8300 Greensboro Dr.
Suite 1200
McLean, VA 22102

(703) 584-8660
www.fcclaw.com

LNGS | LUKAS, NACE, GUTIERREZ & SACHS, LLP

March 4, 2015

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: AT&T Inc. and DIRECTV
MB Docket No. 14-90

Dear Ms. Dortch:

The Minority Cellular Partners Coalition ("MCPC") filed comments in the above-referenced proceeding that directed the Commission's attention to the fact that AT&T, Inc. ("AT&T") had agreed to pay $126.75 million to settle claims that it had engaged in serious Commission-related misconduct. *See* Response of the MCPC, MB Docket No. 14-90, at 2 (Nov. 5, 2014) ("Response"). MCPC noted that AT&T had entered into a consent decree under which it agreed to pay a record-setting $105 million settlement just three weeks after MCPC filed its initial comments. *See AT&T Mobility LLC*, 29 FCC Rcd 11803 (Enf. Bur. 2014). MCPC argued that AT&T's misconduct called into question its qualifications to acquire DIRECTV's licenses.

MCPC also argued that AT&T's involvement in government surveillance programs warranted Commission action to protect the privacy interests of telecommunications consumers. *See* Response at 3-5. It subsequently scoured public records concerning AT&T's cooperation with such programs to determine whether AT&T complied with federal telecommunications law, particularly the Communications Assistance for Law Enforcement Act ("CALEA"). MCPC discovered that AT&T violated CALEA in its role in the warrantless domestic surveillance programs run by the National Security Agency ("NSA") following the terrorist attacks of September 11, 2001.

MCPC will show that AT&T's recently-reported violations of the Communications Act of 1934 ("Act") and the Commission's rules ("Rules"), as well as its obvious and long-unaddressed violations of CALEA, must be examined by the Commission before it can find that AT&T is qualified to acquire DIRECTV's licenses.

AT&T'S CONTINUING PATTERN OF MISCONDUCT

On January 29, 2015, the Commission issued AT&T a notice of apparent liability for a forfeiture ("NAL") of $640,000 for violating § 301 of the Act and §§ 1.903 and 1.947 of the

Rules by "operating numerous wireless stations throughout the United States without authorization over a multiyear period and failing to provide required license modification notices to the Commission." *AT&T Inc.*, FCC 15-12, at 1 (Jan. 29, 2014). In particular, AT&T "acknowledge[d] that it operated 59 of its common carrier fixed point-to-point microwave stations at variance from the stations' licenses for periods ranging from three and a half years to over four years." *Id.* at 4.

While the recent, unadjudicated NAL cannot be used against AT&T in this proceeding, *see* 47 U.S.C. § 504(c), the Commission can, and should, examine the facts underlying the NAL to determine whether AT&T "is engaging in a pattern of non-compliant behavior." *The Commission's Forfeiture Policy Statement and Amendment of § 1.80 to Incorporate the Forfeiture Guidelines*, 15 FCC Rcd 303, 304 (1999). *See Infinity Radio Operations, Inc.*, 22 FCC Rcd 9824, 9827 (2007) (underlying facts from a non-final NAL can be used in a subsequent Commission proceeding). If the Commission looks at the facts that have now made AT&T liable for a $640,000 forfeiture in light of the recent misconduct that forced AT&T to settle for $126.75 million, it will clearly see a "pattern of flagrant disregard" for the Act and the Rules that precludes a finding that AT&T is qualified to acquire DIRECTV's licenses. *Radio Station WABZ, Inc.*, 90 F.C.C. 2d 818, 827 (1982). The Commission should designate the issue of AT&T's qualifications for an evidentiary hearing.

AT&T'S CALEA VIOLATIONS

Media reports abound that suggest that AT&T has run afoul of CALEA. *See, e.g.*, Charlie Savage, *C.I.A. Is Said to Pay AT&T for Call Data*, N.Y. Times, Nov. 7, 2013 (embedded AT&T employees allowed the FBI to obtain call data without issuing subpoenas), *available at* http://www.nytimes.com-/2013/11/07/us/cia-is-said-to-pay-att-for-call-ata.html?pagewanted=all. But the public record is clear that AT&T violated CALEA in its role in the NSA's warrantless domestic surveillance programs.

