

1 Ronald L. Motley, Esq. (SC Bar No. RM-2730)
 Jodi Westbrook Flowers, Esq. (SC Bar No. 66300)
 2 Donald Migliori, Esq. (RI Dar No. 4963;
 MA Bar No. 567562; and MN Bar No. 0245951)
 3 Vincent I. Parrett (CA Bar No. 237563)
MOTLEY RICE LLC
 4 28 Bridgeside Boulevard
 P.O. Box 1792
 5 Mount Pleasant, South Carolina 29465
 Telephone: (843) 216-9000
 6 Facsimile: (843) 216-9027
MDL1791@motleyrice.com
 7

INTERIM CLASS COUNSEL

8

9 **UNITED STATES DISTRICT COURT**

10 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

11 **SAN FRANCISCO DIVISION**

12

13 IN RE NATIONAL SECURITY AGENCY)
 TELECOMMUNICATIONS RECORDS)
 14 LITIGATION, MDL No. 1791)
)
 15 This Document Relates To:)
)
 16 ALL CASES BROUGHT AGAINST)
 17 DEFENDANTS TRANSWORLD NETWORK)
 CORP., COMCAST)
 18 TELECOMMUNICATIONS, INC., T-MOBILE)
 USA, INC., AND MCLEODUSA)
 19 TELECOMMUNICATIONS SERVICES, INC.)

MDL Docket No 06-1791 VRW

CLASS ACTION

**MASTER CONSOLIDATED
 COMPLAINT AGAINST DEFENDANTS
 TRANSWORLD NETWORK CORP.,
 COMCAST TELECOMMUNICATIONS,
 INC., T-MOBILE USA, INC., AND
 MCLEODUSA
 TELECOMMUNICATIONS SERVICES,
 INC., FOR DAMAGES, DECLARATORY
 AND EQUITABLE RELIEF**

)
) Courtroom: 6, 17th Floor
) Judge: The Hon. Vaughn R. Walker
)
)
)

20

21

22

23 **DEMAND FOR JURY TRIAL**

24

25

26

27

28

1
2 Plaintiffs, by their attorneys, for their Master Consolidated Complaint against Defendants
3 Transworld Network Corp., Comcast Telecommunications, Inc., T-Mobile USA, Inc., and
4 McLeodUSA Telecommunications Services, Inc., allege, upon information and belief, as follows:

5
6 **PRELIMINARY STATEMENT**

7 1. This Master Consolidated Complaint Against Defendants Transworld
8 Network Corp (“Transworld”), Comcast Telecommunications, Inc. (“Comcast”), T-Mobile USA,
9 Inc. (“T-Mobile”), and McLeodUSA Telecommunications Services, Inc. (“McLeod”), hereafter
10 referred to as the Master Complaint, is filed pursuant to the Order of this Court and presents all
11 federal constitutional and statutory claims brought against Defendants Transworld, Comcast, T-
12 Mobile, and McLeod, (“Defendants”), in the separate cases transferred by the Panel on
13 Multidistrict Litigation in this matter in its orders dated August 14, 2006, and September 25, 2006
14 (“transferred cases”). Unless otherwise ordered by this Court, all federal claims presented in any
15 case against Defendants subsequently transferred to this Court by the Panel on Multidistrict
16 Litigation in this matter shall be deemed to be included in this Master Complaint.
17

18 2. This Master Complaint is filed solely as an administrative device to promote
19 judicial efficiency and economy in the adjudication and resolution of pretrial matters and is not
20 intended to effect consolidation for trial of the transferred cases. Neither is this Master Complaint
21 intended to cause, nor to change the rights of the parties, nor to make those who are parties in one
22 transferred case parties in another.
23

24 3. This case challenges the legality of Defendants’ participation in a secret and
25 illegal government program to intercept and analyze vast quantities of Americans’ telephone and
26 Internet communications and records, surveillance done without any statutorily authorized
27 permission, customers’ knowledge or consent, or the authorization of a court, and in violation of
28

1 federal electronic surveillance and telecommunications statutes, as well as the First and Fourth
2 Amendments to the United States Constitution. In addition, Plaintiffs challenge Defendant's
3 conduct under state law.

4
5 **JURISDICTION AND VENUE**

6 4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331,
7 28 U.S.C. § 1332(d), 18 U.S.C. § 2707, and 47 U.S.C. § 605. Supplemental jurisdiction over state
8 law claims is founded on 28 U.S.C. § 1367.

9 5. Venue is proper in this District pursuant to the order of the Panel on
10 Multidistrict Litigation.

11 **PARTIES**

12 6. Plaintiff Travis Cross is an individual residing in Indianapolis, Indiana, and
13 has been a subscriber and user of Comcast Telecommunications, Inc.'s Internet service for more
14 than three years, and has used it to send and receive e-mail messages.

15 7. Plaintiffs Christopher and Rebecca Yowitz, husband and wife, reside in
16 Coopersville, Michigan, and are subscribers and users of Transworld's telecommunications
17 services, and have used them to make telephone or wireless calls and/or to send and receive
18 Internet messages and e-mails.

19 8. Plaintiff Sam Goldstein is an individual residing in Indianapolis, Indiana,
20 and has been a subscriber and user of McLeod's, long distance service since at least 2000 and has
21 used it to make long distance telephone calls. Plaintiff Goldstein has also been a subscriber and
22 user of Comcast's Internet service for at least two years and has used it to send and receive e-mail
23 messages.

24 9. Plaintiff The Libertarian Party of Indiana is a political party with its central
25 office located in Indianapolis, Indiana, and is a subscriber and user of McLeod's long distance
26
27
28

1 service, and has used it to make long distance telephone calls. The Libertarian Party of Indiana has
2 a special interest in this action as Defendants' wrongful conduct affects its specially protected rights
3 to political speech.

4 10. Plaintiff Carolyn W. Rader is an individual living in Indianapolis, Indiana,
5 and has been a subscriber and user of MCE Communications Services, Inc. since 2001 and has
6 used it to make telephone calls. Ms. Rader was previously a user and subscriber of T-Mobile's
7 cellular phone services, and used it to make wireless calls. Ms. Rader has a special interest in this
8 action in that she is a licensed attorney legally obligated to protect communications with her
9 clients.
10

11 11. Plaintiff Sam Goldstein Insurance Agency, Inc. is a domestic corporation
12 doing business in Indianapolis, Indiana, and has been a subscriber and user of McLeod's long
13 distance service since at least 2000, and has used it to make long distance telephone calls. It has
14 also been a user and subscriber to Comcast's Internet services for at least two years, and has used it
15 to send and receive e-mail messages.
16

17 12. Plaintiff Sean Sheppard is an individual residing in Indianapolis, Indiana,
18 and has been a subscriber and user of Comcast's Internet services for approximately four years and
19 has used it to send and receive e-mail messages.
20

21 13. Defendant Transworld is a Minnesota corporation registered to do business
22 in many states, including but not limited to the State of Michigan, and is a "telecommunication
23 carrier" within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and
24 provides remote computing and electronic communications services to the public.

