http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

# UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA

(San Francisco Division)

IN RE NATIONAL SECURITY TELECOMMUNICATIONS RECORDS LITIGATION

THIS DOCUMENT RELATES
TO: ALL CASES BROUGHT AGAINST
DEFENDANTS SPRINT NEXTEL
CORPORATION., SPRINT
COMMUNICATIONS CO. LTD.
PARTNERSHIP, NEXTEL
COMMUNICATIONS INC., EMBARQ
CORPORATION, UCOM, INC., U.S.
TELCOM, INC., UTELCOM, INC., AND
DOES 1-100.

MDL Docket No. 06-1791 (VRW)

MASTER CONSOLIDATED COMPLAINT
AGAINST DEFENDANTS SPRINT NEXTEL
CORPORATION, SPRINT
COMMUNICATIONS CO. LTD.
PARTNERSHIP, NEXTEL
COMMUNICATIONS, INC., EMBARQ
CORPORATION, UCOM, INC., U.S.
TELCOM, INC., UTELCOM, INC., AND
DOES 1-100 FOR DAMAGES,
DECLARATORY AND
EQUITABLE RELIEF

JUDGE: Hon. Vaughn R. Walker

## **DEMAND FOR JURY TRIAL**

Plaintiffs, by their attorneys, for their Master Consolidated Complaint against Sprint Communications Co. Ltd. Partnership, Nextel Partners, Inc., and Embarq Corporation, allege, upon information and belief, as follows:

#### PRELIMINARY STATEMENT

1. This Master Consolidated Complaint against Sprint Nextel Corporation, Sprint Communications Co. Ltd. Partnership, Nextel Communications, Inc., Embarq Corporation, UCOM, Inc., U.S. Telcom, Inc., Utelcom, Inc., and Does 1-100 ("Sprint Master Complaint" or "Complaint") is filed pursuant to the Order of this Court and presents all claims brought against Defendants Sprint Nextel Corporation, Sprint

Communications Co. Ltd. Partnership, Nextel Communications, Inc., Embarq Corporation, UCOM, Inc., U.S. Telcom, Inc., Utelcom, Inc. and Does 1-100 (collectively "Defendants" or "Sprint") in the separate cases transferred by the Panel on Multidistrict Litigation in this matter in its orders dated August 14, 2006, and September 25, 2006 ("transferred cases"). Unless otherwise ordered by this Court, all claims presented in any case against Sprint Nextel Corporation, Sprint Communications Co. Ltd. Partnership, Nextel Communications, Inc., Embarq Corporation, UCOM, Inc., U.S. Telcom, Inc., Utelcom, Inc., and Does 1-100 subsequently transferred to this Court by the Panel on Multidistrict Litigation in this matter shall be deemed to be included in this Sprint Master Complaint.

- 2. This Sprint Master Complaint is filed solely as an administrative device to promote judicial efficiency and economy in the adjudication and resolution of pretrial matters and is not intended to effect consolidation for trial of the transferred cases. Neither is this Sprint Master Complaint intended to cause, nor to change the rights of the parties, nor to make those who are parties in one transferred case parties in another.
- 3. This case challenges the legality of Defendants' participation in a secret and illegal government program to intercept and analyze vast quantities of Americans' telephone communications and records, surveillance done without any statutorily authorized permission, customers' knowledge or consent, or the authorization of a court, and in violation of federal electronic surveillance and telecommunications statutes, as well as the First and Fourth Amendments to the United States Constitution. In addition, Plaintiffs challenge Defendants' conduct under state law.

### **JURISDICTION AND VENUE**

- 4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1332(d), 18 U.S.C. § 2707, and 47 U.S.C. § 605. Supplemental jurisdiction over state law claims is founded on 28 U.S.C. § 1367.
- 5. Venue is proper in this District pursuant to the order of the Panel on Multidistrict Litigation.

## **PARTIES**

- 6. Plaintiff Richard D. Suchanek, III is an individual residing in Bowling Green, Kentucky. Plaintiff is a subscriber and user of Sprint/Nextel cellular telephone service.
- 7. Defendant Sprint Nextel Corporation is a Kansas corporation with its principal place of business in Virginia. Sprint Nextel Corporation is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 8. Defendant Sprint Communications Co. Ltd. Partnership is a Delaware partnership with its principal place of business in Kansas. Sprint Communications Co. Ltd. Partnership is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 9. Defendant Nextel Communications, Inc. is a Delaware corporation with its principal place of business in Virginia. Nextel Communications, Inc. is a "telecommunication carrier" within the meaning of the Communications Act of 1934,

- 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 10. Defendant Embarq Corporation is a Delaware corporation with its principal place of business in Kansas. Embarq Corporation is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, et seq. and provides remote computing and electronic communications services to the public.
- 11. Defendant UCOM, Inc. is a Missouri corporation with its principal place of business in Kansas. UCOM, Inc. is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 12. Defendant U.S. Telcom, Inc. is a Kansas corporation with its principal place of business in Kansas. U.S. Telcom, Inc. is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 13. Defendant Utelcom, Inc. is a Kansas corporation with its principal place of business in Kansas. Utelcom, Inc. is a "telecommunication carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote computing and electronic communications services to the public.
- 14. Plaintiff is currently unaware of the true names and capacities of all potentially liable parties sued herein and therefore sue these Defendants by using fictitious names as Does 1-100. Upon information and belief each fictitiously named Defendant is responsible in some manner for the occurrences herein alleged and the

injuries to Plaintiffs and class members herein alleged were proximately caused in relation to the conduct of Does 1-100 as well as the named Defendants. Plaintiffs will amend this complaint to allege the true identities and capacities of such fictitiously named Defendants when ascertained.

### **FACTUAL ALLEGATIONS**

- 15. In Section 222 of the Communications Act of 1934 (47 U.S.C. § 222(c)(1)), Congress imposed upon telecommunication carriers, such as Defendants, a duty to protect sensitive, personal customer information from disclosure. This information includes "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 data concerning service customers' telephone calling histories (*i.e.*, date, time, duration, and telephone numbers of calls placed or received) or call-detail records, and such information constitutes "individually identifiable customer proprietary network information" within the meaning of Section 222 of the Communications Act of 1934.
- 16. Federal law prohibits telecommunications providers such as Defendants from disclosing customers' call-detail records to the government without a court order, subpoena, or other lawful authorization.
- 17. In the aftermath of September 11, 2001, Defendants commenced their programs of providing the federal government with the telephone call contents and records of its customers and subscribers. Defendants continue to provide this information to the federal government.

- 18. On December 16, 2005, in an article entitled "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times* reported on an NSA program of eavesdropping on the telephone conversations of Americans without court order as required by the Foreign Intelligence Surveillance Act.
- 19. In a December 17, 2005 radio address, President Bush admitted that "[i]n the weeks following the terrorist attacks on our nation, [he] authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations." President Bush further stated that "the activities [he] authorized are reviewed approximately every 45 days"; that he had "reauthorized this program more than 30 times since the September the 11<sup>th</sup> attacks"; and that he intended to continue authorizing such activity "for as long as our nation faces a continuing threat from al Qaeda and related groups."
- 20. In a press briefing on December 19, 2005 by Attorney General Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the government claimed that the NSA Surveillance Program targets communications between a party outside the United States and a party inside the United States when one of the parties of the communication is believed to be "a member of al Qaeda, <u>affiliated</u> with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."
- 21. In a press release on December 19, 2005, Attorney General Alberto Gonzales stated that the Program involved "intercepts of contents of communications . . . ." While the Attorney General's description of the Program was

limited to interception of communications with individuals "outside the United States," Attorney General Gonzales explained that his discussion was limited to those parameters of the program already disclosed by the President and that many other operational aspects of the program remained highly classified.