BACKGROUND

CALEA is codified in Chapter 9 of Title 47 of the United States Code ("Title 47"). Under § 105 of CALEA, telecommunications carriers have the statutory duty to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission." 47 U.S.C. § 1004. The statute defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.* § 1001(2). Call-identifying information includes "customer proprietary network information" ("CPNI") protected by § 222 of the Act. *See id.* § 222(h)(1).

CALEA requires a telecommunications carrier to deliver "intercepted communications

and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier." 47 U.S.C. § 1002(a)(3). However, in certain "emergency or exigent circumstances," a carrier may provide intercepted communications and call-identifying information to the government "by allowing monitoring at its premises if that is the only means of accomplishing the interception or access." *Id.* § 1002(c). Finally, a carrier must facilitate authorized communications interceptions and access to call-identifying information in a manner that protects **"**the privacy and security of communications and call-identifying information not authorized to be intercepted." *Id.* § 1002(a)(4)(A).

Because the Commission's rulemaking authority is limited to prescribing rules to carry out the provisions Chapter 5 of Title 47, *see id*. §§ 201(b), 303(r), Congress added § 229 to the Act in order to give the Commission the authority to prescribe rules to implement the provisions of CALEA. *See id.* § 229(a). Congress expressly required the Commission to adopt rules implementing the "systems security and integrity" ("SSI") requirement of § 105 of CALEA, *see id.* § 229(b), which is codified in Chapter 9. *See id*. § 1004. Accordingly, a carrier's violation of any of the Rules implementing CALEA is considered a violation of a rule prescribed and enforceable under the Act. *See id*. § 229(d).

To implement § 105 of CALEA, the Commission was required to promulgate rules requiring carriers to establish policies and procedures (1) "to require appropriate authorization to activate interception of communications or access to call-identifying information," and (2) "to prevent any such interception or access without such authorization." *Id.* § 229(b)(1). When it implemented CALEA, the Commission interpreted § 105 and § 229(b) of the Act to require carriers "to supervise the conduct of their personnel to ensure that any interception of communications or access to call-identifying information is lawfully conducted." *Communications Assistance for Law Enforcement Act*, 14 FCC Rcd 4151, 4166 ("*First R&O*"), *recon. on other grounds*, 15 FCC Rcd 20735 (1999).

The Commission construed the term "lawful authorization" in § 105 of CALEA to be encompassed by the term "appropriate authorization" in § 229(b)(1) of the Act. *See First R&O*, 14 FCC Rcd at 4166. It concluded that "'appropriate authorization' refers to the legal authorization that law enforcement must present to a carrier in the form of an order, warrant, or other authorization issued by a judge or magistrate pursuant to federal or state authority ('appropriate legal authorization') and the authorization a carrier's employee must receive from the carrier to assist law enforcement ('appropriate carrier authorization') to engage in the interception of communications or the access to call-identifying information." *Id.* Hence, § 1.20002(a) of the Rules defines the term "appropriate legal authorization" to mean: "(1) [a] court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications; or (2) [o]ther authorization, pursuant to 18 U.S.C. [§] 2518(7), or any other relevant federal or state statute." 47 C.F.R. § 1.20002(a). With respect to the "appropriate legal authorization" requirement, the Commission concluded that "in order to satisfy [§§] 105 and 229, a carrier must, upon receipt of a proffered authorization by law enforcement, determine if

such authorization is what it purports to be, and whether it can be implemented technically, including that the authorization is sufficiently and accurately detailed to enable the carrier to comply with its terms." *First R&O*, 14 FCC Rcd at 4167.

AT&T was required to establish policies and procedures to comply with CALEA. *See id*. at 4193 (47 C.F.R. § 64.2103(a)). *See also* 47 C.F.R. § 1.20003(b). AT&T's policies and procedures – its so-called SSI plan – was to include: (1) a statement that its personnel "must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information;" and (2) "[a]n interpretation of the phrase 'appropriate authorization' that encompasses the definitions of appropriate legal authorization and appropriate carrier authorization." *First R&O*, 14 FCC Rcd at 4193 (47 C.F.R. § 64.2103(c), (d)). *See also* 47 C.F.R. § 1.20003(b)(1), (2). AT&T was required to file its initial SSI plan with the Commission for its approval, and thereafter to file an SSI plan within 90 days of its merger or divestiture or the amendment of its existing SSI Plan. *See First R&O*, 14 FCC Rcd at 4195 (47 C.F.R. § 64.2105(a)). *See also* 47 C.F.R. § 1.20005(a).