25 14. Defendant Comcast is a Pennsylvania corporation registered to do business
26 in many states, including but not limited to the State of Indiana, and is a "telecommunication
27
28

1 carrier” within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and
2 provides remote computing and electronic communications services to the public.

3 15. Defendant McLeod is an Iowa corporation registered to do business in many
4 states, including but not limited to the State of Indiana, and is a “telecommunication carrier” within
5 the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides remote
6 computing and electronic communications services to the public.
7

8 16. Defendant T-Mobile is a Delaware corporation registered to do business in
9 many states, including but not limited to the State of Indiana, and is a “telecommunication carrier”
10 within the meaning of the Communications Act of 1934, 47 U.S.C. §§ 151, *et seq.* and provides
11 remote computing and electronic communications services to the public.
12

13 **FACTUAL ALLEGATIONS**

14 17. In Section 222 of the Communications Act of 1934 (47 U.S.C. § 222(c)(1)),
15 Congress imposed upon telecommunication carriers such as Defendants a duty to protect sensitive,
16 personal customer information from disclosure. This information includes “information that relates
17 to the quantity, technical configuration, type, destination, location, and amount of use of a
18 telecommunications service subscribed to by any customer of a telecommunications carrier, and
19 that is made available to the carrier by the customer solely by virtue of the carrier-customer
20 relationship” and data concerning service customers’ telephone calling histories (*i.e.*, date, time,
21 duration, and telephone numbers of calls placed or received) or call-detail records, and such
22 information constitutes “individually identifiable customer proprietary network information”
23 within the meaning of Section 222 of the Communications Act of 1934.
24

25 18. Federal law prohibits the federal government, which should be construed throughout
26 this Master Complaint to include the National Security Agency (“NSA”) and affiliated
27 governmental agencies, from obtaining customers’ call-detail records without a warrant, subpoena,
28

1 or other valid legal process, and similarly prohibits telecommunications providers, such as
2 Defendants, from giving such information to the government without judicial or other lawful
3 authorization, probable cause, and/or individualized suspicion.

4 19. Defendants Transworld, Comcast, T-Mobile, and McLeod, provide remote
5 computing and electronic communication services to the public.

6 20. In the aftermath of September 11, 2001, the Defendants commenced their
7 programs of providing the federal government with the telephone call contents and records of its
8 customers and subscribers. The Defendants continue to provide this information to the federal
9 government.

10 21. On December 16, 2005, in an article entitled “Bush Lets U.S. Spy on Callers
11 Without Courts,” *The New York Times* reported on an NSA program of eavesdropping on the
12 telephone conversations of Americans without court order as required by the Foreign Intelligence
13 Surveillance Act (“NSA Program”).

14 22. In a December 17, 2005, radio address, President George W. Bush admitted
15 that “[i]n the weeks following the terrorist attacks on our nation, [he] authorized the National
16 Security Agency, consistent with U.S. law and the Constitution, to intercept the international
17 communications of people with known links to al Qaeda and related terrorist organizations.”
18 President Bush further stated that “the activities [he] authorized are reviewed approximately every
19 45 days”; that he had “reauthorized this program more than 30 times since the September the 11th
20 attacks”; and that he intended to continue authorizing such activity “for as long as our nation faces
21 a continuing threat from al Qaeda and related groups.”

22 23. In a press briefing on December 19, 2005, by Attorney General Alberto
23 Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the
24 government claimed that the NSA Surveillance Program targets communications between a party
25
26
27
28

1 outside the United States and a party inside the United States when one of the parties of the
2 communication is believed to be “a member of al Qaeda, affiliated with al Qaeda, or a member of
3 an organization affiliated with al Qaeda, or working in support of al Qaeda.”

4 24. In a press release on December 19, 2005, Attorney General Alberto
5 Gonzales stated that the Program involved “intercepts of contents of communications” While
6 the Attorney General’s description of the Program was limited to interception of communications
7 with individuals “outside the United States,” Attorney General Gonzales explained that his
8 discussion was limited to those parameters of the program already disclosed by the President and
9 that many other operational aspects of the program remained highly classified.
10

11 25. On December 24, 2005, *The New York Times* reported in an article entitled,
12 “Spy Agency Mined Vast Data Trove, Officials Report,” that:

13 [t]he National Security Agency has traced and analyzed large volumes of telephone
14 and Internet communications flowing into and out of the United States as part of the
15 eavesdropping program that President Bush approved after the Sept. 11, 2001,
16 attacks to hunt for evidence of terrorist activity, according to current and former
17 government officials. The volume of information harvested from
18 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.

19 The officials said that as part of the program, “the N.S.A. has gained the cooperation of American
20 telecommunications companies to obtain backdoor access to streams of domestic and international
21 communications” and that the program is a “large data-mining operation” in which N.S.A.
22 technicians have combed through large volumes of phone and Internet traffic in search of patterns
23 that might point to terrorism suspects. *Id.* In addition, the article reports,

24 “[s]everal officials said that after President Bush’s order authorizing the N.S.A.
25 program, senior government officials arranged with officials of some of the nation’s
26 largest telecommunications companies to gain access to switches that act as
27 gateways at the borders between the United States’ communication networks and
28 international networks.”

1 26. In a January 3, 2006, article entitled, “Tinker, Tailor, Miner, Spy” (available
2 at <http://www.slate.com/toolbar.aspx?action=print&id=2133564>), Slate.com reported,

3 “[t]he agency [the NSA] used to search the transmissions it monitors for key words,
4 such as names and phone numbers, which are supplied by other intelligence
5 agencies that want to track certain individuals. But now the NSA appears to be
6 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.”

7 27. In a January 17, 2006, article, “Spy Agency Data After Sept. 11 Led F.B.I.
8 to Dead Ends,” *The New York Times* stated that officials who were briefed on the N.S.A. program
9 said that “the agency collected much of the data passed on to the F.B.I. as tips by tracing phone
10 numbers in the United States called by suspects overseas, and then by following the domestic
11 numbers to other numbers called. In other cases, lists of phone numbers appeared to result from
12 the agency’s computerized scanning of communications coming into and going out of the country
13 for names and keywords that might be of interest.”

14 28. A January 20, 2006, article in the *National Journal*, entitled “NSA Spy
15 Program Hinges On State-Of-The-Art Technology,” reported that

16 “[o]fficials with some of the nation’s leading telecommunications companies have
17 said they gave the NSA access to their switches, the hubs through which enormous
18 volumes of phone and e-mail traffic pass every day, to aid the agency’s effort to
19 determine exactly whom suspected Qaeda figures were calling in the United States
20 and abroad and who else was calling those numbers. The NSA used the intercepts
to construct webs of potentially interrelated persons.”

21 29. In a January 21, 2006, article in *Bloomberg News* entitled “Lawmaker
22 Queries Microsoft, Other Companies On NSA Wiretaps,” Daniel Berninger, a senior analyst at Tier
23 1 Research in Plymouth, Minnesota, said,

24 “[i]n the past, the NSA has gotten permission from phone companies to gain access
25 to so-called switches, high-powered computer into which phone traffic flows and is
26 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,
27 length, origin and destination.”

