. Verizon Communications, Inc.,* No. CV-06-2455 (E.D.N.Y., filed May 19, 2006), was filed in the Eastern District of New York against Verizon Communications Inc.

- *Mayer v. Verizon Communications, Inc*., No. 1:06-cv-03650 (S.D.N.Y., filed May 12, 2006), was filed in the Southern District of New York against Verizon Communications.

- *Conner v. AT&T*, No. 06-0225 (E.D. Cal., removed May 23, 2006), was filed in the Superior Court of California, and later removed to the Eastern District of California, against AT&T, BellSouth, and Verizon.

[44] The subpoenaed documents were, *inter alia*, (1) all names and addresses of all Persons including but not limited to, all affiliates, subsidiaries, and entities, that provided Telephone Call History Data to the NSA; (2) all Executive Orders issued by the President of the United States and provided to Verizon Concerning any demand or request to provide Telephone Call History Data to the NSA; (3) all "orders, subpoenas, and warrants issued by or on behalf of any unit or office of the Executive Branch of the Federal Government and provided to Verizon Concerning any demand or request to provide Telephone Call History Data to the NSA;" and (4) all "orders, subpoenas, and warrants issued by or on behalf of any Federal or State judicial authority and provided to Verizon Concerning any demand or request to provide Telephone Call History Data to the NSA." 3:06CV02683, Document No. 32, p. 10 of 11 (capitalization of words connotes terms defined in the subpoena).

- *Dolberg v. AT&T Corp*, No. CV 06-78-M-DWM (D. Mont., filed May 15, 2006), was filed in the District of Montana against AT&T Corp. and AT&T Inc.

- *Harrington v. AT&T, Inc*., No. A06CA374-L Y (W.D. Tex., filed May 18, 2006), was filed in the Western District of Texas against AT&T Inc.

- *Ludman v. AT&T Inc*., No. 1:06-cv-00917-RBW (D.D.C., filed May 15,2006), was filed in the District of Columbia against AT&T. Inc.

- *Schwarz v. AT&T Corp*., No. 1:06-cv-02680 (N.D. Ill., filed May 15, 2006), was filed in the Northern District of Illinois against AT&T.

- *Souder v. AT&T, Corp.*, No. 06CV1058-DMS AJB (S.D. Cal., filed May 12,2006), was filed in the Southern District of California against AT&T Corp. and AT&T Inc.

- *Trevino v. AT&T Corp*., No. 2:06-cv-00209 (S.D. Tex., filed May 17,2006), was filed in the Southern District of Texas against AT&T Corp. and AT&T Inc.

- *Terkel v. AT&T Inc*., No. 06C-2837 (N.D. Ill., filed May 22, 2006) was filed in the Northern District of Illinois against AT&T Inc.

- *Phillips v. BellSouth Corp*., No: 3:06-CV-00469 (D.D.C., filed May 15, 2006), filed in the District of Columbia against BellSouth.

- *Potter v. BellSouth Corp*., No. 3 06-0469 (M.D. Tenn. filed May 15, 2006), in the Middle District of Tennessee against BellSouth.

- *Riordan, et. al. v. Verizon*, (Superior Court of California, City and County of San Francisco, filed May 25, 2006).

- *Campbell, et. al. v. AT&T*, (Superior Court of California, City and County of San Francisco, filed May 26, 2006).

33. On May 24, 2006, Verizon asked the Judicial Panel on Multidistrict Litigation on to consolidate many of these actions before a single federal district court for pretrial proceedings. The Justice Department filed a motion supporting Verizon on June 19, 2006. The reasons given for consolidation involve alleged national security concerns and the possible need to share highly classified information with federal judges.

E. The FCC Decision Not to Investigate.

34. In a May 22, 2006 letter, FCC Chairman, Kevin J. Martin, responded to a letter from the Honorable Edward J. Markey (D-MA), Ranking Member of the Subcommittee on Telecommunications and the Internet Energy and Commerce Committee.[45] Rep. Markey's letter asked whether, given that § 222 of the Telecommunications Act provides that carriers have a duty to protect the confidentiality of customer proprietary information, the FCC would be "investigating and resolving these alleged violations of consumer privacy."[46]

35. The Chairman responded that while the Commission takes "very seriously our charge to faithfully implement the nation's laws, including our authority to investigate potential violations of the Communications Act," in this case, "the classified nature of the NSA's activities makes us unable to investigate the alleged violations…at this time."[47]

36. The FCC also noted that several lawsuits are pending regarding the issues raised by Rep. Markey and "the government has moved to dismiss the action on the basis of the military and state secrets privilege."[48] The Chairman noted that in the declarations offered by the government in the *Hepting* case, the government took the position that, with regard to "the NSA's purported involvement" with specific telephone companies, "the United States can neither confirm nor deny alleged NSA activities, relationships, or targets," because "[t]o do otherwise when challenged in litigation would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in genera1."[49] Therefore, according to the Chairman, it would not be possible for the FCC to investigate without

[45] Letter from Kevin J. Martin, Chairman Federal Communications Commission to the Honorable Edward J. Markey, May 22, 2006.

[46] *Id*., at p. 1.

[47] *Id*.

[48] *Id*., at p. 2, citing the government's motion to dismiss in *Hepting, et. al. v. AT&T*. (N.D. CA, January 30, 2006).

[49] *Id*.

examining highly sensitive classified information and the Commission has no power to order the production of classified information.[50] To the contrary, said the Chairman, since the Supreme Court has held that "the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment."[51]

37. In addition, according to the Chairman, the "statutory privilege applicable to NSA activities also effectively prohibits any investigation by the Commission."[52] Specifically, the National Security Act of 1959 provides that "nothing in this Act or any other law ... shall be construed to require the disclosure of the organization or any function of the National Security Agency [or] of any information with respect to the activities thereof."[53]

38. Moreover, according to Chairman Martin, the United States Court of Appeals for the District of Columbia Circuit has held that the NSA statute's "explicit reference to 'any other law' ... must be construed to prohibit the disclosure of information relating to NSA's functions and activities as well as its personnel."[54] Therefore, the NSA statute "displaces any authority that the Commission might otherwise have to compel, at this time, the production of information relating to the activities discussed in your letter."[55]

39. Federal Communications Commissioner Michael J. Copps, however, did not agree with the Chairman and other members of the Commission. On May 15, 2006, Commissioner Copps, made the following statement:

> Recent news reports suggest that some – but interestingly not all – of the nation's largest telephone companies have provided the government with their customers'

---

[50] *Id.*

[51] *Id.*, quoting *Department of the Navy v. Egan*, 484 U.S. 518, 529 (1988).

[52] *Id.*

[53] *Id.*, quoting Pub. 1. No. 86-36, § 6(a), 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note.

[54] *Id.*, quoting *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996).

[55] *Id.*

calling records. There is no doubt that protecting the security of the American people is our government's number one responsibility. But in a Digital Age where collecting, distributing, and manipulating consumers' personal information is as easy as a click of a button, the privacy of our citizens must still matter. To get to the bottom of this situation, the FCC should initiate an inquiry into whether the phone companies' involvement violated Section 222 or any other provisions of the Communications Act. We need to be certain that the companies over which the FCC has public interest oversight have not gone – or been asked to go – to a place where they should not be.[56]

F. Relevant Public Utility Commissions Activities.

40. The *USA Today* story also resulted in the initiating of various proceedings in state public utility commissions, including Washington. Again, we identify some of these activities and, where known, their current status.

- **ARIZONA**
  ACLU Letter to the Public Utilities Commission

- **COLORADO**

1. ACLU Letter to the Attorney General
2. ACLU Letter to the Public Utilities Commission

- **CONNECTICUT**

1. ACLU Letter to the Public Utilities Commission Filing Complaint, Requesting an Investigation and Seeking Rulemaking.

2. The PUC opened a docket, Docket No. 06-05-13 and requested comments. See http://www.dpuc.state.ct.us/DOCKCURR.NSF/f5c4efacb773316a8525664e0049ea32/4e7be625dc40ef738525717f00562fa7?OpenDocument&Highlight=0,06-05-13%20 for request for comments. Comments were due on due June 14, 2006 and Reply Comments are due June 28, 2006. Initial comments were filed by the Attorney General of Connecticut, the Office of Consumer Counsel, the ACLU of Connecticut, the Southern New England Telephone Company d/b/a AT&T Connecticut and The Woodbury Telephone Company d/b/a AT&T Woodbury, and Verizon.

- **DELAWARE**

1. ACLU Letter to the Public Utilities Commission
2. AT&T Response to ACLU Letter

- **FLORIDA**
  ACLU Letter to the Public Utilities Commission

[56] Michael J. Copps, *Calls for the FCC to Open an Inquiry Into the Lawfulness of the Disclosure of America's Phone Record,*.http://www.fcc.gov/commissioners/copps/statements2006.html.