AT&T apparently filed its initial SSI plan with the Commission in March 1999, and the plan is on file with the Commission. *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, 19 FCC Rcd 15676, 15687 (2004). MCPC attempted to obtain a copy of AT&T's SSI plan, but was informed by the Public Safety & Homeland Security Bureau staff that the plan was not available for public inspection.

A violation of AT&T's SSI plan by one of its officers or employees is a violation of § 1.2003 of the Rules. *See* 47 U.S.C.§ 229(d). In the event of such a violation, the Commission "shall enforce the penalties articulated" in § 503(b) of the Act and § 1.80 of the Rules. 47 C.F.R. § 1.20008.

At the time of the September 11, 2001, terrorist attacks, the Foreign Intelligence Surveillance Act ("FISA") provided the means by which electronic surveillance of foreign intelligence communications were to be conducted. *See Clapper v. Amnesty International USA*, 133 S. Ct 1138, 1143 (2013). FISA authorized judges of the Foreign Intelligence Surveillance Court ("FISC") "to approve electronic surveillance for foreign intelligence purposes if there was probable cause to believe that 'the target of the electronic surveillance is a foreign power or an agent of a foreign power,' and that each of the specific 'facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.'" *Id*. at 1143 (quoting 50 U.S.C. § 1804(a)(3)).

Section 215 of FISA, as amended in 2001, authorizes the FBI to obtain an order from the FISC requiring any person or entity to turn over "any tangible things … for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1). FISA also prohibited persons from intentionally engaging in electronic surveillance "under color of law except as authorized by statute." *Id*. § 1809(a).

Under § 301 of FISA, a telecommunications carrier is authorized to provide "information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance," 18 U.S.C. § 2511(2)(a)(ii), if the carrier had been provided with a "certification in writing by a person specified in [18 U.S.C. §] 2518(7)" – the Deputy Attorney General or the Associate Attorney General – "or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." *Id.* § 2511(2)(a)(ii)(B).

Under Title III of the Omnibus Crime Control and Safe Streets Act of 1986, as amended ("Title III"), a telecommunications carrier is required to provide "subscriber information and toll billing records information, or electronic communication transactional records" in response to a so-called "national security letter" ("NSL") issued under 18 U.S.C. § 2709(b). *See ACLU v. Clapper*, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013). The Director of the FBI (or his designee) issues NSLs by which he "certifies in writing" that the information or records requested are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b).

Finally, Title III authorizes any investigative or law enforcement officer "specially designated by the Attorney General, the Deputy Attorney General, [or] the Associate General Counsel" to intercept a wire, oral, or electronic communication, if: (1) the officer reasonably determines that an "emergency situation exists" involving "conspiratorial activities threatening the national security interest" that requires the communication be intercepted before a court order can, "with due diligence," be obtained; (2) there are grounds upon which an order authorizing the interception could be entered; and (3) an application for such an order is made within 48 hours of the interception. 18 U.S.C. § 2518(7).

We turn now to AT&T's role as the NSA's "collection partner" in the President's Surveillance Program ("PSP"), which Congress defined as the "intelligence activity involving communications that was authorized … by the President during the period beginning on September 11, 2001, and ending on January 17, 2007." 50 U.S.C. § 1885a(a)(4)(A)(i). *See* Offices of the Inspectors General, *Unclassified Report on the President's Surveillance Program* 1 n.1 (Jul. 10, 2009), *available at* http://www.fas.org/irp/eprint/psp.pdf.

FACTS

On October 4, 2001, President Bush issued a memorandum authorizing the NSA to conduct electronic surveillance on targets related to Afghanistan and international terrorism. *See* Office of the Inspector General, National Security Administration, *Working Draft ST-09-002* 1, 7 (Mar. 24, 2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection. "Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority." *Id.* at 1. Under FISA, the "NSA could not collect from a wire in the United States, without a court order, either content or metadata from communications links with either one of both ends in the United States." *Id.* at 6-7.

President Bush authorized NSA to collect two different types of bulk information: telephony and Internet metadata, and telephone and Internet content. *See Working Draft* at 1, 7-8, 11, 15. The memorandum ("Authorization") specified that:

> NSA could acquire the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority.

Id. at 1, 8. The PSP was reauthorized by the President approximately every 45 days with some modifications. *See Unclassified Report* at 1.