1 30. On February 5, 2006, an article appearing in the Washington Post entitled
2 “Surveillance Net Yields Few Suspects” stated that officials said

3 “[s]urveillance takes place in several stages . . . the earliest by machine. Computer-
4 controlled systems collect and sift basic information about hundreds of thousands of
5 faxes, e-mails and telephone calls into and out of the United States before selecting
6 the ones for scrutiny by human eyes and hears. Successive stages of filtering grow
7 more intrusive as artificial intelligence systems rank voice and data traffic in order
8 of likeliest interest to human analysts.”

9 The article continues,

10 “[f]or years, including in public testimony by Hayden, the agency [the NSA] has
11 acknowledged use of automated equipment to analyze the contents and guide
12 analysts to the most important ones. According to one knowledgeable source, the
13 warrantless program also uses those methods. That is significant . . . because this
14 kind of filtering intrudes into content, and machines ‘listen’ to more Americans than
15 humans do.”

16 31. On February 6, 2006, in an article entitled “Telecoms Let NSA Spy On
17 Calls,” *USA Today* reported that “[t]he National Security Agency has secured the cooperation of
18 large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop
19 without warrants on international calls by suspected terrorists, according to seven
20 telecommunications executives.” The article acknowledged that *The New York Times* had
21 previously reported that the telecommunications companies had been cooperating with the
22 government but had not revealed the names of the companies involved. In addition, it stated that
23 long-distance carriers AT&T, MCI, and Sprint “all own ‘gateway’ switches capable of routing calls
24 to points around the globe:

25 “Decisions about monitoring calls are made in four steps, according to two U.S.
26 intelligence officials familiar with the program who insisted on anonymity because
27 it remains classified:

- 28 • Information from U.S. or allied intelligence or law enforcement points to a terrorism-related target either based in the United States or communicating with someone in the United States.
- Using a 48-point checklist to identify possible links to al-Qaeda, one of three NSA officials authorized to approve a warrantless intercept decides whether the surveillance is justified. Gen. Michael Hayden, the nation’s No. 2 intelligence

1 officer, said the checklist focuses on ensuring that there is a ‘reasonable basis’
2 for believing there is a terrorist link involved.

- 3 • Technicians work with phone company officials to intercept communications
4 pegged to a particular person or phone number. Telecommunications executives
5 say MCI, AT&T, and Sprint grant the access to their systems without warrants
6 or court orders. Instead, they are cooperating on the basis of oral requests from
7 senior government officials.
- 8 • If the surveillance yields information about a terror plot, the NSA notifies the
9 FBI or other appropriate agencies but does not always disclose the source of its
10 information. Call-routing information provided by the phone companies can
11 help intelligence officials eavesdrop on a conversation. It also helps them
12 physically locate the parties, which is important if cell phones are being used. If
13 the U.S. end of a communication has nothing to do with terrorism, the identity
14 of the party is suppressed and the content of the communication destroyed,
15 Hayden has said.

16 32. On May 11, 2006, in an article entitled “NSA Has A Massive Database Of
17 Americans’ Phone Calls,” *USA Today* reported that “[t]he National Security Agency has been
18 secretly collecting the phone call records of tens of millions of Americans, using data provided by
19 AT&T, Verizon and Bellsouth,” according to multiple sources with “direct knowledge of the
20 arrangement.” One of the confidential sources for the article reported that the NSA’s goal is “to
21 create a database of every call ever made” within the United States. The confidential sources
22 reported that AT&T and the other carriers are working “under contract” with the NSA, which
23 launched the program in 2001 shortly after the September 11, 2001 terrorist attacks. At the U.S.
24 Senate confirmation hearing on his nomination to become Director of the Central Intelligence
25 Agency, General Michael Hayden, who was the Director of the NSA at the time, confirmed that the
26 program was “launched” on October 6, 2001.

27 33. The May 11, 2006, *USA Today* story was confirmed by a U.S. intelligence
28 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

1 pay for the cooperation, and that both “AT&T, which at the time was headed by C. Michael
2 Armstrong,” and “SBC, headed by Ed Whitacre,” agreed to provide the NSA with the requested
3 information.

4
5 34. The May 11, 2006, *USA Today* story reported that the NSA requested that
6 Qwest Communications, Inc. (“Qwest”), another telecommunications carrier, provide the NSA
7 with its customers’ call-detail records, but Qwest refused. Qwest requested that the NSA first
8 obtain a court order, a letter of authorization from the U.S. Attorney General’s office, or
9 permission from a Court operating under the Foreign Intelligence Surveillance Act (“FISA”), but
10 the NSA refused, because it was concerned that the FISA Court and the Attorney General would
11 find the NSA’s request unlawful.

12
13 35. As of the date of the filing of this complaint, no part of the May 11, 2006,
14 *USA Today* story has been publicly denied by any representative of the federal government,
15 including the NSA.

16
17 36. Qwest’s decision not to participate was also reported in an article from *The*
18 *New York Times* on May 13, 2006, entitled, “Questions Raised For Phone Giants In Spy Data
19 Furor.” The article reported that Qwest’s former CEO, Mr. Joseph Nacchio,

20 “made inquiry as to whether a warrant or other legal process had been secured in
21 support of that request. When he learned that no such authority had been granted,
22 and that there was a disinclination on the part of the authorities to use any legal
23 process,” Mr. Nacchio concluded that the requests violated federal privacy
24 requirements ‘and issued instructions to refuse to comply.’”

25
26 37. Senator Christopher “Kit” Bond (R-MO), who also has received access to
27 information on warrantless surveillance operations, explained on May 11, 2006, on a PBS Online
28 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.”

1 38. On May 14, 2006, when Senate Majority Leader William Frist (R-TN) was
2 asked on CNN Late Edition with Wolf Blitzer whether he was comfortable with the program
3 described in the *USA Today* article, he stated "Absolutely. I am one of the people who are briefed .
4 . . I've known about the program. I am absolutely convinced that you, your family, our families are
5 safer because of this particular program."

6 39. On May 29, 2006, Seymour Hersh reported in *The New Yorker* in an article
7 entitled "Listening In" that a security consultant working with a major telecommunications carrier
8 "told me that his client set up a top-secret high-speed circuit between its main
9 computer complex and Quantico, Virginia, the site of a government-intelligence
10 computer center. This link provided direct access to the carrier's network core – the
11 critical area of its system, where all its data are stored. 'What the companies are
12 doing is worse than turning over records,' the consultant said. 'They're providing
total access to all the data.'"

13 40. A June 30, 2006, *USA Today* story reported that 19 members of the
14 intelligence oversight committees of the U.S. Senate and House of Representatives "who had been
15 briefed on the program verified that the NSA has built a database that includes records of
16 Americans' domestic phone calls," and that four of the committee members confirmed that "MCI,
17 the long-distance carrier that Verizon acquired in January, did provide call records to the
18 government."

19 41. The Defendants knowingly and intentionally provided the aforementioned
20 telephone contents and records to the federal government.