- **IOWA**
  Public Utilities Board Response

- **KANSAS**
  ACLU Letter to the Attorney General

- **MAINE**

1. "Ten Person Complaint" filed with the Public Utilities Commission against Verizon and docketed as Docket No. 2006-274 regarding domestic wiretapping but after USA Today story was expanded to phone records. Commission issued a procedural order requesting that Verizon address, in its response to the complaint, the extent to which the actions alleged in the complaint and in the *USA Today* article implicate the privacy rights of described by state statute.
2. ACLU Petitioned for Intervention
3. Verizon Response to Complaint
4. Comments due June 30, 2006.

- **MASSACHUSETTS**
  Complaint, Request for Hearing, Proposed Rule filed by four mayors, which requires a public hearing by statute.

- **MISSOURI**
  ACLU Letter to the Attorney General

- **NEBRASKA**
  ACLU Letter to the Public Utilities Commission

- **NEVADA**
  ACLU Letter to the Public Utilities Commission

- **NEW JERSEY**
  ACLU Letter to the Public Utilities Commission

- **NEW YORK**
  ACLU Letter to the Public Utilities Commission

- **OREGON**

1. ACLU Letter to the Public Utilities Commission
2. ACLU Letter to the Attorney General

- **PENNSYLVANIA**
  May 24, 2006, the ACLU of Pennsylvania filed a complaint with the PUC on behalf of 20 organizations and individuals. The complaint asks the Commission to order the

telephone companies to reveal what information they have disclosed to the NSA and asks the Commission to hold such releases in violation of Pennsylvania law and to prohibit future releases.

- **RHODE ISLAND**
  Letter to the Public Utilities Commission

- **TENNESSEE**
  ACLU Letter to the Public Utilities Commission

- **TEXAS**
  ACLU Letter to the Public Utilities Commission

- **VERMONT**

1. Letter to the Public Utilities Commission
2. Letter to AT&T
3. Letter to Verizon
4. AT&T Response
5. Verizon Response

- **VIRGINIA**
  ACLU Letter to the Public Utilities Commission

III. LEGAL AUTHORITY

41. The Commission's Notice invited commentary on five "preliminary" questions. Before turning to these questions, we review relevant law and then apply this analysis to the questions posed by the Commission.

42. In order to perform this legal analysis, it was necessary to work with an assumed set of facts. Therefore, based on the statements made by governmental officials, the telephone companies and press reports, the following is assumed for the purposes of this memorandum: (1) the NSA phone records program exists and its purpose is to perform "social network" analysis in order to prevent terrorist attacks, (2) that certain telecommunications companies have participated in the program by turning over, without a warrant or special permission from the FISA Court, private call detail information from their subscribers, and (3) telecommunications companies failed to obtain consent from customers for the release of this information.

A. Section 222 of the Telecommunications Act of 1996.

43. A legal analysis of the questions posed by the Commission hinges largely on Section 222 of the Telecommunications Act of 1996 and its requirement that Customer Proprietary Network Information (CPNI) be kept confidential, except in limited circumstances. 42 U.S.C. § 222 (hereinafter § 222).[57] In particular, § 222(c)(1) defines when a carrier may breach confidentiality by providing CPNI to third parties. A carrier may give CPNI to third parties in two primary situations: "as required by law" or "with the approval of the customer." *Id*.

44. We explicitly do not address the customer consent issue here because we assume for the purposes of these comments that no consent was sought or received for the records allegedly given to the NSA. Nevertheless, even if a carrier had received consent to disclose the information to third parties under § 222, whether the scope of that consent included disclosure to the NSA is one we do not address here because it is a fact-specific question. It requires examination of the specific forms of consent obtained by each carrier and is not pertinent at this time given the questions posed by the Commission.[58]

1. Customer Proprietary Network Information (CPNI).

45. What constitutes CPNI is defined by § 222(h)(1). There are two categories of CPNI described in the statute. First, CPNI is defined as any "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." Second, CPNI is defined as any "information contained in the bills pertaining to telephone

[57] We focus on § 222 of the Act because the WUTC exercises concurrent jurisdiction to enforce § 222. *See, supra*, 17 F.C.C.R. 14820 (July 2002), at ¶ 71. Indeed, as noted, the WUTC's current privacy rule incorporates by reference the FCC's rules implementing § 222. WAC 480-120-202.

[58] In our responses to the Commission's questions below, however, we recommend that the Commission require companies to provide information regarding their privacy policies, and in particular, those related to consent.

exchange service or telephone toll service received by a customer of a carrier" not related to subscriber list information (e.g., telephone directories) as defined by the federal statute.

46. If the public statements of government officials, company officials and press reports accurately describe the information that allegedly was released to the NSA, the information constitutes CPNI as defined by § 222(h)(1). The information allegedly provided by telecommunications carriers contained telephone records with the name and phone number of the caller, the phone numbers he or she called, where the call terminated, and the length of the call.[59] This is clearly CPNI under both § 222(h)(1) categories. *See, Verizon Northwest v. Showalter*, 282 F.Supp.2d at 1189.

2. "As required by law".

47. Section 222 allows a carrier to give CPNI to third-parties "as required by law." Public Counsel has identified only one federal district court case discussing what it means for a carrier to be "required by law" to disclose CPNI to third-parties in the absence of a subpoena.[60] *ICG Communications v. Allegiance Telecom, et. al.*, 211 F.R.D. 610 (N.D. Cal. 2002)[61] [hereinafter *ICG Communications*].

48. In *ICG Communications*, ICG, a telecommunications provider had filed for bankruptcy protection. *Id.*, at 610-11. As part of its reorganization, ICG was required to determine which of its customers were profitable and which were not. *Id*., at 611. The Company then sent a letter to its profitable customers saying it would continue serving them even though it was in bankruptcy. *Id*. To its unprofitable customers, ICG sent a letter indicating that it would be terminating their services. *Id*.

---

[59] Newsweek, "Only the Beginning?," Stephen Levy, May 22, 2006, p. 33.

[60] *Parastino v. Conestoga Tel. & Tel. Co*., 1999 WL 636664 (E.D.Pa.1999) involved a § 222(c)(1) claim against a carrier for wrongfully disclosing telephone records to third parties without his consent. Since the defendant disclosed the telephone records in response to subpoenas issued in state criminal proceedings against the plaintiff and the plaintiff conceded that a valid subpoena would qualify as an exception under § 222(c)(1), the court did not reach the question whether § 222(c)(1) applies to a court order such as a subpoena.

[61] *See*, Appendix A.

49. Allegiance Telecom, a competitor, allegedly sent ICG's unprofitable letter to ICG's profitable customers in order to get ICG's profitable customers to switch to Allegiance. *Id*. Allegiance also allegedly called ICG's profitable customer claiming to be ICG and told those customers it would be terminating service in 30 days. As a result, ICG filed a number of claims against Allegiance, including trademark infringement, unfair competition, and deceptive trade practices.

50. Statutory interpretation of § 222 was necessitated by a discovery dispute arising from that lawsuit. Specifically, ICG requested (1) that Allegiance produce all documents regarding each "ICG customer" that switched from ICG to Allegiance and (2) that Allegiance produce all documents regarding each "ICG customer" who received a letter from Allegiance indicating the ICG would be terminating service. *Id*.

51. Allegiance objected to the discovery requests, claiming that it could not answer under § 222 since the information requested was CPNI. *Id*. Conceding it was CPNI, ICG offered a protective order but the defendant rejected that offer. *Id*. ICG moved to compel.

52. The question presented to the court was whether the phrase "Except as required by law" in § 222(c)(1) allowed the court to compel Defendant to answer Plaintiff's interrogatories and produce the documents requested. *Id*., at 612. In answering the question, the district court's analysis centered on whether Rule 26(b)(1) of the Federal Rules of Civil Procedure (that a party "may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party" and the court may order discovery of any matter that "appears reasonably calculated to lead to the discovery of admissible evidence") is a "law" as that term is used in § 222(c)(1).

53. The court concluded that the Federal Rules of Civil Procedure "constitute 'law'as that term is ordinarily understood." *Id*.[62] First, the Federal Rules have been found to "have the

[62] The Court discussed, in general, what constitutes "law." *Id*., at 612-13:

> In common parlance, "law" includes "a rule or order that is advisable or obligatory to observe." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 659 (10th ed.1993). BLACK'S LAW

force and effect of a federal statute" and second, Congressional authorization of the rules "dates back to 1934 with the codification of the Rules Enabling Act, 28 U.S.C. § 2072." *Id*., at 613.

