10-462-cv(L)

10-464-cv(CON)

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Securities and Exchange Commission,
Plaintiff-Appellee,
v.
Raj Rajaratnam and Danielle Chiesi,
Defendants-Appellants,

(Additional Caption on Reverse)

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANTS AND URGING REVERSAL

Marc Rotenberg
Counsel of Record
John Verdi
Jared Kaprove
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

April 30, 2010

and

Galleon Management, LP, Raiv Goel, Anil Kumar,
Mark Kurland, Robert Moffat, New Castle Funds LLC,
Roomy Khan, Deep Shah, Ali T. Far, Choo-Beng Lee,
Far & Lee LLC, Spherix Capital LLC, Ali Hariri, Zvi Goffer,
David Plate, Gautham Shankar,
Schottenfeld Group LLC, Steven Fortuna,
S2 Capital Management, LP,

Defendants.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c) for Case No. 10-462-cv(L)

Amicus Curiae Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

EPIC has participated as *amicus curiae* in several cases before the U.S. Supreme Court and other courts concerning privacy issues, new technologies, and Constitutional interests, including *City of Ontario v. Quon*, 554 F.3d 769 (9th Cir. 2009), *cert. granted*, 130 S. Ct. 1011 (U.S. Dec. 14, 2009) (No. 08-1332), *Doe v. Reed*, 529 F.3d 892 (9th Cir. 2008), *cert. granted*, 130 S. Ct. 1011 (U.S. Dec. 14, 2009) (No. 09-559); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Local Rule 29.1, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable and Telecommunications Association v. Federal Communications Commission*, 555 F.3d 996 (D.C. Cir. 2009); *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a longstanding interest in citizens' rights to be free from government surveillance absent a criminal predicate. In 2009, EPIC submitted a brief[2] in *Herring v. United States*.[3] EPIC's *amicus* brief highlighted the error rates in law enforcement databases, and supported citizens' Fourth Amendment right to be free from searches based on erroneous information. EPIC also has a particular interest in the proper interpretation of the Wiretap Act. In 2009, EPIC submitted a brief[4] in *Bunnell v. MPAA*.[5] EPIC's *amicus* brief supported the

[2] *See* EPIC: *Herring v. U.S.*, http://epic.org/privacy/herring/.
[3] *Herring v. United States*, 129 S. Ct. 695 (2009).
[4] *See* EPIC: *Bunnel v. MPAA*, http://epic.org/privacy/bunnell/.

application of the federal Wiretap Act's protections to email messages in circumstances when the messages are briefly stored while they pass through mail servers. In *Bunnell*, a former employee hacked his ex-employer's corporate email server to secretly swipe private emails as they were transmitted. EPIC argued that the Wiretap Act applies to these sorts of circumstances by barring "interception" of electronic communications. EPIC has long advocated for application of the "interception" standard to email, and filed a 2004 *amicus* brief on this issue in *United States v. Councilman*.[6]

EPIC supports the privacy rights of innocent individuals recorded on wiretaps. As discussed below, government statistics indicate that hundreds of thousands of individuals are recorded on wiretaps every year. Approximately 80% of those personal communications are wholly unrelated to criminal activity. They are personal, lawful phone calls, emails, and text messages exchanged by ordinary Americans with individuals who are the targets of wiretaps. In the present case, more than 550 of these individuals' communications were intercepted. These

---

[5] *Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007).

[6] *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004).

individuals are not parties to this litigation, and cannot meaningfully advocate for the preservation of their privacy. EPIC files this brief to represent the privacy interests of the 550 innocent individuals wiretapped in this matter. Further, we write on behalf of the hundreds of thousands of Americans who are wiretapped every year, though they are suspected of no crime, and their communications are irrelevant to any criminal investigation.

ARGUMENT

I. Law Enforcement Agents Wiretap Hundreds of Thousands of Individuals Every Year

> The tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.

Olmstead v. United States, 277 U.S. 438, 475 (1928) (Brandeis, J., dissenting).