21 42. Upon information and belief, the NSA accomplishes its surveillance
22 activities through the installation, maintenance and operation of various electronic routing and
23 trapping equipment placed on the premises, or attached to the property, of Defendants to gain
24 access to Defendants' stored databases of customer records and live electronic communication
25 pathways ("NSA Program"). Such equipment, which provides the NSA with a direct tap into the
26
27
28

1 nations' telecommunication pipelines, would not have been installed, operated and/or maintained
2 by the NSA absent cooperation, permission, and/or knowledge of the Defendants.

3 43. As part of the NSA Program, the NSA's operational personnel identify
4 particular individual targets, and their communications, through a software data mining process
5 that NSA runs against vast databases of the Defendants' stored electronic records of their
6 customers' domestic and international telephone and Internet communications in search of
7 particular names, numbers, words or phrases and patterns of interest. The NSA's operational
8 personnel also identify communications of interest in real-time through similar data-mining
9 software functionality.
10

11 44. Besides actually eavesdropping on specific conversations, NSA personnel
12 have intercepted large volumes of domestic and international telephone and Internet traffic in
13 search of patterns of interest, in what has been described in press reports as a large "data mining"
14 program.
15

16 45. As part of this data-mining program, the NSA intercepts millions of
17 communications made or received by people inside the United States, and uses powerful computers
18 to scan their contents for particular names, numbers, words, or phrases.

19 46. Additionally, the NSA collects and analyzes a vast amount of
20 communications traffic data to identify persons whose communications patterns the government
21 believes may link them, even if indirectly, to investigatory targets.
22

23 47. The NSA has accomplished its massive surveillance operation by arranging
24 with some of the nation's largest telecommunications companies to gain direct access to the
25 telephone and Internet communications transmitted via those companies' domestic
26 telecommunications facilities, and to those companies' records pertaining to the communications
27 they transmit.
28

1 48. The Defendants have intercepted and continue to provide the government
2 with direct access to all or a substantial number of the communications transmitted through its key
3 domestic telecommunications facilities, including direct access to streams of domestic,
4 international, and foreign telephone and Internet communications.

5 49. Since in or about October of 2001, the Defendants have disclosed and/or
6 divulged the “call-detail records” of all or substantially all of their customers, including Plaintiffs,
7 to the NSA, in violation of federal law, as more particularly set forth below.

8 50. The Defendants have, since in or about October 2001, been disclosing to the
9 NSA “individually identifiable customer proprietary network information” belonging to all or
10 substantially all of their customers, including, but not limited to, Plaintiffs, in violation of federal
11 law, as more particularly set forth below.

12 51. The Defendants have disclosed and continue to disclose and/or provide the
13 government with direct access to its databases of stored telephone and Internet records, which are
14 updated with new information in real time or near-real time.

15 52. The Defendants have provided at all relevant times and continue to provide
16 computer or storage processing services to the public, by means of wire, radio, electromagnetic,
17 photo-optical, or photo-electronic facilities for the transmission of wire or electronic
18 communications, and/or by means of computer facilities or related electronic equipment for the
19 electronic storage of such communications.

20 53. The Defendants have knowingly authorized, and continue to knowingly
21 authorize, NSA and affiliated governmental agencies to install and use, or have assisted
22 government agents in installing or using, interception devices and pen registers and/or trap and
23 trace devices on the Defendants’ domestic telecommunications facilities in connection with the
24 Program.

1 54. The interception devices and pen registers and/or trap and trace devices
2 capture, record or decode the various information pertaining to individual class member
3 communications including dialing, routing, addressing and/or signaling information (“DRAS
4 information”) for all or a substantial number of all wire or electronic communications transferred
5 through the Defendants’ domestic telecommunications facilities where those devices have been
6 installed.

8 55. Using these devices, government agents have acquired and are acquiring
9 wire or electronic communications content and DRAS information directly via remote or local
10 control of the device.

11 56. In addition, or in the alternative, the Defendants have disclosed and are
12 disclosing wire or electronic communications content and DRAS information to the government
13 after interception, capture, recording or decoding.

15 57. The Defendants have knowingly authorized, and continue to knowingly
16 authorize, the NSA and affiliated governmental agencies to directly access, through the installed
17 devices, all domestic, international and foreign telephone and wireless telephone and Internet
18 communications transmitted through the Defendants’ domestic telecommunications infrastructure
19 and facilities for use in the Program.

20 58. The Defendants provide the aforementioned telephone contents and records
21 to the federal government without judicial or other lawful authorization, a court order, warrant,
22 subpoena, statutory authorization, or certification pursuant to Chapters 119 and 121 of Title 18 of
23 the United States Code, and records pertaining to their communications occurred without judicial
24 or other lawful authorization, probable cause, and/or individualized suspicion.

26 59. The Defendants did not disclose to its customers, including plaintiffs, that it
27 was providing the aforementioned telephone contents and records to the federal government. Thus,
28

1 the Defendants' customers, including plaintiffs, were not given the opportunity to, nor did they
2 consent to the disclosure of their telephone contents and records.

3 60. The telephone contents and records intercepted and/or disclosed and/or
4 divulged by the Defendants to the federal government pursuant to the program challenged herein
5 were not divulged (a) pursuant to a law enforcement investigation concerning telemarketing fraud;
6 (b) as a necessary incident to the rendition of services to customers; (c) to protect the rights or
7 property of the Defendants; (d) based on a reasonable and/or good faith belief that an emergency
8 involving danger of death or serious physical injury required disclosure without delay; (e) to the
9 National Center for Missing and Exploited Children; or (f) to a non-governmental person or entity.
10

11 61. Defendants' violations were done with knowledge of the illegality, and
12 therefore were made in bad faith.
13

14 **CLASS ACTION ALLEGATIONS**

15 62. Plaintiffs brings this action under Federal Rule of Civil Procedure 23 on
16 behalf of themselves and a Class, defined as:

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

23 63. Plaintiff seeks certification of the Class under Federal Rule of Civil
24 Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

25 64. The Class number{s} in the millions, so that joinder of all members is
26 impractical.
27
28

1 communication service, and/or while carried or maintained by a Telecom Defendant remote
2 computing service, in violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2).

3 91. The Defendants did not notify Plaintiffs of the divulgence of their
4 communications, nor did Plaintiffs consent to such.

5 92. Neither the NSA nor any other governmental entity has obtained a warrant
6 authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(A).

7 93. Neither the NSA nor any other governmental entity has obtained a court
8 order authorizing the disclosures, pursuant to 18 U.S.C. § 2703(c)(1)(B) and (d).

9 94. Neither the NSA nor any other governmental entity has issued or obtained an
10 administrative subpoena authorized by a federal or state statute authorizing such disclosures,
11 pursuant to 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

12 95. Neither the NSA nor any other governmental entity has issued or obtained a
13 federal or state grand jury or trial subpoena authorizing such disclosures, pursuant to 18 U.S.C.
14 § 2703(c)(1)(E) and (c)(2).

15 96. Defendants have not been provided with a certification in writing by a
16 person specified in 18 U.S.C. § 2518(7) or by the Attorney General of the United States meeting
17 the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B), *i.e.*, a certification that no warrant or court order
18 authorizing the disclosures is required by law, and that all statutory requirements have been met.

19 97. The disclosures were and are not authorized by any statute or legislation.