For email, the metadata that NSA collected included the sender and recipient email addresses. *See Working Draft* at 13. The telephony metadata collected included "as to each call, the telephone numbers that placed and received the call, the date, time, and duration of the call, other session-identifying information (for example, International Mobile Subscriber Identity number…), trunk identifier, and any telephone calling card number." *ACLU*, 959 F. Supp. 2d at 733-34. Thus, NSA collected call-identifying information under CALEA and CPNI under § 222 of the Act.

Between the September 11, 2001, attacks and the issuance of the Authorization on October 4, 2001, AT&T contacted the NSA to offer its help. *See Working Draft* at 29. Once the Authorization was signed, NSA began the process visiting carriers and other "commercial entities" requesting their support. *Id.* NSA personnel made it clear to the carriers that "the PSP was a cooperative program and participation was voluntary." *Id*. On October 6, 2001, the NSA began to receive telephony and Internet content from AT&T through communications links owned and operated by AT&T. *See id.* at 33.

On or shortly after October 8, 2001, NSA personnel met with AT&T and obtained its agreement to cooperate in the PSP. *Id*. at 29. After receiving confirmation that a formal NSA letter requesting its assistance was forthcoming, AT&T, acting independently, initiated collection to support the PSP. *See id.* at 30. It provided NSA with telephone and Internet metadata "as early as November 2001." *Id.* at 34. A former AT&T engineer, Mark Klein, revealed that in 2002-2003, AT&T allowed NSA to install "a Narus 6400" in its San Francisco switching center that had the capability "to shift through large amounts of data looking for preprogrammed targets." *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 989 (N.D. Cal. 2006).

AT&T did not receive a certification under 18 U.S.C. § 2511(2)(a)(ii)(B), and the government subsequently claimed that "the issue of whether AT&T received a certification

authorizing its assistance is a state secret." *Hepting*, 439 F. Supp. 2d at 995. Instead of receiving a certification in writing from the Attorney General that no warrant or court order was required by law and that all statutory requirements had been met, AT&T received 44 request-for-assistance letters from the Director of the NSA between October 16, 2001 and December 14, 2006. *See Working Draft* at 31, 32.

The October 16, 2001, letter stated that the NSA and the FBI required AT&T's assistance "to collect intelligence vital to the national security arising from the events of 11 September 2001,' and specifically requested that it "provide survey, tasking and collection against international traffic, some of which terminates in the United States; provide aggregated call record information; and supply computer to computer data which can be used to determine the communicants.'" *Id.* at 31. The NSA Director informed AT&T that its assistance was "needed to identify members of international terrorist cells in the United States and prevent future terrorist attacks against the United States." *Id.* The letter also stated that "the requested assistance was authorized by the President with the legal concurrence of the Attorney General, pursuant to Article II of the Constitution." *Id.*

Subsequent request-for-assistance letters were sent to AT&T by the NSA Director (or his deputy) referencing the October 16, 2001, letter; repeating the need to provide the Presidentially-authorized assistance; emphasizing that such assistance was necessary to counter a future terrorist attack; and stating that such assistance was reviewed by the Attorney General and had been determined to be a lawful exercise of the President's powers as Commander-in-Chief. *See Working Draft* at 31. Starting in mid-2003, the wording of the request-for-assistance letters "was revised but in substance remained the same." *Id*.

In March 2004, a review of the PSP by the Department of Justice's Office of Legal Counsel ("OLC") determined that the collection of bulk Internet metadata appeared to be prohibited by the terms of FISA and Title III. *See id*. at 38. *See also Unclassified Report* at 21-29. Based on the OLC's finding, President Bush rescinded the authority to collect bulk Internet metadata on March 19, 2004, and he gave NSA "one week to stop collection and block collection to previously collected bulk Internet metadata." *Working Draft* at 38. NSA did so on March 26, 2004. *See id.*

The media reported the existence of the PSP in December 2005. *See In re NSA Telecommunications Records Litigation*, 633 F. Supp. 2d 949, 955 (N.D. Cal. 2009), *aff'd*, 671 F.3d 881 (9th Cir. 2011). On January 24, 2006, the Attorney General finally sent a letter to AT&T in which he certified under 18 U.S.C. § 2511(2)(a)(ii)(B) that "no warrant or court order was or is required by law for the assistance, that all statutory requirements have been met, and that the assistance has been and is required." *Working Draft* at 32. Shortly thereafter, dozens of lawsuits were filed against telecommunications carriers by their customers alleging various causes of action related to the carriers' cooperation with the NSA in the PSP. *See NSA Telecommunications Records Litigation*, 633 F. Supp. 2d at 955, 958-59. Collectively, the suits sought "hundreds of billions of dollars in damages." *Id.* at 959. A suit against AT&T was the first of the suits to be filed. *See id*. at 955 (citing *Hepting*).