22. On December 24, 2005, *The New York Times* reported in an article entitled, "Spy Agency Mined Vast Data Trove, Officials Report," that:

[t]he National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials. The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said. It was collected by tapping directly into some of the American telecommunication system's main arteries, they said.

The officials said that as part of the program, "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications" and that the program is a "large data-mining operation" in which N.S.A. technicians have combed through large volumes of phone and Internet traffic in search of patterns that might point to terrorism suspects. In addition, the article reports, "[s]everal officials said that after President Bush's order authorizing the N.S.A. program, senior government officials arranged with officials of some of the nation's largest telecommunications companies to gain access to switches that act as gateways at the borders between the United States' communication networks and international networks."

23. In a January 3, 2006 article entitled, "Tinker, Tailor, Miner, Spy" (available at http://www.slae.com/toolbar.aspx?action=print&id=2133564), Slate.com

reported, "[t]he agency [the NSA] used to search the transmissions it monitors for key words, such as names and phone numbers, which are supplied by other intelligence agencies that want to track certain individuals. But now the NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target. Reportedly, the agency is analyzing the length of a call, the time it was placed, and the origin and destination of electronic transmissions."

- 24. In a January 17, 2006 article, "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *The New York Times* stated that officials who were brief on the N.S.A. program said that "the agency collected much of the data passed on to the F.B.I. as tips by tracing phone numbers in the United States called by suspects overseas, and then by following the domestic numbers to other numbers called. In other cases, lists of phone numbers appeared to result from the agency's computerized scanning of communications coming into and going out of the country for names and keywords that might be of interest."
- 25. A January 20, 2006 article in the *National Journal*, "NSA spy program hinges on state-of-the-art technology," reported that "[o]fficials with some of the nation's leading telecommunications companies have said they gave the NSA access to their switches, the hubs through which enormous volumes of phone and e-mail traffic pass every day, to aid the agency's effort to determine exactly whom suspected al-Qaeda figures were calling in the United States and abroad and who else was calling those numbers. The NSA used the intercepts to construct webs of potentially interrelated persons."

- 26. In a January 21, 2006 article in the *Bloomberg News* entitled "Lawmaker Queries Microsoft, Other Companies on NSA Wiretaps," Daniel Berninger, a senior analyst at Tier 1 Research in Plymouth, Minnesota, said "[i]n the past, the NSA has gotten permission from phone companies to gain access to so-called switches, high-powered computer into which phone traffic flows and is redirected, at 600 locations across the nation. . . . From these corporate relationships, the NSA can get the content of calls and records on their date, time, length, origin and destination."
- 27. On January 25, 2006, an article appearing in the *Reporter-Times* entitled "NSA Data Mining is Legal, Necessary, Chertoff Says" stated that "while refusing to discuss how the highly classified program works (Department of Homeland Security Secretary) Chertoff made it pretty clear that it involves "data-mining" collecting vast amounts of international communications data, running it through computers to spot key words and honing in on potential terrorists." In that same interview Secretary Chertoff is quoted as saying "... if you're trying to sift through an enormous amount of data very quickly, I think it (obtaining a FISA warrant) would be impractical", and that getting an ordinary FISA warrant is "a voluminous, time-consuming process" and "if you're culling through literally thousands of phone numbers ... you could wind up with a huge problem managing the amount of paper you'd have to generate."
- 28. On February 5, 2006, an article appearing in the *Washington Post* entitled "Surveillance Net Yields Few Suspects" stated that officials said "[s]urveillance takes place in several stages . . . the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human

eyes and hears. Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order of likeliest interest to human analysts." The article continues "[f]or years, including in public testimony by Hayden, the agency [the NSA] has acknowledged use of automated equipment to analyze the contents and guide analysts to the most important ones. According to one knowledgeable source, the warrantless program also uses those methods. That is significant . . . because this kind of filtering intrudes into content, and machines 'listen' to more Americans than humans do."

- 29. On February 6, 2006, in an article entitled "Telecoms let NSA spy on calls," the nationwide newspaper *USA Today* reported that "[t]he National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives." The article acknowledged that *The New York Times* had previously reported that the telecommunications companies had been cooperating with the government but had not revealed the names of the companies involved. In addition, it stated that long-distance carriers AT&T, MCI, and Sprint "all own 'gateway' switches capable of routing calls to points around the globe, and that "[t]elecommunications executives say MCI, AT&T, and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials."
- 30. On May 11, 2006, in an article entitled "NSA has massive database of Americans' phone calls," *USA Today* reported that "[t]he National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using

data provided by AT&T, Verizon and Bellsouth," according to multiple sources with "direct knowledge of the arrangement." One of the confidential sources for the article reported that the NSA's goal is "to create a database of every call ever made" within the United States. The confidential sources reported that AT&T and the other carriers are working "under contract" with the NSA, which launched the program in 2001 shortly after the September 11, 2001 terrorist attacks. At the U.S. Senate confirmation hearing on his nomination to become Director of the Central Intelligence Agency, General Michael Hayden, who was the Director of the NSA at the time, confirmed that the program was "launched" on October 6, 2001.

- 31. The *USA Today* story was confirmed by a U.S. intelligence official familiar with the program. The story reports that the NSA requested that AT&T, SBC, and the other carriers "turn over their 'call-detail records,' a complete listing of the calling histories of their millions of customers," and provide the NSA with "updates" of the call-detail records. The confidential sources for the story reported that the NSA informed the carriers that it was willing to pay for the cooperation, and that both "AT&T, which at the time was headed by C. Michael Armstrong," and "SBC, headed by Ed Whitacre," agreed to provide the NSA with the requested information.
- 32. The *USA Today* story reported that the NSA requested that Qwest Communications, Inc. ("Qwest"), another telecommunications carrier, provide the NSA with its customers' call-detail records, but Qwest refused. Qwest requested that the NSA first obtain a court order, a letter of authorization from the U.S. Attorney General's office, or permission from a Court operating under the Foreign Intelligence Surveillance

Act ("FISA"), but the NSA refused, because it was concerned that the FISA Court and the Attorney General would find the NSA's request unlawful.

- 33. As of the date of the filing of this Complaint, no part of the *USA Today* story has been publicly denied by any representative of the federal government, including the NSA.
- 34. On May 16, 2006, in an article entitled "BellSouth Denies NSA Contract," eWeek.com reported that BellSouth's vice president of corporate communications, Jeff Battcher, in an interview disputed the accuracy of information contained in the May 11, 2006 *USA Today* article but "note[d] that his company owns 40 percent of wireless carrier Cingular" and that he "[didn't] want to speak for Cingular".
- 35. Qwest's decision not to participate was also reported in an article from *The New York Times* on May 13, 2006 entitled, "Questions Raised for Phone Giants in Spy Data Furor." The article reported that Qwest's former CEO, Joseph Nacchio, "made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process,' Nacchio concluded that the requests violated federal privacy requirements 'and issued instructions to refuse to comply." According to the May 11, 2006 *USA Today* article, "Nacchio's successor, Richard Notebaert, finally pulled the plug on the NSA talks in late 2004."
- 36. Senator Christopher "Kit" Bond (R-MO), who also has received access to information on warrantless surveillance operations, explained on May 11, 2006 on a PBS Online NewsHour program entitled "NSA Wire Tapping Program Revealed" that "[t]he

president's program uses information collected from phone companies . . . what telephone number called what other telephone number."