20 98. Defendants' disclosures in violation of 18 U.S.C. § 2702(a)(3) were and are
21 knowing, intentional, and willful.

22 99. Defendants' continued engagement in the above-described divulgence of
23 Plaintiffs' communications while in electronic storage by Defendants' electronic communication
24
25
26
27
28

1 service(s), and/or while carried or maintained by Defendants' remote computing service(s)
2 represents a credible threat of immediate future harm.

3 100. Plaintiffs have been and are aggrieved by Defendants' above-described
4 divulgence of the contents of their communications.

5 101. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person
6 aggrieved by knowing or intentional violation of 18 U.S.C. § 2702, Plaintiffs seek such preliminary
7 and other equitable or declaratory relief as may be appropriate; statutory damages of no less than
8 \$1000 for each aggrieved Plaintiff; punitive damages as the Court considers just, and reasonable
9 attorneys' fees and other litigation costs reasonably incurred.
10

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

13 102. Plaintiffs incorporate all of the allegations contained in the preceding
14 paragraphs of this complaint, as if set forth fully herein.

15 103. In relevant part, 18 U.S.C. § 2702 provides that:

16 (a) Prohibitions. – Except as provided in subsection . . . (c) –
17 (3) a provider of . . . electronic communication service to
18 the public shall not knowingly divulge a record or other
19 information pertaining to a subscriber to or customer of
20 such service (not including the contents of communications
covered by paragraph (1) or (2) to any governmental entity.

21 104. Defendants' telephone services are "electronic communication service[s],"
22 as that term is defined in 18 U.S.C. § 2510(15), provided to the public, including Plaintiffs.

23 105. The Defendants violated 18 U.S.C. § 2702(a)(3) by knowingly and
24 intentionally divulging to the federal government records or other information pertaining to
25 subscribers or customers of the Defendants' remote computing and electronic services.
26
27
28

1 106. The Defendants' challenged program of disclosing telephone records to the
2 federal government does not fall within any of the statutory exceptions or immunities set forth in
3 18 U.S.C. §§ 2702(c), 2703(c), or 2703(e).

4 107. Neither the NSA nor any other governmental entity has obtained a warrant
5 authorizing the disclosures, as is required by 18 U.S.C. § 2703(c)(1)(A).

6 108. Neither the NSA nor any other governmental entity has obtained a court
7 order authorizing the disclosures, as is required by 18 U.S.C. § 2703(c)(1)(B) and (d).

8 109. Neither the NSA nor any other governmental entity has issued or obtained an
9 administrative subpoena authorized by any federal or state statute authorizing such disclosures, as
10 is required by 18 U.S.C. § 2703(c)(1)(E) and (c)(2).

11 110. Neither the NSA nor any other governmental entity has issued or obtained a
12 federal or state grand jury or trial subpoena authorizing such disclosures, as is required by 18
13 U.S.C. § 2703(c)(1)(E) and (c)(2).

14 111. Defendants have not been provided with a certification in writing by a
15 person specified in 18 U.S.C. § 2518(7), by the Director of the Federal Bureau of Investigation or
16 his designee or a Special Agent in Charge in a Bureau field office pursuant to 18 U.S.C. § 2709(b),
17 or by the Attorney General of the United States to meet the requirements of 18 U.S.C.
18 § 2511(2)(a)(ii)(B), *i.e.*, certifying that no warrant or court order authorizing the disclosures is
19 required by law, and that all statutory requirements have been met.

20 112. The disclosures were and continue to be unauthorized by any statute or
21 legislation.

22 113. Plaintiffs have been and continue to be aggrieved by the Defendants'
23 knowing and intentional past disclosure and/or imminent future disclosure of their records to the
24
25
26
27
28

1 federal government. Accordingly, Plaintiffs may challenge this violation of 18 U.S.C. § 2702(a)(3)
2 pursuant to the cause of action created by 18 U.S.C. § 2707(a).

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

5 114. Plaintiffs incorporate all of the allegations contained in the preceding
6 paragraphs of this complaint, as if set forth fully herein.

7
8 115. In relevant part, 18 U.S.C. § 2511 provides that:

9 (1) Except as otherwise specifically provided in this chapter, any
10 person who –

11 (a) intentionally intercepts, endeavors to intercept, or
12 procures any other person to intercept or endeavor to
13 intercept, any wire, oral or electronic communication. . .

14 (c) intentionally discloses, or endeavors to disclose, to any
15 other person the contents of any wire, oral, or electronic
16 communication, knowing or having reason to know that
17 the information was obtained through the interception of
18 a wire, oral, or electronic communication in violation of
19 this subsection;

20 (d) intentionally uses, or endeavors to disclose, to any other
21 person the contents of any wire, oral, or electronic
22 communication, knowing or having reason to know that
23 the information was obtained through the interception of
24 a wire, oral, or electronic communication in violation of
25 this subsection. . . .

26 (3)(a) Except as provided in paragraph (b) of this subsection, a
27 person or entity providing an electronic communication service
28 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 than addressee or intended recipient of
such communication or an agent of such addressee or intended
recipient.

29 116. The Defendants violated 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d), and (3)(a)
30 by intentionally intercepting and disclosing to the federal government the contents of telephone
31 calls of the Defendants' customers.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

129. In relevant part 50 U.S.C. §1801 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.

130. The Defendants have intentionally acquired, by means of a surveillance device, the contents of one or more telephone, wireless or Internet communications to or from Plaintiffs or other information in which Plaintiffs have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.

131. By the acts alleged herein, the 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 to such electronic surveillance, in violation of 50 U.S.C. §1809.

1 132. Additionally or in the alternative, by the acts alleged herein, the Defendants
2 have intentionally disclosed or used information obtained under color of law by electronic
3 surveillance, knowing or having reason to know that the information was obtained through
4 electronic surveillance not authorized by statute.

5 133. The Defendants did not notify Plaintiffs of the above-described electronic
6 surveillance, disclosure, and/or use, nor did Plaintiffs consent to such.

7 134. The Defendants' challenged program of electronic surveillance does not fall
8 within any of the statutory exceptions or immunities set forth in 50 U.S.C. § 1809(b).

9 135. Defendants' continued engagement in the above-described electronic
10 surveillance, disclosure, and/or use of Plaintiffs' electronic communications described herein, and
11 that likelihood represents a credible threat of immediate future harm.

12 136. Plaintiffs have been and continue to be aggrieved by the Defendants
13 electronic surveillance, disclosure, and/or use of their wire communications.

14 137. Pursuant to 50 U.S.C. §1810, which provides a civil action for any person
15 who has been subjected to an electronic surveillance or about whom information obtained by
16 electronic surveillance of such person has been disclosed or used in violation of 50 U.S.C. §1809,
17 Plaintiffs seek equitable and declaratory relief; statutory damages for each Plaintiff and class
18 member of whichever is the greater of \$100 a day for each day of violation or \$1,000; punitive
19 damages as appropriate; and reasonable attorneys' fees and other litigation costs reasonably
20 incurred.
21
22
23

24 **SIXTH CLAIM FOR RELIEF**
25 **Violation of the First and Fourth Amendments**
26 **to the United States Constitution**

27 138. Plaintiffs incorporate all of the allegations contained in the preceding
28 paragraphs of this complaint, as if set forth fully herein.

