ELECTRONICALLY FILED ON JUNE 30, 2006

STATE OF MAINE
PUBLIC UTILITIES COMMISSION

JAMES D COWIE, ET AL.	**)**	
	)	
RE: Request for Commission Investigation	**)**	**PUBLIC ADVOCATE'S**
Into Whether Verizon is Cooperating in Maine	**)**	**SECOND SET OF COMMENTS**
With the National Security Agency's	**)**	
Warrantless Domestic Wiretapping Program	**)**	**June 30, 2006**
	)	
Docket No. 2006-274	**)**	

THIS IS A VIRTUAL DUPLICATE OF THE ORIGINAL HARDCOPY SUBMITTED TO THE COMMISSION IN ACCORDANCE WITH ITS ELECTRONIC FILING INSTRUCTIONS

In his Procedural Order issued June 23, 2006, the Presiding Officer asked the parties to make recommendations about the process the Commission should adopt to resolve whether federal law precludes, at a minimum, an investigation by the Maine Public Utilities Commission into whether Verizon's has violated any of the following:

a) Section 7 of Chapter 290 of the Commission's consumer protection rules requiring Verizon to comply with the Federal Communication Commission's customer Proprietary Network Information Rules, 47 CFR §§ 64.2001-2009);

b) 35-A M.R.S.A. § 7101-A(2) (providing a right on the part of telephone subscribers to limit the dissemination of their telephone numbers to persons of their choosing); or

(c) 35-A M.R.S.A. § 7101-A(1) (Maine telephone subscribers have a right to privacy).

The answer to the Presiding Officer's question is no. Neither the federal statutes cited by Verizon in its Response, nor the "state secrets" privilege, prevent the Commission from obtaining the critical information that is relevant to the investigation requested by the Complainants.

The Complaint asks the Commission to determine whether Verizon, by participating in the government's network surveillance program, is violating either state or federal laws. Those state and federal laws limit the extent to which the telephone companies can disseminate customer information and telephone numbers. Federal law also strictly prohibits interception of communications without a court order. It requires that telephone companies refuse to help the government to listen in to citizens' communications without a court's approval. When it created the statutory scheme, Congress recognized that telecommunications providers occupy a pivotal role in protecting their customers' privacy interests[1]. In contrast to those whose houses are searched, customers who are subject to electronic surveillance[2] rarely learn that someone has listened to their telephone conversations without authorization. For that reason, Congress required that telecommunications providers make sure that any surveillance is properly authorized. Verizon and other providers face strict penalties for ignoring that responsibility.

[1] Telecommunications carriers like Verizon stand as the principal barrier between the government's desire to obtain private communications and their subscribers' right to privacy in those communications. That is why the law places a heavy burden on such carriers. They can permit violations of their customers' privacy only when the government couples its request for an interception with an independent and impartial arbiter's assessment that the privacy violation is warranted.

[2]Compared to one-shot physical searches for which a traditional warrant usually suffices, electronic surveillance is intrusive, continuous, hidden and indiscriminate. Electronic surveillance divulges a wide range of private information over a significant period of time, unbeknownst to the target of that surveillance.

A. The State Secret Privilege Will Not Prevent the Commission From Obtaining Information on the Simple Question of Whether Statutes Have Been Violated

The inquiry that the Maine Commission must make is quite simple. If Verizon intercepted its customers' communications, it violated federal electronic surveillance law.[3] If Verizon gave out customers' proprietary information, it violated both state and federal laws against such disclosure.

For Verizon, liability attaches regardless of what Verizon did afterwards with the intercepted communications and independent of the entity to whom the proprietary information was given. While the government's role in those violations may be an important part of public discourse, the government's actions are not implicated here.[4] The Complainants are asking the Commission to investigate simply whether Verizon has violated the law. In order to determine whether Verizon's actions are violating the law, the Commission need not inquire into the details of the NSA's intelligence policies. The law asks only if there was an intentional interception of a wire, oral or electronic communication. It does not matter to the interception claim that Verizon

[3] The statute is violated when an entity intercepts a communication regardless of what it subsequently does with the contents of the communication intercepted. *See Jacobson v. Rose, 592 F.2d 515, 522 (9th Cir. 1978); United States v. Councilman 418 F.3d 67, 84 (1st Cir. 2005).* In this case, Verizon's violation of 18 U.S.C. § 2511(1)(a) would arise from their inception of Plaintiffs' communications without a court order. For purposes of determining whether Verizon has violated the statute, it is not necessary to focus on the recipient to whom they provided the communications, or on what the recipient did with the information. The Commission does not need to know what information, if any, was turned over to the government, or how the government used the information, in order to find that Verizon has violated § 2511(1)(a).