- 37. On May 14, 2006, when Senate Majority Leader William Frist (R-TN) was asked on CNN Late Edition with Wolf Blitzer whether he was comfortable with the program described in the *USA Today* article, he stated "Absolutely. I am one of the people who are briefed . . . I've known about the program. I am absolutely convinced that you, your family, our families are safer because of this particular program."
- 38. Senator Pat Roberts (R-KS), the chair of Senate Intelligence Committee, described the program on "All Things Considered" on NPR on May 17, 2006. When asked about whether he had been briefed that the NSA had collected millions of phone records for domestic calls, Roberts stated: "Well, basically, if you want to get into that, we're talking about business records."
- 39. On May 29, 2006, Seymour Hersh reported in *The New Yorker* in an article entitled "Listening In" that a security consultant working with a major telecommunications carrier "told me that his client set up a top-secret high-speed circuit between its main computer complex and Quantico, Virginia, the site of a government-intelligence computer center. This link provided direct access to the carrier's network core the critical area of its system, where all its data are stored. 'What the companies are doing is worse than turning over records,' the consultant said. 'They're providing total access to all the data.'"
- 40. A June 30, 2006 *USA Today* story reported that 19 Members of the intelligence oversight committees of the U.S. Senate and House of Representatives "who had been briefed on the program verified that the NSA has built a database that includes

records of Americans' domestic phone calls," and that four of the committee Members confirmed that "MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government."

- 41. Defendants knowingly and intentionally provide the aforementioned telephone contents and records to the federal government.
- 42. As part of the Program, NSA's operational personnel identify particular individual targets and their communications, through a software data mining process that NSA runs against vast databases of the Defendants' stored electronic records of their customers' telephone communications, in search of particular names, numbers, words or phrases, and patterns of interest. Upon information and belief, NSA's operational personnel also identify communications of interest in real time through similar datamining software functionality.
- 43. Besides actually eavesdropping on specific conversations, NSA personnel have intercepted large volumes of domestic and international telephone and Internet traffic in search of patterns of interest, in what has been described in press reports as a large "data mining" program.
- 44. As part of this data-mining program, the NSA intercepts millions of communications made or received by people inside the United States and uses powerful computers to scan their contents for particular names, numbers, words, or phrases.
- 45. Additionally, the NSA collects and analyzes a vast amount of communications traffic data to identify persons whose communications patterns the government believes may link them, even if indirectly, to investigatory targets.

- 46. The NSA has accomplished its massive surveillance operation by arranging with some of the nation's largest telecommunications companies to gain direct access to the telephone and Internet communications transmitted via those companies' domestic telecommunications facilities, and to those companies' records pertaining to the communications they transmit.
- 47. Defendants have intercepted and continue to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international, and foreign telephone and Internet communications.
- 48. Since in or about October 2001, Defendants have disclosed and/or divulged the "call-detail records" of all or substantially all of their customers including Plaintiffs to the NSA, in violation of federal law, as more particularly set forth below.
- 49. Defendants have, since in or about October 2001, been disclosing to the NSA "individually identifiable customer proprietary network information" belonging to all or substantially all of their customers including Plaintiffs, in violation of federal law, as more particularly set forth below.
- 50. Defendants have disclosed and continue to disclose and/or provide the government with direct access to its databases of stored telephone records, which are updated with new information in real time or near-real time.
- 51. Defendants have provided at all relevant times and continue to provide computer or storage processing services to the public by means of wire, radio, electromagnetic, photo-optical, or photo-electronic facilities for the transmission of wire

or electronic communications, and/or by means of computer facilities or related electronic equipment for the electronic storage of such communications.

- 52. Defendants have knowingly authorized, and continue to knowingly authorize, NSA and affiliated governmental agencies to install and use, or have assisted government agents in installing or using, interception devices and pen registers and/or trap and trace devices on the Defendants' domestic telecommunications facilities in connection with the Program.
- 53. The interception devices and pen registers and/or trap and trace devices capture, record or decode the various information pertaining to individual class member communications including dialing, routing, addressing and/or signaling information ("DRAS information") for all or a substantial number of all wire or electronic communications transferred through the Defendants' domestic telecommunications facilities where those devices have been installed.
- 54. Using these devices, government agents have acquired and are acquiring wire or electronic communications content and DRAS information directly via remote or local control of the device, and/or the Defendants have disclosed and are disclosing those communications and information to the government after interception, capture, recording, or decoding.
- 55. Defendants have knowingly authorized, and continue to knowingly authorize, NSA and affiliated governmental agencies to directly access through the installed devices all wireless telephone communications transmitted through the Defendants' domestic telecommunications infrastructure and facilities for use in the Program.

- 56. Defendants intercept, divulge, and/or disclose to the federal government the aforementioned telephone communications contents and records without probable cause. Furthermore, Defendants have not received and/or are not acting within the scope of, in accord with, or in good faith reliance on, any statutory authorization, legislative authorization, subpoena, court order or warrant, nor any certification, request, or other lawful authorization under Chapter 119, 121, or 206 of Title 18 or Chapter 36 of Title 50, purporting to authorize the aforementioned conduct.
- 57. To the best of Plaintiffs' counsel's knowledge, information, and belief, formed after reasonable inquiry under the circumstances and likely to have evidentiary support after a reasonable opportunity for further investigation and discovery, Defendants' interception, divulgence and/or disclosure to the of the aforementioned telephone communications content and records is willful, in bad faith, and done in collusion with the government, for purposes of direct or indirect commercial advantage or private financial gain, and a failure to cooperate might have jeopardized their ability to obtain lucrative government contracts.
- 58. Defendants did not disclose to its customers, including Plaintiffs, that it was providing the aforementioned telephone contents and records to the federal government. Thus, Defendants' customers, including Plaintiffs, had no opportunity to, and did not, consent to the disclosure of their telephone contents and records.
- 59. The telephone contents and records intercepted and/or disclosed and/or divulged by the Defendants to the federal government pursuant to the program challenged herein were not divulged (a) pursuant to a law enforcement investigation concerning telemarketing fraud; (b) as a necessary incident to the rendition of services to customers;

(c) to protect the rights or property of the Defendants; (d) based on a reasonable and/or good faith belief that an emergency involving danger of death or serious physical injury required disclosure without delay; (e) to the National Center for Missing and Exploited Children; or (f) to a non-governmental person or entity.

### CLASS ACTION ALLEGATIONS

60. Plaintiff brings this action under Federal Rule of Civil Procedure 23 on behalf of themselves and a Class, defined as:

All individuals and entities located in the United States that have been subscribers or customers of Defendant's wireless, wire and/or electronic communication services at any time since October 6, 2001. Excluded from the Class are Defendant, Defendant's predecessors, affiliates, parents, subsidiaries, officers and directors; all federal, state, and local governmental entities; any and all judges and justices assigned to hear any aspect of this litigation, their court staffs, their spouses, any minor children residing in their households, and any persons within the third degree of relationship to any judge or justice assigned to hear any aspect of this litigation.

- 61. Plaintiffs seek certification of the Class under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).
- 62. The Class numbers in the millions, so that joinder of all Members is impractical.
- 63. The claims of Plaintiffs are typical of the claims of the Class. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no conflicts with any other Class members and have retained competent counsel experienced in class actions, consumer, telecommunications, and civil rights litigation.
  - 64. Common questions of law and fact exist, including:
    - a. Whether Defendants intercepted its customers' wire and electronic communications:

- b. Whether Defendants disclosed and/or divulged its customers' telephone records and content to the federal government;
- c. Whether the Defendants violated federal law in disclosing and/or divulging its customers' telephone records and content to the federal government;
- d. Whether Plaintiffs and Class Members are entitled to damages; and
- e. Whether Plaintiffs and Class Members are entitled to equitable relief.
- 65. These and other questions of law and fact are common to the Class predominate over any questions affecting only individual Members.
- 66. A class action is a superior method for the fair and efficient adjudication of the controversy described herein. A class action provides an efficient and manageable method to enforce the rights of Plaintiff and member of the Class.
- 67. The prosecution of separate actions by individual Members of the Class would create a risk on inconsistent or varying adjudication, establishing incompatible standards of conduct for Defendant.
- 68. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate relief with respect to the Class as a whole.