On July 7, 2008, after months of election-year lobbying by the telecommunications-carrier defendants, Congress enacted the FISA Amendments Act of 2008. *See NSA Telecommunications Records Litigation*, 633 F. Supp. 2d at 956. Section 802 of the new law granted immunity from civil suits to any "communications service provider" that rendered assistance to the intelligence community that was:

> (A) in connection with an intelligence activity involving communications that was- (i) authorized by the President during the period beginning on September 11, 2001 and ending on January 17, 2007; and (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and (B) the subject of a written request or directive, or a series of written requests or directives from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communications service provider indicating that the activity was- (i) authorized by the President; and (ii) determined to be lawful.

50 U.S.C. § 1885a(a)(4).

Congress obviously crafted the retroactive immunity provision of § 802 to effect the dismissal of the pending suits against AT&T and the other communications service providers that partnered with the NSA in the PSP. Section 802 effectively provided that any such suit must be "promptly dismissed" if the Attorney General certified to the court that the defendant rendered assistance to the NSA in the PSP. *See* 50 U.S.C. § 1885a(a). The Attorney General did just that and the suits of the telecommunications customers were dismissed. *See NSA Telecommunications Records Litigation*, 671 F.3d at 893.

DISCUSSION

Research has failed to uncover any reported action by the Commission with regard to AT&T's widely-reported involvement in the NSA's metadata collection programs. MCPC finds that disturbing given that the Act "requires communications providers to protect consumers' sensitive personal information to which they have access as a result of their unique position as network operators," *Implementation of the Telecommunications Act of 1996*, 28 FCC Rcd 9609, 9611 (2013), and provides the Commission with a "clear directive to protect the privacy of consumers utilizing the communications infrastructure." *Id*. at 9622. That directive compels the Commission to take action to ensure that AT&T's blatant violations of CALEA and the CALEA-based Rules, as well as its lesser included violations of the CPNI provisions of § 222 of the Act, never reoccur.

Whether or not the PSP violated the Fourth Amendment, Title III, or FISA is immaterial. What is material are AT&T's violations of CALEA, the Rules, and its SSI plan. And the facts in the public domain conclusively show that AT&T violated § 105 of CALEA, § 1.20003 of the Rules, and the provisions of its SSI plan, when it voluntarily enabled the NSA to implement the PSP in October 2001.

In 1998, AT&T urged the Commission to "recognize that CALEA specifically requires carriers to protect the privacy of communications not authorized to be intercepted because 'Congress intended carriers to do more than blindly implement a surveillance order presented by law enforcement agencies.'" *First R&O*, 14 FCC Rcd at 4165. The Commission agreed, and it required that carrier personnel receive appropriate legal authorization "before taking any action to affirmatively implement the interception of communications or access to call-identifying information." *Id.* at 4166-67. Yet, AT&T agreed to *voluntarily* participate in the PSP, *see Working Draft* at 29, and it began sending telephony and Internet content to NSA before it received any legal authorization. *See id.* at 33.

Under §§ 105 of CALEA and 229 of the Act, AT&T was required to review a proffered legal authorization employing "the level of scrutiny applicable to a carrier's review of a court order or certification" under any federal statute. *First R&O*, 14 FCC Rcd at 4167. That required AT&T to ensure that its senior officers or employees responsible for activating the interception of communications or access to call-identifying information were "fully appraised" of the relevant federal statutory provisions. *See id.* When it finally received NSA's first request-for-assistance letter on October 16, 2001, AT&T either blindly implemented the letter or did not did not carefully review it.

The NSA's request-for-assistance letter of October 16, 2001 clearly did not qualify as an appropriate legal authorization under Title III, FISA, CALEA, the Act, or the Rules. It was not a court order, a warrant, or a subpoena. And the letter did not purport to be a written certification by the NSA Director.