54. The court also found that the legislative history of § 222 supported its interpretation, saying:

> The Senate version of legislation that embodied Section 222 contained an exception to the prohibition against disclosure of CPNI "in response to a court order or to initiate, render, bill and collect for telecommunications services." H.R. Conf. Rep. 104-458, 104th Cong., 2nd Sess. at 203 (1996). The House version of bill contained no explicit language addressing the issue but stated more generally that "this section shall not prevent the use of CPNI to combat toll fraud or to bill and collect for services requested by the customers." *Id*. at 204. The Conference Committee adopted the Senate provisions with modifications. *Id*. at 205. The final wording in the Conference Committee version containing the "except as provided by law" replaced the Senate's "court order" language. Nothing in the legislative history suggests that the Conference Committee version was intended to narrow the Senate version of the language. The natural reading of the change in language was that it was intended to broaden rather than narrow the exception. The language is broader than the Senate's language since it is not limited to court orders but is broad enough to apply literally to other laws such as regulations and administrative rules and orders.

Id., at 613, noting that the Privacy Act, 5 U.S.C. § 552a, contains express language excepting court orders. *Id*., fn. 3.[63] Therefore, Allegiance was required to produce the CPNI under an "attorneys only" protective order. *Id*., at 615.

55. Faced with a similar question of interpretation of § 222, the Colorado Public Utilities Commission (PUC) held that an administrative subpoena requiring a telephone company to give

---

DICTIONARY, Seventh Edition, p. 889 (1999) similarly defines "law" as "the aggregate of legislation, judicial precedents, and accepted legal principles; the body of authoritative grounds of judicial and administrative action."

[63] The court also based its order on the view that "courts generally eschew an 'absolute privilege for trade secrets and similar confidential information' in favor of a case-by-case approach that balances 'privacy against the need for disclosure.'" *Id*., at 614, citing *Federal Open Market Committee v. Merrill*, 443 U.S. 340, 362 (1979). That is, information similar to CPNI is not absolutely privileged. Instead, it is protected only when privacy interests outweigh the need for disclosure. Significantly, not only did the Court impose a protective order in that case, it imposed one that limited the disclosure of the information to only the attorneys in the case. *See*, *Id*. at 614. ("In light of the privacy concerns…there is good cause for a protective order limiting the production for attorney eyes only.")

CPNI to a third party met the "as required by law" standard. *Adams County E-911 Emergency Telephone Service Authority v. Qwest Communications*, Docket No. 06F-039T, Decision No. R06-0496-I (Colo. P.U.C. May 3, 2006)[64] [hereinafter *Adams County*].

56. The *Adams County* case involved a complaint by an E-911 operator against Qwest alleging that Qwest was billing it for telecommunications services under the wrong tariff. Docket No. 06F-039T, Decision No. R06-0252-IA, ¶ 4 (Colo. P.U.C. March 17, 2006). A discovery dispute involving requests from Adams County for (1) Qwest's application of the disputed tariff provisions, (2) a comparison of the tariff rate Qwest charges to Adams County and the City and County of Denver, and (3) the identity of each city, town, and county served by each local switching office in Colorado. Decision No. R06-0496-I, ¶¶ 6-8.

57. Qwest objected and argued that responding to the requests violated § 222. *Id*, ¶¶ 9, 13. Adams County responded that "the purpose of CPNI protections is to protect privacy of customers" and in this instance, "the requested information cannot be sensitive information within the intended protections of 47 U.S.C. § 222 because it is open to the public under the Colorado Open Records Act." *Id*., ¶ 14. Qwest argued that even if the information was subject to the Open Records Act, the Company was not governed by the Act and therefore, was not required by law to produce it. *Id*., ¶ 15. The Administrative Law Judge agreed. *Id*., ¶ 16.

58. Alternatively, Adams County sought to compel responses from Qwest based on the reasoning adopted in *ICG Communications*. *Id*., ¶ 17. Qwest argued that *ICG Communications* did not apply to a governmental entity seeking disclosure. *Id*., ¶ 19, citing 18 U.S.C. § 2703(c).[65] In other words, Qwest argued that "federal law prohibits a wire or electronic service provider from disclosing subscriber information to the government in the absence of a specifically identified legal process." *Id*., ¶ 26. *Id*.

---

[64] *See*, Appendix B.

[65] Please see the discussion regarding the contents of this provision of the Electronic Communications Privacy Act of 1996, 18 U.S.C. § 2703(c), below.

59. The ALJ did not agree with Qwest's argument regarding 18 U.S.C. § 2703(c) but assumed, *arguendo*, that even if § 2703(c) applied to the case, § 2703(c)(2) allows the release of information subject to an administrative subpoena issued by a governmental entity. *Id*., ¶ 27. Finding that the Colorado PUC had such subpoena power and that such a subpoena constituted a disclosure "a required by law" under § 222, Qwest was required to provide the CPNI. *Id*.

B. The Legal Framework for the Lawfulness Debate.

60. The briefing on whether the NSA acted lawfully is occurring in multiple jurisdictions and fora. It is extensive and growing larger every day. It involves, *inter alia*, interpretation of the Constitution of the United States, and the separation of powers between the Executive, Congress, and the Judicial Branch. In particular, the core constitutional and statutory questions regarding the lawfulness of the NSA's actions appear to be: (1) whether the U.S. Constitution gives the President inherent authority as Commander in Chief to order telephone companies to produce their subscriber records without a warrant and without special permission from the Foreign Intelligence Surveillance Act (FISA) Court; (2) whether the U.S. Constitution gives Congress the authority by statute to cabin or limit the President's power in this area (and whether it has in fact done so through FISA or chosen not to do so via the Authorization for Use of Military Force (AUMF); (3) whether the U.S. Constitution allows the Judicial Branch to limit the President's authority on national security issues through application of the Bill of Rights; and (4) whether the U.S. Constitution allows the Judicial Branch to prohibit the President's actions because those actions contravene the Bill of Rights, even where Congress has given the President authority to act on national security affairs. Therefore, before directly addressing § 222 and the question of lawfulness, it is necessary to survey the legal framework background for the debate to follow.

1. **The Omnibus Crime Control and Safe Streets Act of 1968 (Title III).**

61. In 1967, the United States Supreme Court held that electronic eavesdropping on private communications by the government was a search and seizure subject to the Fourth Amendment

of the U.S. Constitution. *Katz v. United States, 389 U.S. 347, 352-353 (1967).* After *Katz*, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, codified as amended at 18 U.S.C. § 2510 et seq. (also known as Title III). Title III requires law enforcement to obtain a search warrant based on probable cause before intercepting wire, oral, or electronic communications. It also generally prohibits any person from intercepting private communications, or using or disclosing intercepted communications. 18 U.S.C. § 2511. Communications providers, including telecommunications providers, are subject to this prohibition, except to the extent their conduct is reasonably necessary to providing service or protecting their rights and property. 18 U.S.C. § 2511(2)(a)(i).

2. The Electronic Communications Privacy Act of 1996 (ECPA).

62. Title III was amended to protect electronic communications as well as phone conversations by the Electronic Communications Privacy Act of 1986.[66] *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001) (through ECPA, Congress "enlarged the coverage of Title III to prohibit the interception of 'electronic' as well as oral and wire communications").

63. ECPA provision, 18 U.S.C. § 2701 *et seq.*, generally prohibits governmental access to telephone records without a court order. "A provider … shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service…to any governmental entity." 18 U.S.C. § 2702(a)(3) (emphasis added). Additionally, § 2702(a)(1) prohibits a provider from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." (emphasis added).

64. However, disclosure is allowed pursuant to warrants, court orders and administrative subpoenas, § 2703(c); with customer consent, § 2703(c)(1)(C), *see also* § 2702(c)(2); and "incident to the rendition of the service or to the protection of the rights of the [company's] property, § 2702(c)(3). Finally, § 2702(c)(4) and § 2702(b)(8) provide that providers may disclose information if the provider believes, in good faith, that an "emergency involving danger

[66] This change was codified in 18 U.S.C. § 2510.

of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." Section 2707 provides a civil action for any person aggrieved by a knowing or intentional violation of 18 USC § 2702.

3. Foreign Intelligence Surveillance Act (FISA).

65. In 1978 Congress enacted the Foreign Intelligence Surveillance Act (FISA). FISA provides a means by which the government can obtain approval to conduct electronic surveillance of a foreign power or its agents without first meeting the more stringent standard in Title III for criminal investigations.[67] 50 U.S.C. §§ 1802, 1804, 1811. While Title III requires a showing of probable cause that a proposed target has committed, is committing, or is about to commit a crime, FISA requires a showing of probable cause to believe that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1801(e).

66. After September 11, 2001, Congress amended FISA so that it no longer requires a certification that the "primary purpose" of a search or surveillance is to gather foreign intelligence information. FISA, as amended by the USA PATRIOT Act, P.L. 107-56 § 218, now requires that a "significant purpose" of the investigation be the collection of foreign intelligence information. In other words, the standard for obtaining a FISA warrant was expanded after September 11.