1 139. Plaintiffs have a reasonable expectation of privacy in their communications,
2 contents of communications, and/or records pertaining to their communications transmitted,
3 collected, and/or stored by the Defendants, which was violated by the Defendants' above-described
4 actions as agents of the government, which constitute a search and seizure of Plaintiffs'
5 communications and records.
6

7 140. Plaintiffs use the Defendants' services to speak or receive speech
8 anonymously and to associate privately.

9 141. The above-described acts of interception, disclosure, divulgence and/or use
10 of Plaintiffs' communications, contents of communications, and records pertaining to their
11 communications occurred without judicial or other lawful authorization, probable cause, and/or
12 individualized suspicion.
13

14 142. At all relevant times, the federal government instigated, directed, and/or
15 tacitly approved all of the above-described acts of the Defendants.

16 143. At all relevant times, the federal government knew of and/or acquiesced in
17 all of the above-described acts of the Defendants, and failed to protect the First and Fourth
18 Amendment rights of the Plaintiffs by obtaining judicial authorization.

19 144. In performing the acts alleged herein, the Defendants had at all relevant
20 times a primary or significant intent to assist or purpose of assisting the government in carrying out
21 the Defendants' program and/or other government investigations, rather than to protect its own
22 property or rights.
23

24 145. By the acts alleged herein, the Defendants acted as instruments or agents of
25 the government, and thereby violated Plaintiffs' reasonable expectations of privacy and denied
26 Plaintiffs their right to be free from unreasonable searches and seizures as guaranteed by the Fourth
27
28

1 Amendment to the Constitution of the United States, and additionally violated Plaintiffs' rights to
2 speak and receive speech anonymously and associate privately under the First Amendment.

3 146. By the acts alleged herein, the Defendants' conduct proximately caused
4 harm to Plaintiffs.

5 147. The Defendants' conduct was done intentionally, with deliberate
6 indifference, or with reckless disregard of, Plaintiffs' constitutional rights.
7

8 **SEVENTH CLAIM FOR RELIEF**
9 **Violation of State Surveillance Statutes**

10 120. Plaintiffs repeat and incorporate herein by reference the allegations in the
11 preceding paragraphs of this complaint, as if set forth fully herein.
12

13 121. Plaintiffs further state that Defendants have engaged and continue to engage
14 in the unlawful eavesdropping, surveillance, and/or interception of wire, oral, and/or electronic
15 communications, the disclosure and/or divulgence and/or use of the contents of such
16 communications, and/or the unlawful installation and/or use of pen registers or trap and trace
17 devices.
18

19 122. The foregoing conduct violates the following state statutes:

- 20 a. Ala. Code §§ 13A-11-30, 13A-11-31 (2006)
- 21 b. Alaska Stat. § 42.20.310 (2005)
- 22 c. Ariz. Rev. Stat. Ann. § 13-3005 (2006)
- 23 d. Ark. Code Ann. § 5-60-120 (2005)
- 24 e. Cal. Penal Code § 630 et seq. (2006)
- 25 f. Colo. Rev. Stat. §§ 18-9-301, 18-9-303 (2006)
- 26 g. Conn. Gen. Stat. § 52-570d (2006)
- 27 h. Del. Code Ann. Tit. 11, § 2402 (2005)
- 28 i. D.C. Code §§ 23-541, 23-542 (2006)
- j. Fla. Stat. §§ 934.01-03 (2005)
- k. Ga. Code Ann. §§ 16-11-62 et seq. (2005)

- 1 l. Haw. Rev. Stat. § 803-42, 803-48 (2005)
- 2 m. Idaho Code Ann. § 18-6702 (2005)
- 3 n. 720 Ill. Comp. Stat. 5/14-1, -2 (2006)
- 4 o. Ind. Code § 35-33.5-1 et seq. (2005)
- 5 p. Iowa Code § 727.8 (2005)
- 6 q. Kan. Stat. Ann. §§ 21-4001, 21-4002 (2004)
- 7 r. Ky. Rev. Stat. Ann. §§ 526.010-.020 (2005)
- 8 s. La. Rev. Stat. Ann. § 15:1303 (2005)
- 9 t. Me. Rev. Stat. Ann. Tit. 15, §§ 709-710 (2006)
- 10 u. Md. Code Ann. Cts. & Jud. Proc. § 10-402 et seq.; § 10-4A-4B et seq. (2006)
- 11 v. Mass. Gen. Laws ch. 272, § 99 (2006)
- 12 w. Mich. Comp. Laws § 750.539 et seq. (2006)
- 13 x. Minn. Stat. §§ 626A.01, .02 (2005)
- 14 y. Miss. Code Ann. § 41-29-501 et seq. (2006)
- 15 z. Mo. Rev. Stat. §§ 392.170, .350, 542.402, .418 (2006)
- 16 aa. Mont. Code Ann. § 45-8-213 (2006)
- 17 bb. Neb. Rev. Stat. § 86-290 (2006)
- 18 cc. Nev. Rev. Stat. 200.610-.620 (2006)
- 19 dd. N.H. Rev. Stat. Ann. §§ 570-A:1, -A:2 (2005)
- 20 ee. N.J. Stat. Ann. § 2A:156A-1 et seq. (2006)
- 21 ff. N.M. Stat. § 30-12-1 (2006)
- 22 gg. N.Y. Penal Law §§ 250.00, .05 (2006)
- 23 hh. N.C. Gen. Stat. § 15A-287 (2006)
- 24 ii. N.D. Cent. Code § 12.1-15-02 (2006)
- 25 jj. Ohio Rev. Code Ann. § 2933.51 et seq. (2006)
- 26 kk. Okla. Stat. tit. 13, § 176.1 et seq. (2006)
- 27 ll. Or. Rev. Stat. §§ 165.540, .543 (2006)
- 28 mm. 18 Pa. Cons. Stat. § 5701 et seq. (2005)
- nn. R.I. Gen. Laws § 11-35-21 (2005)
- oo. S.C. Code Ann. §§ 17-30-20, -30 (2005)
- pp. S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20 (2006)
- qq. Tenn. Code Ann. § 39-13-601 (2006)

- 1 rr. Tex. Penal Code Ann. § 16.02 et seq.; Tex. Code Crim.
- 2 Proc. art. 18.20 § 16(a) (2005)
- 3 ss. Utah Code Ann. § 77-23a-1 et seq. (2005)
- 4 tt. Va. Code Ann. §§ 19.2-61, -62 (2006)
- 5 uu. Wash. Rev. Code § 9.73.030 (2006)
- 6 vv. W. Va. Code § 62-1D-1 et seq. (2006)
- 7 ww. Wis. Stat. §§ 968.27, .31 (2005)
- 8 xx. Wyo. Stat. Ann. §§ 7-3-701, -702 (2005)

EIGHTH CLAIM FOR RELIEF
Violations of the State Consumer Protection Statutes

9
10 159. Plaintiffs incorporate all of the allegations contained in the preceding
11 paragraphs of this complaint, as if set forth fully herein.