#### NECESSITY OF INJUNCTIVE RELIEF

- 69. The named Plaintiffs and the Members of the Class will continue in the future to use their telephones.
- 70. Unless this Court enjoins the Defendants' program challenged herein, the Defendants will continue to engage in the program.

71. The named Plaintiffs and the Members of the Class will suffer irreparable harm as a result of the continuation of the Defendants' program, and they have no adequate remedy at law.

#### **CLAIMS FOR RELIEF**

# FIRST CLAIM FOR RELIEF Violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2)

- 72. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this Complaint, as if set forth fully herein.
  - 73. In relevant part, 18 U.S.C. § 2702 provides that:
    - a. Prohibitions. Except as provided in subsection (b) or (c)
      - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
      - (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service
        - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
        - (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. . . .

- 74. Defendants knowingly divulged b one or more persons or entities the contents of Plaintiffs' and Class Members' communications while in electronic storage by a Defendant electronic communication service, and/or while carried or maintained by a Defendant remote computing service, in violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2).
- 75. On information and belief, Defendants knowingly divulged to one or more persons or entities the contents of Plaintiffs' and Class Members' communications while in electronic storage by a Defendant electronic communication service, and/or while carried or maintained by a Defendant remote computing service, in violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2).
- 76. Defendants did not notify Plaintiffs or Class Members of the divulgence of their communications, nor did Plaintiffs or Class Members consent to such.
- 77. Neither the NSA nor any other governmental entity has obtained a warrant authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(A).
- 78. Neither the NSA nor any other governmental entity has obtained a court order authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(B) and (d).
- 79. Neither the NSA nor any other governmental entity has issued or obtained an administrative subpoena authorized by a federal or state statute authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).
- 80. Neither the NSA nor any other governmental entity has issued or obtained a federal or state grand jury or trial subpoena authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

- 81. Defendants have not been provided with a certification in writing by a person specified in 18 U.S.C. § 2518(7) or by the Attorney General of the United States meeting the requirements of 18 U.S.C. §2511(2)(a)(ii)(B), *i.e.*, a certification that no warrant or court order authorizing the disclosures is required by law, and that all statutory requirements have been met.
- 82. The disclosures were not and are not authorized by any statute or legislation.
- 83. Defendants' disclosures in violation of 18 U.S.C. § 2702(a)(3) were and are knowing, intentional, and willful.
- 84. There is a strong likelihood that Defendants are now engaging in and will continue to engage in the above-described divulgence of Plaintiffs' and Class Members' communications while in electronic storage by Defendants' electronic communication service(s), and/or while carried or maintained by Defendants' remote computing service(s), and that likelihood represents a credible threat of immediate future harm.
- 85. Plaintiffs and Class Members have been and are aggrieved by Defendants' above-described divulgence of the contents of their communications.
- 86. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2702, Plaintiffs and Class Members seek such preliminary and other equitable or declaratory relief as may be appropriate; statutory damages of no less than \$1,000 for each aggrieved Plaintiff or Class Member; punitive damages as the Court considers just; and reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF Violation of 18 U.S.C. § 2702(a)(3)

- 87. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this Complaint, as if set forth fully herein.
  - 88. In relevant part, 18 U.S.C. § 2702 provides that:
    - a. Prohibitions. Except as provided in subsection . . . (c)
      - (3) a provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.
- 89. Defendants' telephone services are "electronic communication service[s]," as that term is defined in 18 U.S.C. § 2510(15), provided to the public, including Plaintiffs and Class Members.
- 90. Defendants violated 18 U.S.C. § 2702(a)(3) by knowingly and intentionally divulging to the federal government records or other information pertaining to subscribers or customers of the Defendants' remote computing and electronic services.
- 91. Defendants' challenged program of disclosing telephone records to the federal government does not fall within any of the statutory exceptions or immunities set forth in 18 U.S.C. §§ 2702(c), 2703(c), or 2703(e).
- 92. Neither the NSA nor any other governmental entity has obtained a warrant authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(A).
- 93. Neither the NSA nor any other governmental entity has obtained a court order authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(B) and (d).

- 94. Neither the NSA nor any other governmental entity has issued or obtained an administrative subpoena authorized by a federal or state statute authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).
- 95. Neither the NSA nor any other governmental entity has issued or obtained a federal or state grand jury or trial subpoena authorizing such disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).
- 96. Defendant has not been provided with a certification in writing by a person specified in 18 U.S.C. § 2518(7) or by the Attorney General of the United States meeting the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B), *i.e.*, a certification that no warrant or court order authorizing the disclosures is required by law and that all statutory requirements have been met.
- 97. The disclosures were not and are not authorized by any statute or legislation.
- 98. Whether or how the NSA, or any other governmental entity, actually used the records after they were divulged is irrelevant to whether Defendants violated 18 U.S.C. § 2702(a)(3).
- 99. Plaintiffs and their Class are aggrieved by the Defendants' knowing and intentional past disclosure and/or imminent future disclosure of their records to the federal government. Accordingly, plaintiffs may challenge this violation of 18 U.S.C. § 2702(a)(3) pursuant to the cause of action created by 18 U.S.C. § 2707(a).

## THIRD CLAIM FOR RELIEF Violation of 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a)

- 100. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this Complaint, as if set forth fully herein.
  - 101. In relevant part, 18 U.S.C. § 2511 provides that:
    - (1) Except as otherwise specifically provided in this chapter, any person who - (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication. . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; (d) intentionally uses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection. . . . (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other addressee or intended recipient communication or an agent of such addressee or intended recipient.
- 102. Defendants violated 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a) by intentionally intercepting and disclosing to the federal government the contents of telephone calls of the Defendants' customers.
- 103. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' wire or electronic

communications, while knowing or having reason to know that the information was obtained through the interception of wire or electronic communications.

- 104. Defendants' challenged program of intercepting and disclosing the contents of telephone calls to the federal government does not fall within any of the statutory exceptions or immunities set forth in 18 U.S.C. §§ 2511(2), 2511(3)(b), or 2520(d). Defendants acted on bad faith and/or acted without a facially valid court order or certification.
- 105. Plaintiffs and their Class are aggrieved by the Defendants' intentional past and/or imminent future interception and disclosure of telephone call contents to the federal government. Accordingly, Plaintiffs may challenge this violation of 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a) pursuant to the cause of action created by 18 U.S.C. § 2520(a).

# FOURTH CLAIM FOR RELIEF Violation of 47 U.S.C. § 605

- 106. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this Complaint, as if set forth fully herein.
  - 107. In relevant part, 47 U.S.C. § 605 provides that:
    - (a) Practices prohibited Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence . . . thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.