Each year, law enforcement agencies intercept communications between hundreds of thousands of individuals in the United States. Law enforcement agents implement approximately 2,000 wiretaps every year. Administrative Office of the U.S. Courts, *2009 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* ("2009 Wiretap Report") at 5 ("A total of 2,376 intercepts authorized by federal and state courts were completed in 2009.")[7] A typical wiretap records communications

[7] *Available at* http://www.uscourts.gov/wiretap09/2009Wiretaptext.pdf; *see also* Administrative Office of the U.S. Courts, *2008 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of*

between approximately 100 individuals. 2009 Wiretap Report at 5 ("The average number of persons whose communications were intercepted [was] 113 per wiretap order in 2009").[8] Each year, wiretaps record the

---

Wire, Oral, or Electronic Communications at 5 (1,891 intercepts) *available at* http://www.uscourts.gov/wiretap08/contents.html; *see also* Administrative Office of the U.S. Courts, *2007 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* at 5 (2,208 intercepts) *available at* http://www.uscourts.gov/wiretap07/contents.html; Administrative Office of the U.S. Courts, *2006 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* at 5 (1,839 intercepts) *available at* http://www.uscourts.gov/wiretap06/contents.html; Administrative Office of the U.S. Courts, *2005 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* at 5 (1,773 intercepts) *available at* http://www.uscourts.gov/wiretap05/contents.html; Administrative Office of the U.S. Courts, *2004 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* at 5 (1,710 intercepts) *available at* http://www.uscourts.gov/wiretap04/contents.html; Administrative Office of the U.S. Courts, *2003 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* at 5 (1,442 intercepts) *available at* http://www.uscourts.gov/wiretap03/contents.html.

[8] *See also* 2008 Wiretap Report at 5 (92 individuals per wiretap); 2007 Wiretap Report at 5 (94 individuals per wiretap); 2006 Wiretap Report at 5 (112 individuals per wiretap); 2005 Wiretap Report at 5 (107

communications of approximately 200,000 individuals.[9] An average wiretap records communications for forty-two days. 2009 Wiretap Report at 5.

Some individual wiretaps substantially exceed these averages. 2008 Wiretap report at 9 ("wiretaps varied extensively with respect to … the number of intercepts per order, the number of persons whose communications were intercepted, the total number of communications intercepted, and the number of incriminating intercepts."). In a single wiretap that terminated in 2009, New York agents intercepted communications over the course of 534 days—more than one and a half years—recording 322,000 communications. 2009 Wiretap Report at 9. One 2008 wiretap intercepted communications over the course of 590 days, recording 168,292 communications. 2008 Wiretap Report at 9. In Illinois, a wiretap recorded 104,777 communications. *Id.* A 2008 California wiretap intercepted 1,961 individuals' communications. 2008 Wiretap Report at Table 4, Summary of Interceptions of Wire, Oral, or

---

individuals per wiretap); 2004 Wiretap Report at 5 (126 individuals per wiretap); 2003 Wiretap Report at 5 (116 individuals per wiretap)

[9] *E.g.* 268,488 individuals' communications recorded in 2009; 173,972 individuals' communications recorded in 2008; 207,552 individuals' communications recorded in 2007; 205,968 individuals' communications recorded in 2006.

Electronic Communications.[10] The interrelated wiretaps at issue in the present case also involved more communications than the national average. They intercepted 18,150 communications involving more than 550 individuals over sixteen months. Appellants' Brief at 9.

Wiretaps record telephone conversations, intercept email, access fax transmittals, and record text messages sent from mobile phones and pagers. 18 U.S.C. § 2519(1) (2009) (wiretaps defined as interceptions of "wire, oral, or electronic communications."); *see also* 2009 Wiretap Report at 9. Approximately 80% of wiretapped communications are characterized as "not incriminating" by the government. *Id.* at 5 ("The average percentage of intercepted communications that were incriminating remained unchanged at 19 percent in 2009.").[11]

II. The Vast Majority of Information Obtained Through Law Enforcement Wiretaps is Not Evidence of Criminal Wrongdoing

Law enforcement wiretaps gather a vast amount of personal information. While investigating potential criminal wrongdoing, agents seek to record as many communications between individuals as possible

---

[10] *Available at* http://www.uscourts.gov/wiretap08/contents.html.
[11] *See also* 2008 Wiretap Report (19% incriminating); 2006 Wiretap Report (20% incriminating); 2005 Wiretap Report (22% incriminating); 2004 Wiretap Report (21% incriminating).

in the hope that some of it may be helpful to the investigation or future prosecution. In the process, the government routinely collects a substantial number of communications that are not evidence of wrongdoing. As described above, approximately 80% of wiretapped communications are unrelated to criminal activity. *Supra* note 11. Many of these communications are sensitive and personal. *E.g.* Appellants' Brief at 23 (stating that some of the participants in the calls at issue in the present case are children); *Bynum v. United States*, 423 U.S. 952, 955 (1975) (Brennan, J., dissenting from denial of cert.) ("The other party in each of these conversations . . . was not a member of the narcotics conspiracy, and the conversations, which were sometimes the subject of jokes by the monitoring agents, were often of a highly personal and intimate nature.") The principles of search minimization and relevance, as well as the Fourth Amendment, limit the state's use of and access to these recordings. In the present case, the SEC seeks to perform an end run around these privacy safeguards and improperly force disclosure of hundreds of individuals' personal communications before a court rules on minimization, relevance, and Constitutional challenges to the wiretaps.