12 160. Plaintiffs further state that Defendants have violated and continue to violate
13 state consumer protection statutes by divulging records or other information pertaining to
14 subscribers and customers to a governmental entity, specifically the NSA, without Plaintiffs'
15 knowledge or consent.

16 161. The unfair and deceptive trade acts and practices of Defendants directly,
17 foreseeably, and proximately cause damages and injury to Plaintiff and the Class.

18 162. The actions and failures to act of Defendants, including the false and
19 misleading representations and omissions of material facts regarding the protection and use of
20 Class members' private information constitute an unfair method and unfair and/or deceptive acts in
21 violation of the following state consumer protection statutes:
22

- 23 a) Defendants engage in unfair competition or deceptive acts or
- 24 practices in violation of Ala. Code § 8-19-1 et seq.;
- 25 b) Defendants engage in unfair competition or deceptive acts or
- 26 practices in violation of Alaska Stat. § 45.50.531(a);
- 27 c) Defendants engage in unfair competition or deceptive acts or
- 28 practices in violation of Ariz. Rev. Stat. § 44-1522 et seq.;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- d) Defendants engage in unfair competition or deceptive acts or practices in violation of Ark. Code § 4-88-101 et seq.;
- e) Defendants engage in unfair competition or deceptive acts or practices in violation of Cal. Bus. & Prof. Code § 17200 et seq.;
- f) Defendants engage in unfair competition or deceptive acts or practices or has made false representations in violation of Colo. Rev. Stat. § 6-1-105 et seq.;
- g) Defendants engage in unfair competition or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b et seq.;
- h) Defendants engage in unfair competition or deceptive acts or practices in violation of 6 Del. Code § 2511 et seq.;
- i) Defendants engage in unfair competition or deceptive acts or practices or made false representations in violation of D.C. Code Ann. § 28-3901 et seq.;
- j) Defendants engage in unfair competition or deceptive acts or practices in violation of Fla. Stat. § 501.201 et seq.;
- k) Defendants engage in unfair competition or deceptive acts or practices in violation of Ga. Stat. § 10-1-392 et seq.;
- l) Defendants engage in unfair competition or deceptive acts or practices in violation of Haw. Rev. Stat. § 480 et seq.;
- m) Defendants engage in unfair competition or deceptive acts or practices in violation of Idaho Code § 48-601 et seq.;
- n) Defendants engage in unfair competition or deceptive acts or practices in violation of 815 Ill. Comp. Stat. § 505.1 et seq.;
- o) Defendants engage in unfair competition or deceptive acts or practices in violation of Ind. Code § 24-5-0.5 et seq.;
- p) Defendants engage in unfair competition or deceptive acts or practices in violation of Iowa Code § 714.16 et seq.;
- q) Defendants engage in unfair competition or deceptive acts or practices in violation of Kan. Stat. Ann. § 50-623 et seq.;
- r) Defendants engage in unfair competition or deceptive acts or practices in violation of Ky. Rev. Stat. § 367.1 10 et seq.;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- s) Defendants engage in unfair competition or deceptive acts or practices in violation of La. Rev. Stat. § 51:1401 et seq.;
- t) Defendants engage in unfair competition or deceptive acts or practices in violation of 5 Me. Rev. Stat. Ann. § 207 et seq.;
- u) Defendants engage in unfair competition or deceptive acts or practices in violation of Massachusetts General Laws Ch. 93A et seq.;
- v) Defendants engage in unfair competition or deceptive acts or practices in violation of Md. Com. Law Code § 13-101 et seq.
- w) Defendants engage in unfair competition or deceptive acts or practices in violation of Mich. Stat. § 445.901 et seq.;
- x) Defendants engage in unfair competition or deceptive acts or practices in violation of Minn. Stat. § 8.31 et seq.;
- y) Defendants engage in unfair competition or deceptive acts or practices in violation of Miss. Code Ann. § 75-24-1 et seq.;
- z) Defendants engage in unfair competition or deceptive acts or practices in violation of Mo. Ann. Stat. § 407.010 et seq.;
- aa) Defendants engage in unfair competition or deceptive acts or practices in violation of Mont. Code § 30-14-101 et seq.;
- bb) Defendants engage in unfair competition or deceptive acts or practices in violation of Neb. Rev. Stat. § 59-1601 et seq.;
- cc) Defendants engage in unfair competition or deceptive acts or practices in violation of Nev. Rev. Stat. § 598.0903 et seq.;
- dd) Defendants engage in unfair competition or deceptive acts or practices in violation of N.H. Rev. Stat. § 358-A:1 et seq.;
- ee) Defendants engage in unfair competition or deceptive acts or practices in violation of violation of N.J. Rev. Stat. § 56:8-1 et seq.;
- ff) Defendants engage in unfair competition or deceptive acts or practices in violation of N.M. Stat. § 57-12-1 et seq.;
- gg) Defendants engage in unfair competition or deceptive acts or practices in violation of N.Y. Gen. Bus. Law § 349 et seq.;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- hh) Defendants engage in unfair competition or deceptive acts or practices in violation of N.C. Gen. Stat. § § 75-1.1 et seq.;
- ii) Defendants engage in unfair competition or deceptive acts or practices in violation of N.D. Cent. Code § 51-15-01 et seq.;
- jj) Defendants engage in unfair competition or deceptive acts or practices in violation of Ohio Rev. Stat. § 1345.01 et seq.;
- kk) Defendants engage in unfair competition or deceptive acts or practices in violation of Okla. Stat. 15 § 751 et seq.;
- ll) Defendants engage in unfair competition or deceptive acts or practices in violation of Or. Rev. Stat. § 646.605 et seq.;
- mm) Defendants engage in unfair competition or deceptive acts or practices in violation of 73 Pa. Stat. § 201-1 et seq.;
- nn) Defendants engage in unfair competition or deceptive acts or practices in violation of R.I. Gen. Laws § 6-13.1-1 et seq.;
- oo) Defendants engage in unfair competition or deceptive acts or practices in violation of S.C. Code Laws § 39-5-10 et seq.;
- pp) Defendants engage in unfair competition or deceptive acts or practices in violation of S.D. Code Laws § 37-241 et seq.;
- qq) Defendants engage in unfair competition or deceptive acts or practices in violation of Tenn. Code Ann. § 47-18-101 et seq.;
- rr) Defendants engage in unfair competition or deceptive acts or practices in violation of Tex. Bus. & Com. Code § 17.41 et seq.;
- ss) Defendants engage in unfair competition or deceptive acts or practices in violation of Utah Code § 13-11-1 et seq.;
- tt) Defendants engage in unfair competition or deceptive acts or practices in violation of 9 Vt. Stat. § 2451 et seq.;
- uu) Defendants engage in unfair competition or deceptive acts or practices in violation of Va. Code § 59.1-196 et seq.;
- vv) Defendants engage in unfair competition or deceptive acts or practices in violation of Wash. Rev. Code § 19.86.010 et seq.;

1 ww) Defendants engage in unfair competition or deceptive acts or
2 practices in violation of W. Va. Code § 46A-6-101 et seq.;

3 xx) Defendants engage in unfair competition or deceptive acts or
4 practices in violation of Wis. Stat. § 100.18 et seq.; and

5 yy) Defendants engage in unfair competition or deceptive acts or
6 practices in violation of Wyo. Stat. Ann. § 40-12-101 et seq.