- 108. Defendants received, assisted in receiving, transmitted, or assisted in transmitting, Plaintiff's and Class Members' interstate communications by wire or radio.
- 109. Defendants violated 47 U.S.C. § 605 by divulging or publishing the "existence" of Plaintiffs' and Class Members' communications to the federal government by means other than through authorized channels of transmission or reception. Defendants' disclosure and publication of the existence of Plaintiffs' and Class Members' communications was not authorized by any provision of 18 U.S.C. §§ 2510-2522.
- 110. Defendants' disclosure and publication of the existence of Plaintiffs' and Class Members' communications was willful and for purposes of direct or indirect commercial advantage or private financial gain as they were paid for their cooperation, and a failure to cooperate might have jeopardized their ability to obtain lucrative government contracts.
- 111. Defendants failed to notify Plaintiff or Class Members of Defendants' disclosure and/or publication of the existence of Plaintiffs' and Class Members' communications nor did Plaintiffs or Class Members consent to such disclosure and publication.
  - 112. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs and Class Members seek:
    - a. a declaration that the disclosures are in violation of 47 U.S.C. § 605(a);
    - b. a preliminary injunction restraining Defendant from continuing to make such unlawful disclosures;
    - c. a permanent injunction restraining Defendant from continuing to make such unlawful disclosures;
    - d. statutory damages of not less than \$1,000 or more than \$10,000 for each violation, plus, in the Court's discretion, an increase in the statutory damages of up to \$100,000 for each violation; and

e. reasonable attorneys' fees and reasonable costs of this litigation.

# FIFTH CLAIM FOR RELIEF Violation of 50 U.S.C. § 1809

- 113. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.
  - 114. In relevant part, 50 U.S.C. §1809 provides that:
    - (a) Prohibited activities A person is guilty of an offense if he intentionally (1) engages in electronic surveillance under color of law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.
  - 115. In relevant part 50 U.S.C. §180l provides that:
    - (f) "Electronic surveillance" means (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio

communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

- 116. Defendants have intentionally acquired by means of a surveillance device, the contents of one or more wire communications to or from Plaintiffs and Class Members, or other information in which Plaintiffs or Class Members have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.
- 117. By the acts alleged herein, Defendants have intentionally engaged in electronic surveillance (as defined by 50 U.S. C. §1801(f)) under color of law but which is not authorized by any statute, and the Defendants have intentionally subjected Plaintiffs and Class Members to such electronic surveillance, in violation of 50 U.S.C. § 1809.
- 118. Additionally, or in the alternative, by the acts alleged herein Defendants have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.
- 119. Defendants did not notify Plaintiffs or Class Members of the above-described electronic surveillance, disclosure, and/or use, nor did Plaintiffs or Class Members consent to such.
- 120. Defendants' challenged program of electronic surveillance does not fall within any of the statutory exceptions or immunities set forth in 50 U.S.C. § 1809(b).
- 121. There is a strong likelihood that Defendants are now engaging in and will continue to engage in the above-described electronic surveillance, disclosure, and/or use

of Plaintiffs' and Class Members' wire communications described herein, and that likelihood represents a credible threat of immediate future harm.

- 122. Plaintiffs and Class Members have been and are aggrieved by the Defendants' electronic surveillance, disclosure, and/or use of their wire communications.
- 123. Pursuant to 50 U.S.C. § 1810, which provides a civil action for any person who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of 50 U.S.C. §1809, Plaintiffs and Class Members seek equitable and declaratory relief; statutory damages for each Plaintiff and Class Member of whichever is the greater of \$100 a day for each day of violation or \$1,000; punitive damages as appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

# SIXTH CLAIM FOR RELIEF Violation of the First and Fourth Amendments to the United States Constitution

- 124. Plaintiffs incorporate all of the allegations contained in the preceding paragraphs of this Complaint, as if set forth fully herein.
- 125. Plaintiffs and Class Members have a reasonable expectation of privacy in their communications, contents of communications, and/or records pertaining to their communications transmitted, collected, and/or stored by Defendants, which was violated by Defendants' above-described actions as agents of the government, which constitute a search and seizure of Plaintiffs' and Class Members' communications and records.
- 126. Plaintiffs and Class Members use the Defendants' services to speak or receive speech anonymously and to associate privately.

- 127. The above-described acts of interception, disclosure, divulgence and/or use of Plaintiffs' and Class Members' communications, contents of communications, and records pertaining to their communications occurred without judicial or other lawful authorization, probable cause, and/or individualized suspicion.
- 128. At all relevant times, the federal government instigated, directed, and/or tacitly approved all of the above-described acts of the Defendants.
- 129. At all relevant times, the federal government knew of and/or acquiesced in all of the above-described acts of the Defendants and failed to protect the First and Fourth Amendment rights of the Plaintiffs and Class Members by obtaining judicial authorization.
- 130. In performing the acts alleged herein, the Defendants had, at all relevant times, a primary or significant intent to assist or purpose of assisting the government in carrying out the Defendants' program and/or other government investigations, rather than to protect its own property or rights.
- 131. By the acts alleged herein, Defendants acted as instruments or agents of the government, and thereby violated Plaintiffs' and Class Members' reasonable expectations of privacy and denied Plaintiffs and Class Members their right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution of the United States, and additionally violated Plaintiffs' and Class Members' rights to speak and receive speech anonymously and associate privately under the First Amendment.
- 132. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs and Class Members.

133. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' and Class Members' constitutional rights.

## SEVENTH CLAIM FOR RELIEF On Behalf of the Class Members for Violations of Kentucky State Privacy Statute

- 134. Plaintiffs incorporate by reference the paragraphs above and further state that Defendants violate various state privacy statutes as set out below by one or more of the following acts without justification: intercepting wire or oral communications; eavesdropping on communications; disclosing communications; recording conversations; wiretapping; using or installing a pen register; and/or using or installing a trap and trace device.
- 135. The acts and practices of Defendants directly, foreseeably, and proximately cause damages and injury to Plaintiffs and the Class.
- 136. The actions of Defendants are in violation of the following statutes Ky. Rev. Stat. Ann. §§ 526.010-.020 (2005).

# EIGTH CLAIM FOR RELIEF On Behalf of the Class Members for Violations of Kentucky Consumer Protection Statute

- 137. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.
- 138. Plaintiffs further state that Defendants violate state consumer protection statutes by divulging records or other information pertaining to subscribers and customers to a governmental entity, specifically, the NSA, without Class Members' knowledge or consent.

- 139. The unfair and deceptive trade acts and practices of Defendants directly, foreseeably, and proximately cause damages and injury to Plaintiffs and the Class.
- 140. The actions and failures to act of Defendants, including the false and misleading representations and omissions of material facts regarding the protection and use of Class Members' private information, constitute an unfair method and unfair and/or deceptive acts in violation of Ky. Rev. Stat. § 367.1 10 et seq.
- 141. This injury is of the type Ky. Rev. Stat. § 367.1 10 *et seq* was designed to prevent and directly results from Defendants' unlawful conduct.

# NINTH CLAIM FOR RELIEF On Behalf of the Class Members for Breach of Contract

- 142. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.
- 143. At all times relevant herein, Defendants agreed to provide for a subscription fee, and Plaintiffs and Class Members agreed to purchase from the Defendants various telecommunication and electronic communication services and/or devices.
- 144. At all times relevant herein, Defendants impliedly and expressly promised to protect the privacy and confidentiality of its customers' information, identity, records, subscription, use details, and communications, and, to abide by federal and state law.
- 145. Defendants by their conduct as alleged, breached their contract with the Plaintiffs and Class Members. (Defendants have also by their conduct as alleged breached the implied covenant of good faith.)

146. As a result of Defendants' breach of contractual duties owed to the Plaintiffs and Class Members, Defendants are liable for damages including, but not limited to nominal and consequential damages.

# TENTH CLAIM FOR RELIEF On Behalf of the Class Members for Breach of Warranty

- 147. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.
- 148. At all times relevant herein, Defendants agreed to provide for a subscription fee, and Plaintiffs and Class Members agreed to purchase from the Defendants various telecommunication and electronic communication services and/or devices.
- 149. At all times relevant herein, Defendants impliedly and expressly warranted or otherwise represented to Plaintiffs and Class Members that Defendants would safeguard, protect, and maintain the privacy and confidentiality of its customers' information, identity, records, subscription, use details, and communications, and to abide by all applicable law.
- 150. Plaintiffs and Class Members relied upon these express and implied warranties and representations in entering into their subscriptions with Defendants.
- 151. At all times relevant, Defendants by their conduct as alleged, breached these warranties and representations.
- 152. As a direct and proximate result of Defendants' breaches of warranty as detailed herein, Plaintiffs and Class Members have suffered damages including, but not limited to, nominal and consequential damages.