4. Authorization for Use of Military Force (AUMF).

67. On September 18, 2001, pursuant to the War Powers Act, Congress authorized the President's use of military force against those responsible for the September 11, 2001 attacks on the United States. Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541). The authorization is reprinted here in its entirety:

> Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, That the President is authorized to use all

[67] See, 18 U.S.C. § 2511(2)(f) (FISA and its criminal law counterparts "shall be the exclusive means by which electronic surveillance . . . may be conducted").

necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

5. The Constitution of the United States.

68. Under the First and Fourth[68] Amendments to the U.S. Constitution, individuals generally have a reasonable expectation of privacy in their telephone communications and records. *Katz, supra*; *United States v. United States District Court for the Eastern District of Michigan et al., 407 U.S. 297, 314 (1972)* ("the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (footnote omitted).

69. Even with a general expectation of privacy in our communications, certain well-established exceptions to the Fourth Amendment have been carved out by the courts. Among these are hot pursuit, plain view, emergency situations, consent, and searches incident to arrest. *U. S. v. Wright*, 577 F.2d 378 (6th Cir. 1978). In connection with the NSA program, the government has cited two exceptions, "the foreign intelligence" exception and "the special needs" exception.[69]

C. Arguments For and Against the Lawfulness of The National Security Agency's Alleged Actions.

70. The arguments for and against the lawfulness of NSA's actions exist within the legal framework outlined in the prior section. What follows are a review of the main arguments

[68] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[69] See summary of DOJ arguments below.

concluding (1) that the NSA activity is lawful and therefore, § 222 is not violated and (2) that the NSA activity is unlawful and therefore a claim under § 222 could be stated.

1. Arguments that NSA Activity is Lawful.

71. The United States Department of Justice (DOJ) has written extensively on the question of President Bush's executive powers, especially in light of the September 11th attacks and the ongoing "war on terrorism." We summarize the DOJ's opinion contained in its January 19, 2006, report here.[70]

- The President's well-recognized inherent constitutional authority as Commander in Chief supports all of NSA's activities. As Commander in Chief, the President has the foremost responsibility under the Constitution to protect America from attack, and all authority necessary to fulfill that charge. DOJ Report, at p. 1. Consequently, the President may exercise this authority to "conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States." *Id.*
- In addition to the President's inherent authority, Congress has confirmed and supplemented the President's authority under Article II by statute. *Id.*, p. 2. On September 18, 2001, Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." *Id.*, quoting

[70] United States Department of Justice, *Legal Authorities Supporting The Activities Of The National Security Agency Described By The President*, January 19, 2006 [hereinafter DOJ report], available online at: http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf. Both the DOJ report and the Congressional Research Service Report discussed later were a response to the NSA wiretapping program debate and not the current debate regarding CPNI. Nevertheless, the legal arguments regarding separation of powers issues are the same.

the Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (AUMF).

- The Supreme Court's interpretation of AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), confirms that Congress gave its express approval to the President's power to engage in a military conflict against al Qaeda and its allies and authorized the President's use of force for this purpose and those actions attendant to the use of force. *Id*., at 2. This includes Congress' authorization of the use of warrantless electronic surveillance to intercept enemy communications at home and abroad. *Id*.[71]
- The NSA's activities are also consistent with the Foreign Intelligence Surveillance Act (FISA) and relevant related provisions in chapter 119 of title 18. While FISA generally requires judicial approval of electronic surveillance, that statute also contemplates that Congress may authorize such surveillance by a statute other than FISA. *See,* 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*"). *Id*., at pp. 2-3, 23 (emphasis added). AUMF, even though a Joint Resolution of Congress is that statute. *Id*., at pp. 23-24.
- The DOJ disagrees with arguments that FISA requires that any subsequent authorizing legislation under 50 U.S.C. § 1809(a) must expressly amend FISA and without such express amendment, the Executive is not freed from FISA's enumerated procedural requirements. The response is that in "authorizing the President's use of force in

[71] The question in *Hamdi* was whether AUMF was an "Act of Congress" under the Non-Detention Act, which bars imprisonment or detention of a citizen "except pursuant to an Act of Congress." 18 U.S.C. § 4001(a). The Supreme Court held that AUMF did authorize Hamdi's detention but remanded the case on due process grounds.

response to the September 11th attacks, Congress did not need to comb through the United States Code looking for those restrictions that it had placed on national security operations during times of peace and designate with specificity each traditional tool of military force that it sought to authorize the President to use. There is no historical precedent for such a requirement: authorizations to use military force traditionally have been couched in general language. Indeed, prior administrations have interpreted joint resolutions declaring war and authorizing the use of military force to authorize expansive collection of communications into and out of the United States." *Id*., at pp. 24-25

- But even if it was unclear whether AUMF trumps FISA, any doubt as to whether these "laws" allow the President to authorize surveillance without FISA procedures must be resolved in such a way as to avoid the serious constitutional questions that a contrary interpretation would raise. *Id*., at pp. 3, 29. Those constitutional questions are: (1) that Congress cannot interfere with the President's determination to collect intelligence since this is a core exercise of his role as Commander in Chief with control over the Armed Forces during armed conflict and (2) that the particular restrictions imposed by FISA are such that their application would impermissibly impede the President's exercise of his constitutionally assigned duties as Commander in Chief. *Id*., at p. 29. If FISA is not read to allow the President to authorize the NSA activities during the current congressionally authorized armed conflict with al Qaeda, FISA would be unconstitutional as applied in this narrow context. *Id*., at p. 35. Thus, any potential conflict between FISA and the AUMF is resolved in favor of AUMF under "the canon of constitutional avoidance." Once harmonized, the President's authority overcomes any restrictions in FISA (and Title

III) with regard to the congressionally authorized armed conflict with al Qaeda. *Id*. at pp. 3, 36.

- The NSA activities fully comply with the Fourth Amendment. The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *U.S. Const. amend. IV*. According to the DOJ, the "touchstone" for review of government action under the Fourth Amendment is whether the search is "reasonable." *Id*., at pp. 36-37, citing *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995).
- Reasonableness in this context, says DOJ, must be assessed under a general balancing approach, "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id*., at p. 37, citing *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (internal quotations omitted). Thus, the NSA's activities are reasonable because the government's interest in defending the Nation from another foreign attack outweighs the individual privacy interests at stake. *Id*. This is all the more so because the NSA's activities seek to intercept only communications where one party is "linked to al Qaeda or an affiliated terrorist organization." *Id*.
- The NSA's activities also fall within the well-established exception to the warrant requirement that the President's inherent constitutional authority allows him to collect foreign intelligence without a warrant. *Id*., at pp. 3, 37, citing *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002).

- The "special needs" exception to the warrant requirement of the Fourth Amendment also allows the NSA's warrantless collection of information. *Id*. To fall within the "special needs" exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary general crime control. In support of its argument the DOJ points to a number of "special needs" cases obviating the warrant requirement, including some that include "suspicionless searches." *Id*., at pp. 38-40.

2. Arguments that NSA Activity is Unlawful.

72. Arguments stating that the NSA's activities are unlawful are summarized in a January 5, 2006, report issued by the Congressional Research Service.[72]

- Foreign intelligence collection is not among Congress's powers enumerated in Article I of the Constitution, nor is it expressly mentioned in Article II as a responsibility of the President. It is more likely that the power to collect intelligence resides somewhere within the domain of foreign affairs and war powers, and both are inhabited to some degree by the President together with the Congress. CRS Report, at pp. 3-4.

- The Constitution specifically gives to Congress the power to "provide for the common Defense," *U.S. Const. Art. I*, § 8, cl. 1; to "declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water," *Id*. § 8, cl. 11; "To raise and support Armies," and "To provide and maintain a Navy," *Id*. § 8, cls. 12-13;

---

[72] Congressional Research Service, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, January 5, 2006 [hereinafter CRS report], available at: http://www.fas.org/sgp/crs/intel/m010506.pdf.

While this report predates the DOJ report discussed above, the CRS report was written in response to a December 22, 2005, letter from Assistant Attorney General William E. Moschella to Chairman Roberts and Vice Chairman Rockefeller of the Senate Select Committee on Intelligence and Chairman Hoekstra and Ranking Minority Member Harman of the House Permanent Select Committee on Intelligence, which apparently raised many of the same arguments.

"To make Rules for the Government and Regulation of the land and naval Forces," *Id*. § 8, cl. 14, "To declare War," *Id*. § 8, cl. 1; and to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof," *Id*. § 8, cl. 18. CRS Report, p. 4, fn. 11.

- The President is responsible for "tak[ing] Care that the Laws [are] faithfully executed," Art. II, § 3, and serves as the Commander-in-Chief of the Army and Navy, *Id*. § 2, cl. 1. CRS Report, p. 4, fn. 11.
- The concurrence in *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579 (1952) (Jackson, J., concurring) [hereinafter *Youngstown*] remains the seminal case for analyzing presidential power. That case arose from President Truman's seizure of American steel mills during the Korean War in order to prevent a labor dispute from shutting down the mills.[73]
- *Youngstown* sets out the following framework:

> 1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. . . .
>
> 2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.

[73] The DOJ discussion of *Youngstown* can be found, in part, in DOJ Report, pp. 2, 11, 33-34. Based on the reasoning discussed above – that the President is acting with his inherent authority and Congressional approval – the DOJ concludes that the President is exercising his power under category one in the instant case. Therefore, he is exercising his maximum power under *Youngstown*.