[4] In its Response, filed May 19, 2006, Verizon asked the Commission to dismiss the ten-person complaint because the Commission will not be able to "adduce any facts" relating to the allegations that Verizon has violated state and federal law by cooperating with the NSA Surveillance Program. However, Verizon's Response appears to misstate what the case here is actually about. The Complainants are not asking for information concerning how the NSA collects intelligence, nor do the Complainants seek details about how the NSA may engage in "data-mining" of telephone and e-mail traffic -- an activity that has already been widely publicized. Instead, the Complainants here are focusing on whether Verizon's activities have violated certain state and federal statutory schemes.

allegedly forwarded the communications to the NSA. It is the capture of the information itself, not the forwarding that the statute prohibits. *See: United Stated v. Councilman, 418 F.3d 67(1st Cir. 2005).*

In short, the central issue in this case in simply whether Verizon's actions have violated well-defined statutory prohibitions against intercepting and disclosing customers' communications. The state secrets privilege will not prevent the Commission from obtaining information that is relevant to that inquiry. For instance -- from Verizon's point of view -- proving that Verizon has a valid defense for intercepting their subscribers' communications does not require disclosure of state secrets. If Verizon does not dispute the allegations that it has violated 18 U.S.C. § 2511(1)(a), it may defend its actions by establishing that it acted pursuant to a court order under 18 U.S.C. § 2518. In the absence of a valid court order, Verizon may produce an invalid court order that it relied upon in good faith. *See 18 U.S.C. § 2520(d).* If Verizon is unable to establish either of those defenses, then it has violated 18 U.S.C. § 2511. Proving either of these defenses requires that Verizon produce a court order. An *in camera* review of that order would not disclose state secrets. For that reason, the Commission should open its investigation and begin to gather the relevant facts

B. The Congress has Limited the Application of the "State Secrets" Privilege in Cases Involving Electronic Surveillance.

In the area of electronic surveillance, Congress has narrowed the common law "state secrets" privilege by a statute that "speaks directly to the question otherwise answered by federal common law." *Kasza v. Browner, 113 F.3d 1159, 1167* (9th Cir. 1988) (quoting *County of Oneida v. Oneida Indian Nation, 470 U.S. 226, 236-37 (1985)* (quoting *City of Milwaukee v. Ill.,*

451 U.S. 304, 315 (1981))) (quotation marks and brackets omitted). In particular, Congress created FISA as the "exclusive means by which electronic surveillance … may be conducted." *18 U.S.C. § 2511(2)(f)* (emphasis added). It adopted FISA "to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." *S.Rep. No. 95-604(I), at 8, 1978 U.S.C.C.A.N. at 3910.* In other words, the government cannot use the common-law state secrets privilege to squelch Congressionally-mandated rights regarding violations of the electronic surveillance statutes.

More specifically, Congress has provided for discovery of classified material pertinent to the legality of electronic surveillance in 50 U.S.C. §§ 1806(f) and 1845(f). Congress has also enacted provisions governing disclosures where the state secrets privilege is applicable and even where the government believes the disclosure would harm national security. *50 U.S.C. § 1806(f).* The law provides:

> Whenever any motion or request is made by an aggrieved person … to discover or obtain applications or orders or other materials relating to electronic surveillance … the United States district court … shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Id. (emphasis added).

C. Neither Verizon Nor the Government Cannot Retroactively Transform Non-Secret Information Into a State Secret.

In its Response, Verizon asks the Maine Commission to decline to decide whether Verizon has violated the law because the case implicates state secrets. However, based on recent news reports and the allegations now before the Commission, many of the questions about whether Verizon is intercepting customers' calls or disclosing customers' proprietary information may be decided based on information that is publicly available and on admissions that have been made by government officials. That information remains available to the Commission.

The state secrets privilege does not bar from the courtroom information that already is in the public domain. *See Spock v. U.S., 464 F. Supp. 510, 518 (S.D.N.Y. 1978).* In *Spock*, the plaintiff sued the government for unlawful interception of his oral, wire, telephone and telegraph communications. *Id. at 512.* As Verizon has argued here, the government in *Spock* argued that the case had to be dismissed because "defendants can neither admit nor deny the allegations of the Complaint without disclosing state secrets." *Id. at 519.* The plaintiffs countered that "[t]his one factual admission or denial … reveals no important state secret, particularly since the interception of Dr. Spock's communications was previously disclosed in an article in the *Washington Post*, dated October 13, 1975." *Id*. The court agreed with plaintiffs and declined to dismiss the case:

> [h]ere where the only disclosure in issue is the admission or denial of the allegation that interception of communications occurred, an allegation which has already received widespread publicity, the abrogation of the plaintiff's right of access to the courts would undermine our country's historic commitment to the rule of law.

Id. at 520; *see also Capital Cities Media, Inc. v. Toole, 463 U.S. 1303, 1306 (1983)* (noting Court has not "permitted restrictions on the publication of information that would have been available to any member of the public"); *MeGehee v. Casey, 718 F.2d 1137, 1151 (D.C. Cir. 1983)* (noting "[t]he government has no legitimate interest in censoring unclassified materials" or "information … derive[d] from public sources.).

The principle that the government cannot engage in after-the-fact reclassifications of non-secret information as "state secrets" certainly applies in this case. Here, many of the key facts have not only been the subject of widespread publicity, but they have also been confirmed in statements made by government officials. In short, the state secrets privilege will not prevent the Commission from obtaining the information that it needs in the course of its investigation.