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and for all others similarly situated, respectfully requests that the Court:

- A. Declare that Defendants' conduct as alleged herein violates applicable law;
- B. Award statutory damages to Plaintiffs and the Class;
- C. Award punitive damages to Plaintiffs and the Class;
- D. Award Plaintiffs' reasonable attorneys' fees and costs of suit;
- E. Award restitution, damages, and all other relief allowed under State law claims;
- F. Enjoin Defendants' continuing violations of applicable law; and
- G. Grant such other and further relief as the Court deems just and proper.

Dated: January 16, 2007.

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason Nicholas A. Migliaccio THE MASON LAW FIRM, P.C. 1225 19<sup>th</sup> Street, NW Suite 500 Washington, D.C. 20038 Telephone: (202) 429-2290

Telephone: (202) 429-2290 Facsimile: (202) 429-2294

John C. Whitfield WHITFIELD & COX, PSC 29 East Center St. Madisonville, KY 42431 Telephone: (270) 821-0656

Facsimile: (270) 825-1163

Document hosted at JDSUPRA

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

# ATTORNEYS FOR PLAINTIFFS

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

## **CERTIFICATE OF SERVICE**

I hereby certify that on January 16, 2007, I electronically filed the foregoing **Master Consolidated Complaint Against Sprint** with the Clerk of the court using the CM/ECF system which will send notification of such filing to the email addresses noted on the attached Electronic Mail Notice List, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants with addresses indicated on the attached manual list.

/s/ Gary E. Mason Gary E. Mason

## M:06-cv-1791 Notice will be electronically mailed to:

Timothy L. Alger timalger@quinnemanuel.com, albertvillamil@quinnemanuel.com

Sam Jonathan Alton salton@stoneleyton.com, usdc@stoneleyton.com

David L. Anderson .

Marc H. Axelbaum marc.axelbaum@pillsburylaw.com

Kevin Stuart Bankston bankston@eff.org

Alexander E Barnett abarnett@masonlawdc.com, mdicocco@masonlawdc.com

Timothy M. Bechtold tim@rossbachlaw.com

Bradford Allan Berenson bberenson@sidley.com, vshort@sidley.com

E. Garth Black GBlack@cwclaw.com, cwadia@cwclaw.com; clee@cwclaw.com

John David Blair-Loy dblairloy@aclusandiego.org

Brian Matthew Boynton brian.boynton@wilmerhale.com

Ann Brick abrick@aclunc.org, lcerri@aclunc.org

James J. Brosnahan jbrosnahan@mofo.com, bkeaton@mofo.com

D. Douglas Brothers dbrothers@georgeandbrothers.com, receptionist@georgeandbrothers.com

Thomas R. Burke thomasburke@dwt.com, natashamajorko@dwt.com

Adam S. Caldwell adamcaldwell@dwt.com, tracyjohnson@dwt.com

David William Carpenter dcarpenter@sidley.com, efilingnotice@sidley.com My ron Milton Cherry mcherry@cherry-law.com, jzolna@cherry-law.com

Cindy Ann Cohn cindy@eff.org, rebecca@eff.org

Anthony Joseph Coppolino tony.coppolino@usdoj.gov,

Elena Maria DiMuzio Elena.DiMuzio@hellerehrman.com

Elizabeth A. Drogula ldrogula@crblaw.com

Joseph Richard Dulle jdulle@stoneleyton.com, usdc@stoneleyton.com

Jon B. Eisenberg jon@eandhlaw.com

Peter Jay Eliasberg peliasberg@aclu-sc.org, ereyes@aclu-sc.org

Derek John Emge derek@inthelaw.com

Bruce A. Ericson bruce.ericson@pillsburylaw.com

Val Patrick Exnicios vpexnicios@exnicioslaw.com, bsergi@exnicioslaw.com

Eric B. Fastiff efastiff@lchb.com

James M. Finberg @altshulerberzon.com, smendez@altshulerberzon.com

Mark D. Flanagan mark.flanagan@wilmerhale.com

Amy Collins Fontenot afontenot@exnicioslaw.com

Robert D. Fram rfram@hewm.com, mawilliams@hewm.com; kim.sydorak@hellerehrman.com; audrey.michalski@hellerehrman.com

Jeff D Friedman JFried! man@lerachlaw.com

R. James George , Jr rjgeorge@georgeandbrothers.com, fjordan@georgeandbrothers.com

Jennifer Stisa Granick JENNIFER@LAW.STANFORD.EDU,

Terry Gross terry@grossbelsky.com, mara@grossbelsky.com

Harvey Michael Grossman hgrossman@aclu-il.org, rhughes@aclu-il.org

Alexander Kenneth Haas Alexander. Haas@usdoj.gov,

Robert Carl Hilliard bobh@hilliardandmunoz.com, dee@hilliardandmunoz.com

Barry R. Himmelstein bhimmelstein@lchb.com

Eric A. Isaacson erici@lerachlaw.com

Samir Chandra Jain samir.jain@wilmerhale.com, alicia.hunt@wilmerhale.com

Reed R. Kathrein reedk@lerachlaw.com, e\_file\_sf@lerachlaw.com; e file sd@lerachlaw.com

Michael P. Kenny mike.kenny@alston.com

Case M:06-cv-01791-VRW

John G. Kester jkester@wc.com, ggreenman@wc.com; idelawala@wc.com

Craig Allen Knot cknot@sidley.com, efilingnotice@sidley.com

Clinton Arthur Krislov clint@krislovlaw.com, ro@krislovlaw.com

Michael M. Markman mmarkman@hewm.com

Brian Martinez brianmartinez@mofo.com

Gary E. Mason gmason@masonlawdc.com

Edward Robert McNicholas emcnicholas@sidley.com, vshort@sidley.com

Corynne McSherry corynne@eff.org

Gerald E Meunier gmeunier@gainsben.com, jwoods@gainsben.com

Candace J. Morey cmorey@fenwick.com,

Maria V. Morris mariam@lerachlaw.com, e\_file\_sf@lerachlaw.com

Roger R. Myers roger.myers@hro.com, adam.brezine@hro.com; nancy.burnett@hro.com

Karl Olson ko@lrolaw.com, amw@lrolaw.com

Kurt Opsahl kurt@eff.org

Renee S. Orleans renee.orleans@usdoj.gov,

Nicole A. Ozer nozer@aclunc.org, mpham@aclunc.org

Clare Pastore cpastore@aclu-sc.org, jbradberg@aclu-sc.org

Jacob B. Perkinson jperkinson@jpclasslaw.com,

Laurence F. Pulgram lpulgram@fenwick.com, mburt@fenwick.com

Daniel John Richert daniel.richert@pillsburylaw.com, susan.hersom@pillsburylaw.com

Elizabeth I. Rogers elizabeth.rogers@wilmerhale.com,

rebecca.mcnew@wilmerhale.com

John Andrew Rogovin john.rogovin@wilmerhale.com

Shana Eve Scarlett shanas@lerachlaw.com, e\_file\_sd@lerachlaw.com; e\_file\_sf@lerachlaw.com