> 3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.

CRS Report, at p. 5, quoting *Youngstown*, at 637-38 (footnotes and citations omitted).

- To ascertain where in the *Youngstown* framework the President's claimed authority to conduct the NSA programs might fall, it is necessary to determine whether Congress has spoken on the matter and assess how the Constitution allocates the asserted power between the President and Congress, if at all. *Id*., at pp. 5-6. If the Constitution forbids the conduct, such as U.S. Const. amend. IV, then a court has the ability and the duty to find the conduct invalid, even if the President and Congress have acted in concert. *Id*., at p. 6.
- In the absence of a constitutional bar, Congress's authorization is required, except in the rare case where the President alone is entrusted with the specific power in question. *Id*. In other words, the President may sometimes have the effective power to take unilateral action in the absence of any action on the part of Congress, but this does not be mean that the President possesses the inherent authority to exercise full authority in a particular field without Congress's ability to encroach – again, where Congress has concurrent authority. *Id*.
- *Dames & Moore v. Regan*, 453 U.S. 668 (1981) refined the *Youngstown* formula with respect to cases falling within the second classification, the "zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain."

Id. There, "Congress's implicit approval of the longstanding presidential practice of settling international claims by executive agreement was critical to its holding that the challenged actions were not in conflict with acts of Congress." *Id*., at p. 7, citing 453 U.S. at 680. The court also quoted a passage from *Youngstown*, saying "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned . . .may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II." *Id*., at p. 7, citing 453 U.S. at 686.

- Applying *Youngstown*, et. al., CRS concludes that the history of intelligence collection and its regulation by Congress suggests that the two political branches have never quite achieved a "meeting of the minds" regarding their respective powers. *Id*., at p. 7. While presidents have long contended that the ability to conduct surveillance for intelligence purposes is a purely executive function, have tended to make broad assertions of authority and have resisted efforts by Congress or the courts to impose restrictions, Congress has asserted itself with respect to domestic surveillance. *Id*. With regard to overseas surveillance, Congress has largely left matters to executive self-regulation, subject to congressional oversight and willingness to provide funds. *Id*.
- Here, the President's inherent presidential authority to conduct electronic surveillance is limited by the statutory language in FISA and its legislative history. *Id*., at pp. 27, 29. In FISA, Congress clearly stated its intention to limit any claim of inherent presidential authority to collect foreign intelligence information and required that FISA would be the exclusive mechanism for the conduct of such electronic surveillance. *Id*. For instance, previous bill language explicitly recognizing the President's inherent authority was deleted from 18 U.S.C. § 2511(3) and language was added Omnibus Crime Control and

Safe Streets Act that the FISA "procedures…shall be the exclusive means by which electronic surveillance…may be conducted." *Id.*, at pp. 27-28. Moreover, the House amendments to the bill provided that the procedures in the bill were to be the exclusive "statutory" means by which electronic surveillance and the interception of domestic wire and oral communications may be conducted. *Id.*, at p. 28.

- The House Conference Report, in accepting the Senate approach, stated, in part, that:

> The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter." *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952)

Id., p. 28. The Supreme Court has yet to rule on this matter but in the Conferee Report, Congress expressly expected it would.

- DOJ's citation to *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) for support of its inherent authority argument is without merit because that case makes only an "oblique" reference to the President's inherent authority without defining it. *Id.*, p. 32, citing 310 F.3d at 746. ("Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly…that FISA as amended is constitutional because the surveillances it authorizes are reasonable.").

- The Authorization for Use of Military Force (AUMF) and the *Hamdi* case do not change this analysis. *Id*., p. 34. Justice O'Connor's opinion in *Hamdi* expressly limited its holding, saying:

> [W]e understand Congress' grant of authority for the use of 'necessary and appropriate force' [through AUMF] to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel.

Id. at, p. 34, quoting *Hamdi*, at 520. Thus, there is reason to believe that AUMF's effect on prior statutory enactments, e.g., FISA, is limited to actual military operations on the battlefield as that concept is traditionally understood. *Id*.

- Justice O'Connor's plurality opinion confirms that the authorization to employ military force against an enemy army under AUMF necessarily encompasses the authority to capture battlefield enemies, because such captures are an essential aspect of fighting a battle. By implication, AUMF does not provide authority for activities aimed at citizens on American soil. *Id*., at pp. 35-37. *See, Hamdi* at 518:

> There can be no doubt that individuals who fought against the United States in Afghanistan as part of the Taliban, an organization known to have supported the al Qaeda terrorist network responsible for those attacks, are individuals Congress sought to target in passing the AUMF. We conclude that detention of individuals falling into the limited category we are considering, for the duration of the particular conflict in which they were captured, is so fundamental and accepted an incident to war as to be an exercise of the "necessary and appropriate force" Congress has authorized the President to use.

- The Supreme Court long ago held that the President has no implied authority to promulgate regulations permitting the capture of enemy property located in the United States during hostilities short of a declared war, even where Congress had authorized a

"limited" war. *Id*., at pp. 36-37, citing *Brown v. United States*, 12 U.S. (8 Cranch) 110 (1814); *Little v. Barreme*, 6 U.S. (2 Cr.) 170 125 (1804). In fact, FISA contains an exception to its requirements for 15 days after a congressional declaration of war. *Id*., at p. 37. The inclusion of this exception strongly suggests that Congress intended for FISA to apply even during wartime, unless Congress were to pass new legislation. *Id*. The fact that Congress amended FISA subsequent to September 11, 2001, in order to maximize its effectiveness against the terrorist threat further bolsters the notion that FISA is intended to remain fully applicable. *Id*. To conclude otherwise would appear to require an assumption that Congress intended the AUMF to authorize the President to conduct electronic surveillance, even against American citizens not involved in combat, under fewer restrictions than would apply during a declared war, notwithstanding FISA provisions strengthened to take such circumstances into account. *Id*. Therefore, even assuming, for argument's sake, that the NSA operations are necessary to prevent another terrorist attack, a presumption that Congress intended to authorize them does not necessarily follow. *Id*.

- Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests and Fourth Amendment rights. *Id*., at p. 7. However, the Supreme Court has long held that the Fourth Amendment protections extend to circumstances involving electronic surveillance of verbal communications without physical intrusion. *Katz v. United States*, 389 U.S. 347, 353 (1967). Indeed, the Omnibus Crime Control and Safe Streets Act of 1968 mandates that a search warrant be obtained in order to engage in electronic surveillance for law enforcement purposes. *Id*. at p., 8.

- While the *Katz* Court did not extend its holding to foreign surveillance, that issue was taken up by the U.S. Supreme Court in 1972 in *United States v. United States District Court*, 407 U.S. 297 (1972) (the Keith case). In other words, the limits of the foreign intelligence exception to the warrant requirement were discussed in *Keith*. The *Keith* case held that prior judicial approval was required to satisfy the Fourth Amendment if it involved domestic security surveillance and intelligence gathering. *Id*., at p. 9, citing 407 U.S. at 313-14, 317, 319-20. And while the Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents" [acting domestically], it invited Congress to establish statutory guidelines for such purposes. *Id*., at p. 10, quoting 407 U.S. at 321-22. Thus, with regard to domestic surveillance of foreign intelligence, the Court recognized Congress' role in establishing rules in matters that touch on national security, bolstering the role of FISA in determining the lawfulness of the NSA programs. *Id*.

D. The Military and State Secrets Privilege.

73. Assuming, *arguendo*, that a § 222 claim can be stated, the question of defenses must be examined. Of particular relevance here is the government's assertion of the military and state secrets privilege.[74] While such a privilege can only be asserted by the government, the practical effect of its application, if upheld by a court, is that any factual matters falling under the

[74] The ACLU has raised the question of whether a telephone company may also seek immunity under § 13(b)(3) of the Securities Exchange Act of 1934, 15 U.S.C. § 78m(b)(3). Under this provision, an agency head (including the Director of the National Security Agency) may immunize any public company from liability for false statements made in concealing matters of national security. This immunity, however, is likely limited to representations made in relation to a public company's issuance of stock and representations to current and prospective stockholders. *Lewis on Behalf of Nat. Semiconductor Corp. v. Sporck*, 612 F.Supp. 1316, 1333-34 (D.C.Cal. 1985) (Section 13(b)(2) enacted "to establish specific recordkeeping obligations for regulated corporations in order to aid the SEC in its fight against accounting mismanagement, and, if violations occur, the SEC or the Department of Justice may bring enforcement actions.) Therefore, we do not address this question here.

privilege will never see the light of day and therefore, there would likely be insufficient facts to sustain any allegations against telecommunications companies under § 222.

74. Similar to the discussion above regarding the lawfulness of the NSA activity, we look to summaries already compiled by others with regard to the applicability of this privilege in this case. This analysis starts with the argument that the military and state secret privilege does not apply.