D. The Statutory Provision Verizon Cites Regarding The NSA Does Not Provide a Blanket Prohibition On The Disclosure Of Information

Verizon argues "Congress has made clear that 'nothing in [the NSA Act] … *or any other law* … shall be construed to require disclosure of … any function of the National Security Agency, [or] of any information with respect to the activities thereof." *Verizon Response* at 3. (citing 50 U.S.C. § 402 note (*emphasis added*)).

While Section 6 of the NSA Act, 50 U.S.C. § 402, provides for the protection of certain NSA functions and activities related to national secrets, it does not conflict with other statutes such as 18 U.S.C. § 1806(f) of FISA and 18 U.S.C. § 2511(2)(a)(ii)(B) of the Wiretap Act which, as outlined by the Public Advocate in its initial comments, deal with access to classified material

that concerns electronic surveillance activity where the legality of the surveillance program is at issue. For example, as we noted in Section C above, parties may seek information through the discovery process that Congress has specifically made discoverable under 18 U.S.C. § 1806(f) which deals with electronic surveillance. Similarly, as the Public Advocate noted in its initial comments, 18 U.S.C. § 2511(2)(a)(ii)(B) specifically provides:

> No provider of wire or electronic communications serve…shall disclose the existence of any interception or surveillance or the devise used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, *except as may otherwise be required by legal process* and then only after prior notification to the AG or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate.

Id. *(emphasis added).* Thus, these statutory provisions specifically allow for the disclosure of information as "required by the legal process."

As discussed earlier, the Maine Commission can investigate the allegations made in this complaint without seeking to discover secret information about the NSA or its activities. Many government officials, including the President of the United States, have acknowledged the existence of the NSA surveillance program that involves collecting consumers' telephone communications information without a warrant or an articulated basis for suspicion. Furthermore, the complainants and the public are aware of the fact that telecommunications companies like Verizon have the capability and in fact a duty to provide certain customer information to the government in certain situations (i.e. pursuant to warrants, court orders and administrative subpoenas). It is public knowledge that companies like Verizon cooperate with the government in these circumstances. The question in this case, is if Verizon disclosed customer information, did it do so lawfully? As has already been discussed, Verizon cannot

assert the state secrets privilege and, to date, the government has not done so as part of this proceeding. In addition, there are legitimate questions about whether the government should be able to invoke the state secrets privilege to shield all information about the NSA program as the government has already acknowledged the program and it has been widely publicized.

Finally, under the standard rules of statutory construction, "where a specific provision conflicts with a general one, the specific governs." *Edmond v. U.S.*, 520 U.S. 651, 657 (1997). Additionally, "a specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it has not been expressly amended." *FDA v. Brown & Williamson Tobacco Corp*., 529 U.S. 120, 143 (2000). "This is particularly so where the scope of the earlier statute is broad but the subsequent statutes more specifically address the topic at hand…" *Id*. (quoting *Unities States v. Estate of Romani*, 523 U.S. 517, 530-31 (1998)). 18 U.S.C. § 1806(f) deals specifically with electronic surveillance. Section 6 of the NSA Act, 50 U.S.C. § 402, the statutory provision cited by Verizon, does not. Instead, it discusses the general protections of information and activities of the NSA.

E. Conclusion

In conclusion, the Public Advocate urges the Commission not to grant Verizon's request to dismiss the complaint. To the extent the government, not Verizon, invokes a valid state secrets privilege over some aspects of this proceeding, there are procedures that can be used, if needed, to protect national security interests. Moreover, the Commission can investigate whether Verizon violated consumer protection and privacy laws without disclosing legitimately classified national security information. The Commission does not need to know the details of

how the information was used. It simply needs to determine what action Verizon took and if that action was legally authorized. The Commission is investigating Verizon's actions, not the government's.

If the Commission were to dismiss the complaint, Maine citizens would be left wondering whether Verizon is protecting their privacy rights as Maine and federal law require. That is not an acceptable result. The Public Advocate urges the Commission not to rely on Verizon's view that national security issues trump *any and all* review by this Commission of Verizon's possible misconduct in this matter. At a minimum, Maine ratepayers are entitled to know whether Verizon has released consumer proprietary information in violation of the FCC's CPNI Rules, Section 7 of Chapter 290 of the Commission's rules and 35-A M.R.S.A. § 7101-A(1) & (2). These questions are entirely within the Commission's jurisdiction.

Verizon states in its Response that the Congress and federal court actions are the more appropriate forums to consider these questions. However, the Senate Judiciary Committee has backed away from holding hearings to investigate this matter. Furthermore, actions in federal courts in other circuits are not binding on this Commission. As a result, the Public Advocate respectfully urges the Commission to open an investigation, as other state commissions have

done, to review the important consumer privacy interests that are squarely within the Committee's jurisdiction.

Respectfully submitted,

William C. Black
Deputy Public Advocate

Paulina McCarter Collins
Contract Attorney