Steven Edward Schwarz stevenschwarz23@yahoo.com

Eric Alan Shumsky eshumsky@sidley.com

W. Russell Sipes wrs@lgrslaw.com, sg@lgrslaw.com

Christopher Slater cslater@slaterross.com, mjross@slaterross.com

Michael W. Sobol msobol@lchb.com

Jacob R. Sorensen jake.sorensen@pillsburylaw.com

Christopher Leo Soriano csoriano@wolfblock.com

Michael Alan St. Pierre mikesp@rrsplaw.com

Lauren A Stern las@skchung.com

Andrew H Tannenbaum an! drew.tannenbaum@usdoj.gov

Tze Lee Tien tien@eff.org, jason@eff.org; vkhall@aol.com; eff-mdl@eff.org

Theresa M. Traber, Esq tmt@tvlegal.com,

James Samuel Tyre jstyre@jstyre.com, jstyre@eff.org

Marc Van Der Hout ndca@vblaw.com

William Joel Vander Vliet joel@krislovlaw.com, ecf@krislovlaw.com

Bert Voorhees by@tvlegal.com

James P. Walsh budwalsh@dwt.com, pamelabaron@dwt.com; allanpatterson@dwt.com

Joshua Graeme Whitaker joshuawhitaker@griffinwhitaker.com, griffinwhitaker@griffinwhitaker.com

Richard Roy Wiebe wiebe@pacbell.net,

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Martin Darren Woodward mwoodward@smi-law.com

Shira R Yoshor shira.yoshor@bakerbotts.com

Matthew J. Zevin mzevin@smi-law.com

## M:06-cv-1791 Notice will be delivered by other means to:

Bruce Ira Afran Bruce Afran, Attorney at Law 10 Braeburn Drive Princeton, NJ 08540

Jessica Ashlee Albies Law Office of J. Ashlee Albies 621 SW Alder Street Suite 621 Portland, OR 97205

Ron Antosko

,

Stephen E. Arthur Harrison & Moberly 135 North Pennylvania Street Suite 2100 Indianapolis, IN 46204

Sidney M. Bach Sidney M. Back, Attorney at Law 5917 Constance Street New Orleans, LA 70115

Darrell Lee Barger Hartline acus et all 800 N. Shoreline Blvd. Suite 2000N Corpus Christi, TX 78401

Todd C. Barnes George & Sipes 156 East Market Street Suite 600 Indianapolis, IN 46204

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Raymond A . Basile Harrison & Moberly 135 North Pennsylvania Suite 2100 Indianapolis, IN 46204

Daniel J. Becka Beigel Schy Lasky Rifkind Goldberg & Fertik Ltd 311 So Wacker Dr 65th Flr Chicago, IL 60606

Marc Oliver Beem Miller Shakman & Hamilton, LLP 180 North LaSalle Street Suite 3600 Chicago, IL 60601

John Beisner O'Melveny & Myers LLP 555 13th Street, N.W. Suite 500 West Washington, DC 20004-1109

Matthew Phineas Bergman Law Office of Matthew Bergman 705 2nd Avenue Suite 1601 Seattle, WA 98104

Steven K. Blackhurst Ater Wynne Hewitt Dodson & Skerritt 222 S.W. Columbia Ste 1800 Portland, OR 97201-6618

Ari Y. Brown Bergman & Frockt 705 Second Avenue Suite 1601 Seattle, WA 98104

James M. Carlson Ungaretti & Harris LLP 3500 Three First National Plaza Chicago, IL 60602

David R. Carpenter

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Sidley Austin LLP One South Dearborn Street Chicago, IL 60603

Edward Morgan Carstarphen , III Ellis Carstearphen et all 5847 San Felipe Suite 1900 Houston, TX 77057

Catherine J. Casey DLA Piper rudnick Gray Cary US LLP 203 North LaSalle Street #1900 Chicago, IL 60601

James E. Chadden, Sr Kalea Seitz Clark Wilmer Cutler Pickering Hale and Door LLC 1875 Pennsylvania Avenue NW Washington, DC 20006

Amato A. DeLuca DeLuca & Weizenbaum, Ltd. 19! 9 North Main Street Providence, RI 02903

Nancy Scott Degan Baker Donelson Bearman Caldwell & Berkowitz, PC 201 St. Charle Avenue Suite 3600 New Orleans, LA 70170

Michael D. Donovan Law Offices of Michael D. Donovan 1608 Walnut Street Suite 1400 Philadelphia, PA 19103

Emilie K. Edling Stoel Rives, LLP 900 SW Fifth Avenue Suite 2600 Portland, OR 97204

Tyrone C. Fahner

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Mayer, Brown, Rowe & Maw LLP 71 South Wacker Drive Chicago, IL 60606

Daniel Martin Feeney Miller Shakman & Beem LLP 180 North LaSalle Street Suite 3600 Chicago, IL 60601

Sheila Marie Finnegan Mayer, Brown, Rowe & Maw LLP 71 South Wacker Drive Chicago, IL 60606

Jodi W. Flowers Motley Rice, LLC 28 Bridgeside Boulevard P.O. Box 1792 Mount Pleasant, SC 29465

F. Larkin Fore Fore, Miller & Schwartz 200 S. Fifth Street Suite 700N, First Trust Centre Louisville, KY 40202-3204

Sarah M. Fore Fore, Miller & Schwartz 200 S. Fifth Street Suite 700N, First Trust Centre Louisville, KY 40202-3204

Zachary J. Freeman Miller Shakman & Beem LLP 180 N. La Salle Street Suite 3600 Chicago, IL 60601

Susan A. Freiwald USF School of LAW 2130 Fulton St San Francisco, CA 94117

Albert L. Frevola , Jr. Gordon Hargrove & James

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

2400 East Commercial Blvd. Suite 1100 Fort Lauderdale, FL 33308-3092

Michael R. Fruehwald Barnes & Thornburg 11 South Meridian Street Indianapolis, IN 46204-3535

Jason L. Fulk Hoover Hull LLP 111 Monument Circle Suite 4400 P.O. Box 44989 Indianapolis, IN 46244-0989

Andrea Marie Gacki US Department of Justice 20 Massachusetts Avenue, NW Room 7334 Washington, DC 20001

Daniel N. Gall c/o Luna Innocations 2851 Commerce Street Blacksburg, VA 24060

Linda S. George Laudig George Rutherford & Sipes 156 East Market Street Suite 600 Indianapolis, IN 46204

John Richard Gillespie Broad & Cassel 100 SE 3rd Avenue Suite 2700 One Financial Plaza Fort Lauderdale, FL 33394

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Cary Neal Goldberg Law Offices of Cary N. Goldberg 30 North LaSalle Street Suite 2300 Chicago, IL 60602

Case M:06-cv-01791-VRW

Steven Goldberg American Bank Building 621 S.W. Morrison Suite 1450 Portland, OR 97205

M. Norman Goldberger Wolf Block Schorr and Solis-Cohen, LLP 1650 Arch Street 22nd Floor Philadelphia, PA 19103

Edward Nelson Griffin Griffin Whitaker LLP 8730 Georgia Avenue Suite LL100 Silver Spring, MD 20910

Mark E. Guzzi 271 Providence Oaks Circle Alpharetta, GA 30004

Zaha S. Hassan Attorney at Law 14614 NW Seward Rd Vancouver, WA 98685

F. Thomas Hecht Ungaretti & Harris LLP 3500 Three First National Plaza Chicago, IL 60602

William J. Heller McCarter & English, LLP Four Gateway Center 100! Mulberry Street P.O. Box 652 Newark, NJ 07102-0652

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Amanda J. Hettinger Thompson Coburn LLP One US Bank Plaza St. Louis, MO 63101

Charles F. Hinkle Stoel Rives, LLP 900 SW Fifth Avenue Suite 2600 Portland, OR 97204

Andrew W. Hull Hoover Hull LLP 111 Monument Circle Suite 4400 P.O. Box 44989 Indianapolis, IN 46244-0989