1. Arguments that the military and state secrets privilege does not apply.

75. The American Civil Liberties Union (ACLU) has briefed this issue extensively in its case against the NSA in the Southern District of Michigan in opposition to the defendants' motion to dismiss. *ACLU et. al. v. NSA*, Case 2:06-cv-10204-ADT-RSW (S.D. Mich., filed January 17, 2006) [Hereinafter "ACLU Response"]. The ACLU's arguments are summarized as follows:

- The state secrets privilege is a common law evidentiary rule that permits the government to "block discovery in a lawsuit of any information that, if disclosed, would adversely affect national security." ACLU Response, at p. 10 quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983). It is employed to protect against disclosure of information that will impair "the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign governments." *Id*., at pp. 10-11, quoting *Ellsberg* at 57.
- It is a rule of evidence, not of justiciability, and is intended to protect from disclosure only such evidence as would legitimately cause harm to national security. *Id*., at p. 11, citing *Ellsberg*, 709 F.2d at 57 (the privilege may not be used to "shield any material not strictly necessary to prevent injury to national security . . . .").

- It is essential for the courts to "ensure that the state secrets privilege is asserted no more frequently and sweepingly than necessary" and thus courts must critically examine "the instances of its invocation." *Id*., quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983).
- Courts have not hesitated to reject state secrets claims where the invocation of the privilege was inappropriate or untimely. *Id*., at pp. 9-10, citing *Jabara v. Kelly*, 75 F.R.D. at 492-93. In *Jabara*, the court rejected application of the privilege to "relevant factual information pertaining to the 'arrangement' by which the FBI had requested and obtained information about the plaintiff from the [NSA]," the "'general' manner such information was ultimately used by the FBI," and the name of the agency (NSA) that intercepted plaintiffs communications without a warrant." *Id*., at 10 quoting *Jabara* at 492-93.
- Similarly, the privilege was rejected in *In re United States*, 872 F.2d at 478 as premature and overbroad. *Id*. Moreover, in *Ellsberg*, 709 F.2d at 60, the court rejected a claim of privilege over the name of the Attorney General who authorized the warrantless wiretapping, explaining that no "disruption of diplomatic relations or undesirable education of hostile intelligence analysts would result from naming the responsible officials." *Id*., quoting *Ellsberg*.
- The D.C. Circuit has cautioned: "Because evidentiary privileges by their very nature hinder the ascertainment of the truth, and may even torpedo it entirely, their exercise should in every instance be limited to their narrowest purpose." *Id*., quoting in *In re United States*, 872 F.2d at 478-79 (internal quotation marks omitted).

- The Supreme Court outlined the proper use of the state secrets privilege fifty years ago in *United States v. Reynolds*, 345 U.S. 1 (1953). *Id.* In *Reynolds*, the family members of three civilians who died in the crash of a military plane in Georgia sued for damages. *Id*. In response to a discovery request for the flight accident report, the government asserted the state secrets privilege, arguing that the report contained information about secret military equipment that was being tested aboard the aircraft during the fatal flight. *Id*. The Court held that the privilege could be invoked only upon "a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer" and there must be a "reasonable danger" that disclosure will harm national security. *Id*, quoting *Reynolds*, at 7-8, 10.
- The *Reynolds* Court upheld the claim of privilege over the accident report, but it did not dismiss the suit. *Id*. To the contrary, it remanded the case for further proceedings, applying a very sharp analysis to what exactly was necessarily secret and what was not, saying:

> There is nothing to suggest that the electronic equipment, in this case, had any causal connection with the accident. Therefore, it should be possible for respondents to adduce the essential facts as to causation without resort to material touching upon military secrets. Respondents were given a reasonable opportunity to do just that, when petitioner formally offered to make the surviving crew members available for examination. We think that offer should have been accepted.

Id., pp. 11-12, quoting *Reynolds*, 345 U.S. at 11. Upon remand, plaintiff's counsel deposed the surviving crew members, and the case was ultimately settled. *Id*.

- In the majority of cases since *Reynolds*, courts have considered the state secrets privilege in response to particular discovery requests, not as the basis for wholesale dismissal of legal claims concerning the facial legality of a government program. *Id*., at pp. 12-13,

citing *Jabara*, 75 F.R.D. at 478-79, 490 (privilege asserted in response to discovery requests).[75] Thus, the typical result of the successful invocation of the states secrets privilege is simply to remove the privileged evidence from the case but to permit the case to proceed. *Id*., at p. 13.

- The government's broad view of the state secrets doctrine, if accepted, would present another serious violation of the separation of powers because it would immunize executive action from judicial scrutiny. *Id*, at p. 3.
- The executive branch cannot disable, by unilateral fiat, the power of Article III courts to be the ultimate arbiters of the law and the Constitution. *Id*., pp. 4, citing *Marbury v. Madison*, 1 Cranch 137, 177 (1803) (it is "the province and duty of the judicial department to say what the law is"); *City of Boerne v. Flores*, 521 U.S. 507, 524 (1997) (the "power to interpret the Constitution in a case or controversy remains in the Judiciary"); *Legal Services Corp. v. Velazquez*, 531 U.S. 533, 545 (2001) ("Interpretation of the law and the Constitution is the primary mission of the judiciary when it acts within the sphere of its authority to resolve a case or controversy").
- The courts should assess the government's state secrets claim with these precedents and principles in mind. *Id*., at p. 9. Ultimately, only the Court can ensure that plaintiffs are not unnecessarily denied their "constitutional right to have access to the courts to redress violations of [their] constitutional and statutory rights." *Id*., quoting *Spock v. United States*, 464 F. Supp. 510, 519 (S.D.N.Y. 1978). "Meaningful access to the courts is a fundamental right of citizenship in this country. Indeed, all other legal rights would be

[75] The ACLU cites multiple cases for this proposition. *See Id*., at p. 12, fn. 27.

illusory without it." *Id*., quoting *Martin v. Lauer*, 686 F.2d 24, 32 (D.C. Cir. 1982) (internal citations and quotations omitted).

- The Supreme Court has cautioned that judicial control in a case "cannot be abdicated to the caprice of executive officers." *Id*., quoting *Reynolds*, 345 U.S. at 9-10. It is "the courts, and not the executive officer claiming the privilege, who must determine whether the claim is based on valid concerns." *Id*., quoting *Jabara v. Kelley*, 75 F.R.D. 475, 484 (E.D. Mich. 1977). A 'court must not merely unthinkingly ratify the executive's assertion of absolute privilege, lest it inappropriately abandon its important judicial role." *Id*, quoting *In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989). Arguments that the military and state secrets privilege does apply.

76. The United States Government has also briefed this issue extensively in a lawsuit brought in the Northern District of California. It is this privilege that dominates the government's motion to dismiss in *Hepting, et. al. v. AT&T*, C-06-0672-VRW (N.D. CA, January 30, 2006). The government's arguments below are derived from its Reply Brief in that case, dated June 16, 2006. [hereinafter U.S. Reply].[76] We summarize those arguments here.

- The government invokes the military and states secrets privilege based on determinations by the Director of National Intelligence and the Director of the National Security Agency that the lawsuit entails the disclosure information that will cause harm to the national security interests of the United States. U.S. Reply, at p. 1. Indeed, no aspect of this case can be litigated without disclosing state secrets. *Id*.

[76] The government's extensive motion to dismiss, along with supporting declarations of government officials (including Director of National Intelligence John D. Negroponte) was filed on May 13, 2006.

- The United States has not lightly invoked the state secrets privilege, and the weighty reasons for asserting the privilege are apparent from the classified material submitted in support of its assertion. *Id*. The need to protect against the harm to national security that would arise from the disclosure of classified information, however, makes it impossible for the United States to explain on the public record more precisely what those reasons are. *Id*. To allow the court to fully consider the details of the government's state secrets privilege assertion, it has, at least in the Southern District of Michigan case, included material for in *camera, ex parte review*. *Id*.
- Furthermore, an assertion that the Court should defer determination of whether the privilege applies because a prima facie case can be made on materials available in the public record reflects a fundamental misconception of the scope, nature and effect of the government's invocation of the state secrets privilege. *Id*., at p. 2. As described in the United States' public filing and in the supporting classified materials, state secrets are central to the plaintiffs' allegations and any attempt to proceed with the litigation will threaten the disclosure of privileged matters. *Id*. Plaintiffs simply cannot prove their prima facie case without resort to classified material.
- If "the 'very subject matter of the action' is a state secret, then the court should dismiss the plaintiff's action based solely on the invocation of the state secrets privilege." *Id*., at pp. 13-14, quoting *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) (citing *United States v. Reynolds*, 345 U.S. 1, 11 n.26 (1953); *Totten v. United States*, 92 U.S. 105, 107 (1875) ("[P]ublic policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not

allow the confidence to be violated."); *Tenet v. Doe*, 544 U.S. 1,8 (2005) (applying *Totten* to bar a suit brought by former Soviet double agents seeking to enforce their alleged employment agreements with the CIA and making clear that the *Totten* bar applies whenever a party's "success depends upon the existence of [a] secret espionage relationship with the government"). In such cases, the state secrets are "so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters." *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1241-42 (4th Cir. 1985). *Id*., at p. 14. For the reasons discussed in the Government's *in camera, ex parte* filing, the very subject matter of Plaintiffs' allegations is a state secret and further litigation would inevitably risk their disclosure. *Id*.