AT&T could not, and apparently did not, consider the NSA's letter to be an NSL. It was obviously not issued by the FBI Director, a designated Deputy Director at FBI headquarters, or a Special Agent in Charge in an FBI field office. *But see* 18 U.S.C. § 2709(b). Nor did it constitute a written *certification* that "the name, address, length of service," or the "local or long distance billing records," of a person or entity was relevant to an authorized international-terrorism investigation. *Id.*

Finally, AT&T could not have reviewed the request-for-assistance letter from the Director of the NSA and concluded that it was a valid certification under 18 U.S.C. § 2511(2)(a)(ii). It was not a "written certification" by either the Attorney General, the Deputy Attorney General, or the Associate Attorney General that no warrant or court order was required to collect the requested intelligence, and that all statutory requirements for the collection had been met. 18 U.S.C. § 2511(2)(a)(ii)(B). The NSA's letter did not even make the claims that (1) no warrant or order was required, or (2) all statutory requirements had been met. *See Working Draft* at 31. For the same reasons, none of the 43 subsequent request-for-assistance letters could be reviewed by AT&T and considered to be a valid § 2511(2)(a)(ii)(B) certification. *See id.*

Considering the state of the law in October 2001, AT&T could not have thought either that the NSA's letter was adequate legal authorization or that the PSP was lawful. In *United States v. United States District Court*, 407 U.S. 297 (1972) ("*Keith*"), the Court held that the

Fourth Amendment does not permit warrantless wiretaps to track domestic threats to national security, *see id*. at 321, reaffirmed the "necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest," *id*. at 308, and did not pass judgment "on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* FISA was enacted in 1978 in response to the Supreme Court's decision in *Keith. See United States v. Warsame*, 547 F. Supp. 2d 982, 985 (D. Minn. 2008).

FISA struck a balance between the President's need to "conduct legitimate electronic surveillance for foreign intelligence purposes" and "this Nation's commitment to privacy and individual rights." *ACLU v. Barr*, 952 F.2d 457, 461 (D.C. Cir. 1991). The centerpiece of the legislation was the rule that "electronic surveillance of a foreign power or its agents may not be conducted unless the [FISC] authorizes it in advance." *Id.* The government had to obtain an FISC order granting its application for electronic surveillance of an agent of a foreign power. *See* 50 U.S.C. §§ 1805(a), 1824(a).

Considering the *Keith* decision and the FISA requirements, AT&T must have known– and the Commission required it to know– that a FISC order was required before the NSA could be given access to "all or substantially all of the communications transmitted through [its] key domestic telecommunications facilities." *Hepting*, 439 F. Supp. 2d at 1010. Because AT&T's alleged actions had been held to be unlawful in *Keith*, "AT&T cannot seriously contend that a reasonable entity in its position could have believed that the … domestic dragnet was legal." *Id.*

It appears that Qwest Communications International ("Qwest") refused to participate in the PSP. It has been reported Qwest's former chief executive, Joseph P. Nacchio, was the chairman of the President's National Security Telecommunications Advisory Committee in the Fall of 2001, when he was approached to give the government access to the private phone records of Qwest's customers. *See* Ellen Nakashima and Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, Washington Post, Oct. 13, 2007, *available at* http://www.washington-post.com/wp-yn/content/article/2007/10/12/AR2007101202485.html. When he inquired and was told that no warrant or other legal process had been obtained (and that the government was disinclined to obtain authorization from the FISC), Mr. Nacchio concluded that the government's request "violated the privacy requirements of the Telecommunications Act." *Id.*

According to the NSA, three private sector companies did not participate in the PSP. NSA had discussions with "COMPANY E" that began in early 2002 and continued in 2003, but its general counsel ultimately decided not to support the NSA. *See Working Draft* at 30. At a meeting on October 29, 2002, the NSA "requested COMPANY F's support under the PSP for email content." *Id.* However, "COMPANY F requested a letter from the Attorney General certifying the legality of the PSP." *Id.* It did not participate in the PSP because of "corporate liability concerns." *Id.* Finally, when the general counsel of "COMPANY G" stated that he wanted to seek the "opinion of outside counsel" in April 2003, "NSA determined the risk associated with additional disclosure outweighed what COMPANY G would have provided" and it "decided not to pursue a partnership with this company." *Working Draft* at 30.