Anthony D. Irpino Irpino Law Firm 365 Canal Street 22nd Floor New Orleans, LA 70130

Lisa Robin Jaskol Horvitz & Levy LLP 15760 Ventura Blvd 18FL Encino, CA 91436

Joseph G. Jevic , III St. Martin & Williams 4084 Highway 311 P.O. Box 2017 Houma, LA 70361-2017

Philip J. John, Jr. Baker & Botts One Shell Plaza 910 Louisiana Street Houston, TX 77002

C. J. Johnson Kalkstein Law Firm P.O. Box 8568 Missoula, MT 59807 http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Kelly Overstreet Johnson 215 S. Monroe Street Suite 400 P.O. Box 11300 Tallahassee, FL 32302

Joshua Karsh Gessler Hughes Piers Resnick & Dym Ltd. Three First National Plaza 70 West Madison Street, Suite 4000 Chicago, IL 60602

Peter D. Keisler United States Department of Justice Assistant Attorney General 20 Massachusetts Avenue, NW Room 7312 Washington, DC 20530

Andrew Kierstead 1001 S.W. Fifth Avenue Suite 1100 Portland, OR 97204

Jonathan D. King DLA Piper Rudnick Gray Cary US LLP 203 North LaSalle Street, #1900 Chicago, IL 60601-1293

Michael E. Kipling Kipling Law Group PLLC 3601 Fremont Avenue N. Suite 414 Seattle, WA 98103

Joseph R. Knight Baker Botts LLP 98 San Jacinto Blvd. Suite 1500 Austin, TX 78701-4039

Leondra Kruger Wilmer Cutler Pickering Hale & Dorr LLP 1875 Pennsylvania NW Avenue Washington, DC 20006-3642

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Melanie G. Lagarde St. Martin & Williams 4084 Highway 311 Houma, LA 70360

Stephen Laudig 2440 Campus Road, #429 Honolulu, HI 96822

David L. Lawson Sidley Austin Brown & Wood 172 Eye Street, N.W. Washington, DC 20006

Roger L. Mandel Stanley Mandel & Iola LLP 3100 Mo! nticello ave Suite 750 Dallas, TX 75205

Lori McAllister Dykema Gossett PLLC 201 Townsend Street Suite 900 Lansing, MI 48933

Howard A. Merten Partridge, Snow & Hahn LLP 180 South Main Street Providence, RI 02903

Donald A. Migliori Motley Rice LLC 321 South Main Street Providence, RI 02940

Benjamin C. Mizer 1875 Pennsylvania Ave., N.W. Washington, DC 20006

Alice McKenzie Morical Hoover Hull LLP 111 Monument Circle Suite 4400 P.O. Box 44989 Indianapolis, IN 46244-0989 http://www.jdsupra.com/post/document Viewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Randolph D. Moss Wilmer, Cutler, Pickering, Hale & Dorr LLP 1875 Pennsylvania Avenue, N.W. Washington, DC 20006

Thomas H. Nelson Thomas H. Nelson & Associates 825 NE Multnomah Suite 925 Portland, OR 97232

Michael C. O'Malley Siben & Siben, LLP 90 East Main Street BayShore, NY 11706

Michele L. Odorizzi Mayer Brown Rowe & Maw 190 South LaSalle Street Chicago, IL 60603

Wendy Sangbee Park Roger Baldwin Foundation of ACLU, Inc. 180 North Michigan Avenue Suite 2300 Chicago, IL 60601

Robert J. Patterson Watts Law Firm LLP 555 N. Carancahua Street Twr II Bldg 14th Floor Corpus Christi, TX 78401

Paul Lee Peyronnin Baker donelson Bearman Caldwell & Berkowitz, PC 201 St. Charles Ave. Suite 3600 New Orleans, LA 70170

Michael James Philippi Ungaretti & Harris LLP 3500 Three First National Plaza Chicago, IL 60602 http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Jason S. Ritchie Holland & Hart P.O. Box 639 Billings, MT 59103

Harry Rosenberg Phelps Dunbar, LLP Canal Place 365 Canal Street Suite 2000 New Orleans, LA 70130-6534

Michael J. Ross Slater Ross 1850 Benjamin Franklin Plaza 1 S.W. Columbia Street Portland, OR 97258

William A. Rossbach Rossbach & Whiston 401 North Washington Street P.O. Box 8988 Missoula, MT 59807-8988

Alan Norris Salpeter Mayer, Brown, Rowe & Maw 190 South LaSalle Street Chicago, IL 60603

Ronald P. Schiller DLA Piper Rudnick Gray Cary US LLP One Liberty Place Suite 4900 1650 Market Street Philadelphia, PA 19103

Mark Schlosberg American Civil Liberties Union Fndt. 1663 Mission Street, Suite 460 San Francisco, CA 94103

Eric Schneider 1730 South Federal Hwy. #104 Delray Beach, FL 33483

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Adam D. Schwartz Roger BaldwinFoundation of ACLU, Inc. 180 North Michigan Avenue Suite 2300 Chicago, IL 60601-7401

John D. Seiver Cole Raywid & Braverman, LLP 1919 Pennsylvania Ave., N.W. Suite 200 Washington, DC 20006

Donald A. Statland Attorney at Law 55 West Monroe St Ste 1200 Chicago, IL 60603

David H. Sternlieb Shapiro & Sternlieb, LLC 800 Tennent Road Manalapan, NJ 07726

A. David Stippler Bingham McHale, LLP 270! 0 Market Tower 10 West Market Street Indianapolis, IN 4! 6204

Ted W. Stroud Oade Stroud & Kleiman PC 200 Woodland Pass P.O. Box 1296 East Lansing, MI 48826-1296

Brendan V. Sullivan Williams & Connolly 725 12th St N.W. Washington, DC 20005

Davis Wright Tremaine Attorney at Law 101 California Street Ste 3275 San Francisco, CA 94111

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

M. Stephen Turner Broad & Cassel 215 South Monroe Street Suite 400 P.O. Box 11300 Tallahassee, FL 32302

Marc Ver Der Hout Ver Der Hout & Brigagliano 180 Sutter Street, 5th Floor San Francisco, CA 94123

Nicholas Wagner Law Offices of Wagner & Jones 1111 East Herndon, Suite 317 Fresno, CA 93720

Thomas P. Walsh United States Attorney's Office NDIL 219 South Dearborn Street Suite 500 Chicago, IL 60604

Peter Wasylyk Law Offices of Peter Wasylyk 1307 Chalkstone Avenue Providence, RI 02908

Mikal C. Watts Watts Law Firm, LLP Bank of America Plaza 300 Convent Street Suite 100 San Antonio, TX 78205

Brian W. Welch Bingham McHale, LLP 10 West Market Street Market Tower, Suite 2700 Indianapolis, IN 46204

John C. Whitfield Whitfield & Cox PSC 29 East Center Street Madisonville, KY 42431

http://www.jdsupra.com/post/documentViewer.aspx?fid=bda65afe-d4e0-4a68-8c00-8a6fe51bbfd6

Conrad S.P. Williams , III St. Martin, Williams & Bourque P.O. Box 2017 Houma, LA 70361

Daniel D. Williams Williams & Connolly LLP 725 Twelfth Street, NW Washington, DC 20005!

Matthew A. Woolf Baker Donelson Bearman Caldwell & Berkowitz, PC 201 St. Charles Ave. Suite 3600 New Orleans, LA 70170

Anthony J. Zarillo , Jr Courter, Kobert & Cohen, PC 1001 Route 517 Hackettstown, NJ 07840

Jacie C. Zolna Myron M. Cherry & Associates 30 North LaSalle Street Suite 2300 Chicago, IL 60602