- The government's privilege assertion covers any information that tends to confirm or deny (a) the alleged intelligence activities, (b) whether AT&T was involved with any such activity, and (c) whether a particular individual's communications were intercepted as a result of any such activity. *Id*., at p. 15, citing Declaration of John D. Negroponte, Director of National Intelligence. Because such information cannot be confirmed or denied without causing exceptionally grave damage to the national security, plaintiffs' attempt to make out a prima facie case would run into privileged information. *Id*. Where, as here, a plaintiff cannot make out a prima facie case in support of its claims absent the excluded state secrets, the case must be dismissed. *Id*., at p. 16 citing *Kasza*, 133 F.3d at 1166; *Halkin II*, 690 F.2d at 998-99; *Fitzgerald*, 776 10 F.2d at 1240-41.

- The analysis is not limited to determining whether a prima facie complaint exists since where the state secrets privilege "'deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant.'" *Id*. at, pp. 16-17 citing *Kasza*, 133 F.3d at 1166 (quoting *Bareford v. General Dynamics Corp*., 973 F.2d 1138, 1141 (5th Cir. 1992)) and citing *Molerio v. Fed. Bureau of Investigation*, 749 F.2d 815,825 (D.C. Cir. 1984) (granting summary judgment where state secrets privilege precluded the Government from using a valid defense).
- In this case - as noted in the United States' public brief and as demonstrated in the *in camera, ex parte* materials - neither AT&T nor the government could defend this action on the grounds that, among other things, the activities alleged by the Complaint (i) were authorized by the Government; (ii) did not require a warrant under the Fourth Amendment; (iii) were reasonable under the Fourth Amendment; or (iv) were otherwise authorized by law. *Id*., at p. 17.
- An assertion that a court adjudicate whether AT&T received any certification or authorization from the Government relating to the alleged surveillance activity is without merit. *Id.* The state secrets assertion "covers any information tending to confirm or deny" whether "AT&T was involved with any" of the "alleged intelligence activities." *Id*. Clearly, the existence or non-existence of any certification or authorization by the Government relating to any AT&T activity would be information tending to confirm or deny AT&T's involvement in any alleged intelligence activity. *Id.* Thus, any such activity would fall within the Government's state secrets assertion, and the Court could not adjudicate, or allow discovery

regarding, whether any Government certification or authorization exists without considering the Government's assertion of the state secrets privilege. *Id.*

- An assertion that the government must make a more specific - i.e., public - showing about the information subject to the state secrets privilege is also without merit. *Id*. Requiring such a showing would be improper where, as here, it would "force 'disclosure of the very thing the privilege is designed to protect.'" *Id*., at pp. 17-18, quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 63 (D.C. Cir. 1983) (quoting *United States v. Reynolds*, 345 U.S. 1, 8 (1953)).

E. The WUTC Lacks the Jurisdiction to Decide Whether The NSA Program is Lawful Such that a Request for CPNI is "Required by Law" under § 222 and Whether the Military and State Secrets Privilege Applies in this Case.

77. The threshold matter presented by the questions in the Commission's notice is whether the Commission has the authority to determine the federal questions reviewed above, that is: (1) whether the disclosure of CPNI by regulated telecommunications carriers to the United States Government occurred pursuant to the "as required by law" exception to § 222 of the Telecommunications Act of 1996 and (2) if not, whether the military and states secret privilege may be properly invoked.

78. The Commission is a state agency created by the Legislature and so it enjoys only those powers expressly conferred by statute or necessarily implied from its statutory delegation of authority. *Wash. Indep. Tel. Ass'n; v. WUTC*, 110 Wn. App. 147, 155, 159 (2002), citing *In re Registration of Elec. Lightwave, Inc*., 123 Wn.2d 530, 536 (1994).

79. Here, the question is not whether the WUTC has jurisdiction over telephone companies release of CPNI. There is no question that the Commission possesses such authority**.** *See, supra*, 17 F.C.C.R. 14820 (July 2002), at ¶ 71; Order R-505, Docket UT-990146. The question is whether the WUTC, in order to reach issues clearly within its purview, has the authority to

resolve the threshold issues of (1) the lawfulness of the NSA program and the carriers' participation in the program and (2) the government's invocation of the state secrets privilege and the carrier's assertion that it enjoys the penumbra of the privilege. We can find nothing within the express authority granted by the Legislature or necessarily implied from its statutory delegation of authority that would allow the Commission to decide these two questions.

80. RCW 80.01.040 outlines the general powers and duties of commission. That statute gives the Commission the authority to exercise "all the powers and perform all the duties prescribed therefor by this title [Title 80] and by Title 81 RCW, or by any *other law*." Titles 80 and 81 contain no provisions allowing the Commission to resolve the NSA and state secrets privilege matters. There exist no powers or duties under "other law" granting the Commission authority on these questions. Nor can the Commission's authority be implied from Titles 80 and 81.

81. Indeed, with regard to complex issues of federal law, the Washington Supreme Court specifically endorsed a Commission decision not to act until federal law was clearly established. *Willman v. Washington Utilities and Transp. Com'n,* 154 Wn.2d 801, 807 (2005). In *Willman,* the Commission was presented with the question of whether a Yakama Nation tribal franchise fee could be passed through to ratepayers by utilities serving the Nation, in the same manner as a municipal tax. *Id*. at 804.

82. Opponents to the collection of the tax argued that the tax was presumptively invalid under federal Indian law. *Id*., at 806. The Commission held that the tax could be collected by the utilities and passed-through to ratepayers so long as it was not "clearly invalid." *Id*. (a tax is a prudent expense unless the tax is "clearly invalid"). The Commission argued that the logical conclusion of the opponent's reasoning would require the WUTC to analyze the complexities of

federal Indian tax law in every case. *Id*., at 807.[77] The Washington Supreme Court agreed, observing that:

> Determining the validity of an Indian law tax involves complex issues of federal law. Since such analysis is outside the expertise and normal review of the WUTC, it has adopted a standard that *presumes validity* unless clearly shown to the contrary by federal law.

154 Wn.2d at 807 (emphasis in original). The Commission went on to hold:

> We agree with the WUTC that instead of diving into the complexity of federal Indian law tax analysis, the WUTC and this court must primarily apply Washington State law, thereby requiring utilities to pay only prudent expenses…By keeping indepth [sic] federal Indian law analysis in the federal courts, the role of state administrative agencies is more clearly delineated.

Id., at 808.

83. Had the federal Indian law issue been resolved in the proper forum, and the tax had been held invalid, the Supreme Court noted that Commission should have taken action to protect customers by removing the charge from bills. *Id*. at 808. ("This presumptive validity test *still* would allow for the petitioners to obtain a federal court disposition in their favor, thereby showing the tax is "clearly invalid," and, at which point, the WUTC *must* remove it from ratepayers' bills) (emphasis added).

84. The Commission in this case finds itself an analogous position to the *Willman* case, where the Commission's ratemaking authority clearly gave it jurisdiction over the inclusion of taxes in a utility's charges. *Id.*, at 806. However, it faced practical and legal limitations on its authority when asked to adjudicate the validity of a tax imposed by an entity governed exclusively by a unique area of federal law – one which was outside of its expertise and normal purview.

85. It is undisputed that the validity of the NSA program and the government's invocation of the state secrets privilege raise complex issues of federal statutory and constitutional law. These

[77] The Commission took the position that it did not have the authority to determine the validity of the tax and that complaining ratepayers could challenge the tax in an appropriate forum such as tribal or federal court, and that the Commission would then apply that decision. *Willman v. WUTC*, 122 Wn. App. 194, 201 (The Court of Appeals also affirmed the WUTC position).

issues have been raised in and will likely be resolved by the federal courts. Like *Willman*, here, while the Commission clearly has jurisdiction over portions of the issue regarding unlawful disclosure of CPNI and over those companies allegedly involved, complex issues of federal law must be resolved in order for it to proceed. Once those issues are resolved, however, as in *Willman* the Commission can exercise its authority to investigate and take action against unlawful carrier conduct.[78]

IV. THE COMMISSION'S QUESTIONS

1. Does WAC 480-120-202 or any other state law or regulation prohibit a regulated telephone company or its affiliated interests from providing customer telephone calling information to the National Security Agency (NSA)?

86. Absent the NSA's role in the factual allegations of this case, the telephone companies' disclosure of CPNI appears to be unlawful. In addition, based on Public Counsel's review of the legal arguments on the NSA issues, there appear to be a substantial basis to question the lawfulness of the NSA's request for telephone records and the carrier's cooperation with the program.