AT&T apparently had no misgivings with regard to partnering with the NSA in the performance of the PSP. Having not requested nor received appropriate legal authorization, AT&T began giving NSA telephone and Internet content on October 6, 2001. The first appropriate legal authorization that was presented to AT&T was the FISC's "Pen Register/Trap & Trace" order that was issued on July 15, 2004. *See id.* at 34. Thus, AT&T delivered intercepted telephony and Internet communications, and gave access to call-indentifying information concerning substantially all of the communications that were carried on its network, to the NSA for a period of at least 33 months without receiving appropriate legal authorization. By so doing, AT&T knowingly committed egregious and continuing violations of § 105 of CALEA, § 1.20003 of the Rules, and the provisions of its SSI plan. *See* 47 U.S.C. § 1004; 47 C.F.R. § 1.20003(b)(1); *First R&O*, 14 FCC Rcd at 4166.

Finally, it appears the AT&T did not adhere to any of the limits that CALEA imposed on its cooperation with the NSA. AT&T not only delivered intercepted communications and call-identifying information to the NSA without a FISC order, it did so at its own premises (*e.g.*, its San Francisco switching center) in violation of CALEA. *See* 47 U.S.C. § 1002(a)(3). There were no conceivable "emergency of exigent circumstances" that would have justified AT&T "allowing monitoring at its premises if that is the only means of accomplishing the interception or access." *Id.* § 1002(c).

CONCLUSION

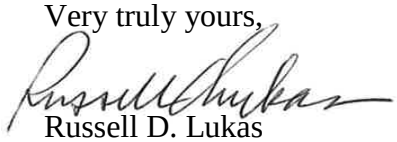
No cause of action could have been brought in any court against AT&T for participating in the PSP if it had provided "information, facilities, or assistance" to the NSA "in accordance with the terms of a court order, statutory authorization, or certification under [18 U.S.C. § 2511(2)(a)(ii)(B)]." 18 U.S.C. § 2511(2)(a)(ii). *See* 50 U.S.C. §§ 1805(h), 1842(f), 1861(e), 1881a(h)(3), 1881b(e). The fact that Congress found it necessary to grant immunity to AT&T in 2008 attests to the fact that AT&T participated in an unlawful surveillance program without appropriate legal authorization. To one court, the grant of immunity "appear[ed] to be *sui generis* among immunity laws: it create[d] a retroactive immunity for past, completed acts committed by private parties acting in concert with governmental entities that allegedly violated constitutional rights." *NSA Telecommunications Records Litigation*, 633 F. Supp. 2d at 959.

AT&T has been granted immunity for civil damages claims arising from its participation in the PSP, and it is no longer liable for a forfeiture for its violations of § 1.20003 of the Rules and its SSI plan. *See* 47 U.S.C. § 503(b)(6)(B). But the Commission is still obliged to execute and enforce the provisions of § 229 of the Act, *see* 47 U.S.C. § 151, and it is still empowered to conduct an investigation to insure that AT&T complies with the requirements of CALEA. *See id.* § 229(c). And the Commission is obliged to determine whether AT&T is qualified to obtain DIRECTV's licenses in light of its egregious violations of CALEA. This is particularly true given AT&T's continued and ongoing pattern of misconduct. Accordingly, the Commission should investigate AT&T's complicity in the PSP to determine whether AT&T engaged in unlawful conduct that abridged the privacy interests of telecommunications consumers on a vast scale and, if so, whether AT&T is qualified to obtain DIRECTV's licenses.

At the very least, the Commission should exercise its authority in this proceeding to ensure that AT&T will abide by CALEA in the future. Since AT&T must submit a SSI plan within 90 days of a merger with DIRECTV, *see* 47 C.F.R. § 1.20005(a), MCPC respectfully requests that the Commission only grant its consent to the AT&T/DIRECTV merger on the condition that AT&T submit a detailed SSI plan to the Commission within 90 days that is subject to a public notice-and-comment proceeding. AT&T should be permitted to redact the information called for by § 1.20003(4) of the Rules from the SSI plan it makes available for public inspection and comment. *See id.* § 1.20003(4).

This letter is being filed electronically pursuant to § 1.1206 of the Rules. Should any questions arise with regard to this matter, please direct them to me.

Very truly yours,



Russell D. Lukas

cc: Jamillia Ferris
Vanessa Lemmé
Brendan Holland
Christopher Sova
Daniel Ball
Jim Bird
Maureen R. Jeffreys
William M. Wiltshire
Best Copy and Printing, Inc.