7 163. This injury is of the type the state consumer protection and deceptive
8 practices statutes were designed to prevent and directly results from Defendants' unlawful conduct.

9 **NINTH CLAIM FOR RELIEF**
10 **Unlawful and Unfair Business Practices in Violation of the**
11 **State Law**

12 164. Plaintiffs incorporate all of the allegations contained in the preceding
13 paragraphs of this complaint, as if set forth fully herein.

14 165. By engaging in the acts and practices described herein, Defendants have
15 engaged in unlawful and unfair business practices in violation of California's Unfair Competition
16 Law, Business & Professions Code §§ 17200, *et seq.*

17 166. Defendants' acts and practices are unlawful because, as described above,
18 they violate 47 U.S.C. § 222, 18 U.S.C. §§ 2702(a)(1), (a)(2), and (a)(3), 18 U.S.C. §§ 2511(1)(a),
19 (1)(c), (1)(d), and (3)(a), 40 U.S.C. § 1809, and 47 U.S.C. § 605.

20 167. Defendants' acts and practices are also unlawful because they violate
21 18 U.S.C. § 3121. In relevant part, 18 U.S.C. § 3121 provides that:

22
23 In general. – Except as provided in this section, no person may install or
24 use a pen register or a trap and trace device without first obtaining a court
25 order under section 3123 of this title or under the Foreign Intelligence
26 Surveillance Act of 1978 (50 U.S.C. 1801 *et seq.*).

27 As defined by 18 U.S.C. § 3127:

28 (3) the term “pen register” means a device or process which records or
decodes dialing, routing, addressing, or signaling information transmitted
by an instrument or facility from which a wire or electronic
communication is transmitted, provided, however, that such information

1 shall not include the contents of any communication, but such term does
2 not include any device or process used by a provider or customer of a wire
3 or electronic communication service for billing, or recording as an
4 incident to billing, for communications services provided by such provider
or any device or process used by a provider or customer of a wire
communication service for cost accounting or other like purposes in the
ordinary course of its business;

5 (4) the term “trap and trace device” means a device or process which
6 captures the incoming electronic or other impulses which identify the
7 originating number or other dialing, routing, addressing, and signaling
information reasonably likely to identify the source of a wire or electronic
communication, provided, however, that such information shall not
include the contents of any communication

8 168. Defendants have installed or used pen registers and/or trap and trace devices
9 without first obtaining a valid court order under 18 U.S.C. § 3123 or a subpoena.

10 169. The pen registers and/or trap and trace devices installed and used by
11 Defendants have captured, recorded, or decoded, and continue to capture, record or decode, dialing,
12 routing, addressing or signaling information pertaining to Plaintiffs and/or California Subclass
13 members’ telephone, wireless, and Internet communications.

14 170. Defendants did not notify Plaintiff or California Subclass members of the
15 installation or use of pen registers and/or trap and trace devices. Plaintiff and California Subclass
16 members have not consented to Defendants’ installation or use of pen registers and/or trap and
17 trace devices.

18 171. Defendants are telecommunications carriers that obtain and have obtained
19 customer proprietary network information by virtue of its provision of telecommunications service.

20 172. Defendants used and/or disclosed to the NSA, a government entity,
21 individually identifiable customer proprietary network information pertaining to Plaintiffs and
22 California Subclass members.

23 173. Defendants failed to notify Plaintiffs or California Subclass members of the
24 disclosure and/or divulgence of their personally identifiable customer proprietary network
25 information to the NSA, nor did Plaintiff or California Subclass members consent to such.

26 174. Defendants’ acts and practices also constitute unfair business practices in
27 violation of California’s Unfair Competition Law, Business & Professions Code §§ 17200, *et seq.*,
28

1 because they contravene Defendant's privacy policy, which assures Plaintiffs and California
2 Subclass members that information pertaining to their telephone calls and/or Internet
3 communications will not be disclosed to third parties absent a valid court order or subpoena.

4 175. In violation of this policy and in breach of its trust with Plaintiffs and Class
5 members, including the California Subclass Members, Defendants disclosed the customer
6 proprietary network information belonging to Plaintiffs and the California Subclass, *i.e.*, their call-
7 detail records, to the NSA without a court order or subpoena.

8 176. Plaintiffs and the California Subclass seek restitution, injunctive relief, and
9 all other relief available under §§ 17200, *et seq.*]

10
11 **TENTH CLAIM FOR RELIEF**
Breach of Contract

12 177. Plaintiffs incorporate all of the allegations contained in the preceding
13 paragraphs of this complaint, as if set forth fully herein.

14 178. At all times relevant herein, Defendants agreed to provide for a subscription
15 fee, and Plaintiffs agreed to purchase from the Defendants various telecommunication and
16 electronic communication services.

17 179. At all times relevant herein, Defendants impliedly and expressly promised to
18 protect the privacy and confidentiality of its customers' information, identity, records, subscription,
19 use details, and communications, and, to abide by federal and state law.

20 180. At all times relevant herein, Defendants by their conduct as alleged, breach
21 their contract with the Plaintiffs, and breached the implied covenant of good faith and fair dealing
22 as well.¹

23 181. As a result of Defendants' breach of contractual duties owed to the Plaintiff,
24 Defendants are liable for damages including, but limited to nominal and consequential damages.
25

26
27 _____
28 ¹ Plaintiffs preserve such claims with respect to states where breach of the implied covenant of
good faith and fair dealing is plead separately.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PRAYER FOR RELIEF

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

- A. Declare that Defendant’s conduct as alleged herein violates applicable law;
- B. Award statutory damages to Plaintiff and the Class;
- C. Award punitive damages to Plaintiff and the Class;
- D. Award Plaintiff’s reasonable attorneys’ fees and costs of suit;
- E. Award restitution and all other relief allowed under State law claims
- F. Enjoin Defendant’s continuing violations of applicable law; and

Grant such other and further relief as the Court deems just and proper.

Dated: January 16, 2007

Respectfully submitted,

MOTLEY RICE LLC

/s/ Ronald L. Motley_____

Ronald L. Motley, Esq. (SC Bar No. RM-2730)
Jodi W. Flowers, Esq. (SC Bar No. 66300)
Donald Migliori, Esq. (RI Bar No. 4936;
MA Bar No. 567562; and MN Bar No. 0245951)
Vincent I. Parrett (CA Bar No. 237563)
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, South Carolina 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9027

INTERIM CLASS COUNSEL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I, Shana E. Scarlett, am the ECF User whose ID and password are being used to file this Master Consolidated Complaint Against Transworld Network Corp., et al. In compliance with General Order 45, X.B., I hereby attest that Ronald L. Motley has concurred in this filing.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on January 16, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List.

/s/
SHANA E. SCARLETT

LERACH COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
100 Pine Street, 26th Floor
San Francisco, CA 94111
Telephone: 415/288-4545
415/288-4534 (fax)
E-mail:shanas@lerachlaw.com