87. Whether WAC 480-120-202, the FCC Rules or § 222 itself prohibit telephone companies from providing CPNI turns entirely on whether the NSA's request was lawful. This remains to be resolved by the courts.

[78] *See also, Moore v. Pacific Northwest Bell*, 34 Wn. App. 448 (1983)(doctrine of primary jurisdiction does not apply to deprive court of jurisdiction over negligence claim against telephone company where WUTC has "neither the power to grant the relief…nor special competence over the subject matter." *Id.* at 451-455). A number of federal cases have addressed the scope of state commission jurisdiction over federal issues. *See e.g., Evans v. New York State Public Service Commission*, 287 F.3d 43, 46-47 (2d Cir. 2002)(federal court jurisdiction over constitutional and statutory claims not related to rates is not barred by Johnson Act); *United States v. Alaska Public Utilities Commission*, 23 F.3d 257, 259 (9th Cir. 1994)(application of an Alaska PUC procedural statute to federal government is an unconstitutional exercise of state power in violation of the Supremacy Clause); *McGee v. East Ohio Gas Company*, 111 F. Supp. 2d 979, 985 (SD Ohio 2000)(Ohio PUC jurisdiction over rates and services does not extend to claim under federal Equal Credit Opportunity Act).

2. Does the Commission have the legal authority to compel a regulated telephone company or its affiliates to disclose whether it has provided customer calling information to the NSA?

88. The Commission may generally compel a regulated telephone company to disclose whether it has given CPNI to a third party. *See e.g.*, RCW 80.04.050 (power to compel the attendance of witnesses at any place within the state); RCW 80.04.060 (right to take the testimony of any witness by deposition); RCW 80.04.070 ("the right, at any and all times, to inspect the accounts, books, papers and documents of any public service company, and … may examine under oath any officer, agent or employee of such public service company in relation thereto, and with reference to the affairs of such company").

89. Here, it is likely that such a request will be met by an assertion of the state secrets privilege as well as assertions by telephone companies that federal law related to national security concerns bar them from disclosing such information.[79] As the review above indicates, however, there are substantial questions about the scope of the privilege. It is far from clear that the privilege bars disclosure by telephone companies of *all* facts relevant to this matter. For example, to the extent that the program has been publicly disclosed and acknowledged, there may been a waiver or partial waiver of the privilege. In that case, the fact of a company's participation in the program and a company's acknowledgement that CPNI was released (information already within the public domain), would involve only the telephone companies, and would be sufficient to bring a complaint for violation of WAC 480-120-202.

90. Nevertheless, because of the scope of the state secrets privilege and the telephone companies' role in relation to that privilege remains to be resolved by the courts, the

[79] For example, in its letter to the Commission dated May 26, 2006, AT&T identified a number of statutory prohibitions. AT&T Letter, pp. 4-5. For example, it is a federal felony for any person to divulge classified information "concerning the communication intelligence activities of the United States" to any person not authorized to receive such information. Additionally, there are other statutory prohibitions on divulging information or records pertaining to surveillance activities undertaken pursuant to FISA or ECPA and the activities of the NSA. See, 18 U.S.C. § 798; 50 U.S.C. §§ 1805(c)(2)(B),(c); 18 U.S.C. § 2511(2)(a)(ii)(B); and 50 U.S.C § 402 note. Whether these statutes apply will also likely turn on the lawfulness of the NSA's actions.

Commission cannot, at this time, compel a telephone company to disclose whether it provided CPNI to the NSA.

3. Does the Commission have the legal authority to compel regulated telephone companies or their affiliates to release relevant information about such allegations?

91. The government has asserted the states secret privilege in response to both the *existence* of the program as well as its *contours*. These issues must be resolved before the Commission can proceed.

4. Would an assertion of the military and state secrets privilege by the United States Government preclude the Commission from taking action against a regulated telecommunications company?

92. We do not believe that the mere assertion would preclude the Commission from acting. As a practical matter, however, if the Commission sought to take action in the case of an assertion of the privilege, it would likely be enjoined from proceeding until the privilege is determined to apply.

5. If the Commission decides to investigate the matter raised in the ACLU's May 25, 2006, letter, which procedural options would be most appropriate? (*e.g.*, informal investigation, formal investigation, complaint).

93. Public Counsel, having concluded that the Commission may not bring a complaint against or seek information from telephone companies related to release of CPNI to the NSA, makes the following recommendations.

94. First, the Commission should keep the docket open as an investigation until the federal issues are resolved. To that end, the Commission should monitor ongoing legal developments on this matter. Once there is clearly established law stating that the NSA's request was unlawful and telecommunications companies may disclose their participation in the program, the Commission should initiate its own complaint and convert the proceeding to an adjudication.

95. Second, and in the meantime, the Commission should use the docket to monitor and collect factual information within the public domain, this includes requiring all licensed telephone companies in Washington to provide the Commission with information regarding their privacy policies, and in particular, those related to consent.[80]

96. Third, the Commission should immediately exercise its authority under WAC 480-120-202 and RCW 80.04.090 to order all telecommunications companies all telecommunications companies registered in Washington to preserve all evidence related to the disclosure of CPNI to the NSA. This should include evidence dating back to September 2001 and any future disclosure. Specifically, companies must set aside all records, accounts, memoranda, receipts, expenditures of money and every other tangible piece of evidence that is remotely related to the allegations in this case. In other words, this evidence must be kept at the ready, to be produced if when the Commission has clear authority to proceed.

97. In addition, the Commission should order all telecommunications companies registered in Washington to identify internally those witnesses with knowledge regarding this matter. These witnesses should include those people with information back to September 2001 as well as those gaining information about this matter in the future. Specifically, this includes any of the following with knowledge: the companies' officers, directors, shareholders, owners, agents, servants, employees, sales representatives, attorneys, corporations, subsidiaries, affiliates, successors, assigns, any other individual or entity acting or purporting to act on its behalf as well as those, listed above, over which the companies' exercise control. The companies must keep and maintain the list, along with up to date contract information, so that it will be at the ready if and when such matters become ripe for resolution by this Commission.

[80] *See*, RCW 80.36.320(2)(d) (competitive companies must "[c]ooperate with commission investigations of customer complaints").

98. The Commission jurisdiction to impose the obligation to preserve evidence is well established by its authorizing statutes and its regulations. RCW 80.04.090 empowers the Commission to, in its discretion:

> …prescribe the forms of any and all accounts, records and memoranda to be kept by public service companies, including the accounts, records and memoranda of the movement of traffic, sales of its product, the receipts and expenditures of money… The commission may, in its discretion, prescribe the forms of any and all reports, accounts, records and memoranda to be furnished and kept by any public service company whose line or lines extend beyond the limits of this state, which are operated partly within and partly without the state, so that the same shall show any information required by the commission concerning the traffic movement, receipts and expenditures appertaining to those parts of the line within the state.

Id. Similarly, RCW 80.04.100 allows the Commission to force the production of out-of-state books and records including, "accounts, papers or records kept by any public service company in any office or place without this state, or at the option of the company verified copies thereof, so that an examination thereof may be made by the commission or under its direction." WAC 480-120-349 requires that companies must keep all records and reports "required by these rules or commission order for three years" unless these reports are covered by FCC rule, 47 CFR, Part 42 and the FCC provisions require a different time period for retention. The Washington rule also prohibits the destruction of records "before the expiration of three years" unless the record falls under Part 42. *Id*.

99. Moreover, the Commission's own CPNI rule, WAC 480-120-202, incorporates by reference 47 CFR §§ 64.2003 through 64.2009. Section 64.2009 requires that telecommunications carriers must "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI." *Id*. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. *Id*. Carriers shall retain the record for a minimum of one year. *Id*.

100. Therefore, Public Counsel recommends that the Commission exercise its broad authority in this area to preserve evidence relevant to this matter.

V. CONCLUSIONS

101. While we perceive serious questions about the lawfulness of the telecommunications companies' disclosures of CPNI and the application of the military and states secrets privilege in this context, the federal courts must ultimately decide these issues. However, because the WUTC is not foreclosed from exercising its substantial authority in those areas unrelated to the federal law issues, Public Counsel recommends the following (1) that the Commission keep the docket open as an investigation; (2) that the Commission monitor ongoing factual and legal developments about this matter; (3) that the Commission issue an order directing telecommunications companies registered in Washington to provide details of their privacy

/ /

/ / /

/ / / /

policies; and (4) That the Commission issue an order directing all telecommunications companies registered in Washington to preserve evidence in the event that the NSA program is found to be unlawful and the military and states secret privilege inapplicable.

DATED this 30TH day of June, 2006.

ROB McKENNA
Attorney General

Simon ffitch
Assistant Attorney General
Public Counsel

JUDITH KREBS
Assistant Attorney General
Public Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Regulations

Constitutional Provisions

Commission Orders