A. Law Enforcement Wiretaps are Subject to Standard Minimization Practices

In 1973, the Department of Health, Education, and Welfare (HEW) issued the report "Records, Computers, and the Rights of Citizens." This report recommended that Congress enact legislation adopting a Code of Fair Information Practice for automated personal data systems. U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973). The HEW report formed the basis for now universally recognized principles of Fair Information Practices. *See* Federal Trade Commission, Fair Information Practice Principles.[12] The concept of data minimization is inherent in the Fair Information Practices framework. Data minimization requires that governments and other entities collecting and accessing individuals' personal information do so in a way that limits access and storage to the minimum amount of data necessary to satisfy a given interest. Professor Spiros Simitis, while serving as the Data Protection Commissioner of the German state of Hesse, described this principle over 20 years ago:

---

[12] http://www.ftc.gov/reports/privacy3/fairinfo.shtm

> Personal information should only be processed for unequivocally specified purposes. Both government and private institutions should abstain from collecting and retrieving data merely for possible future uses for still unknown purposes. Both national and international organizations have in fact rejected the unlimited build-up of data files. In order to be retrieved, data must be necessary to a precise goal that is within the legally acknowledged activities of the organization interested in the information. A normative barrier thus prevents the technically possible multifunctional use of the data.

Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 740 (1987).

Security experts agree that the best way to prevent loss or misuse of sensitive personal information is to avoid gathering or storing it in the first place. Larry Dignan, *When it Comes to Data, Less is Better*, eWeek (May 3, 2005).[13] For example, in a proposed legal framework for government data mining, Professor Fred H. Cate suggests "[t]he use of data minimization and anonymization and other tools to limit the amount of information revealed to only what is necessary and authorized." Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 488 (2008). He goes further and suggests a number of tools and techniques so that "analysts

[13] http://www.eweek.com/c/a/Data-Storage/When-it-Comes-to-Data-Less-is-Better/.

can perform their jobs . . . without the need to gain access to personal data until they make the requisite showing for disclosure." *Id.* at 488–89.

If sensitive information must be stored and accessed, the principle of data minimization requires that the smallest possible amount of information to achieve the goal be accessed. In establishing law enforcement wiretap authority, Congress spoke directly to the problem of excessive information capture. Lawmakers established mandatory minimization requirements in Title III of the Omnibus Crime Control and Safe Streets Act. 18 U.S.C. § 2518(5) (2009). The statute requires that every order authorizing a wiretap contain provisions that the collection "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." *Id.*

This Court has spoken eloquently and directly to the Congressional intent of Title III:

> It should be clear by now that the problem of electronic surveillance strikes deep emotional chords in a people whose concern for the protection of privacy—particularly the privacy of words and thoughts—is historic. In Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Congress responded to this by balancing the needs of law

> enforcement against the important public and individual concern for privacy. It authorized electronic surveillance only under the most rigorous, carefully drawn standards. A cavalier, carefree and careless attitude towards the conduct of electronic surveillance makes a mockery of the labors of Congress to tailor the statute with precision. More importantly, it offends the spirit of liberty which has distinguished this nation from its birth.

United States v. Huss, 482 F.2d 38, 52 (2d Cir. 1973). The purpose of this requirement is to prevent indiscriminate seizure of communications and to prevent improper invasions of Americans' right to privacy.

The minimization requirements are especially important, because wiretaps are an extremely intrusive act in an area in which people have a strong expectation of privacy, an "interest of the highest order." *Bartnicki v. Vopper*, 532 U.S. 514, 545 (2001). Minimization is so important that failure to properly minimize can render the entire wiretap illegal and eligible for exclusion. *United States v. Tortorello*, 480 F.2d 764, 784 (2d Cir. 1973) ("It is clear . . . that a court should not admit evidence derived from an electronic surveillance order unless, after reviewing the monitoring log and hearing the testimony of the monitoring agents, it is left with the conviction that on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion.")

These minimization requirements have been a fundamental part of law enforcement wiretaps since the statute was written in the 1960s. Under the requirements, huge portions of recorded communications tend to be minimized and excluded from use. The portion of communications minimized often falls between 70% and 80% of communications subject to minimization requirements. *See, e.g.*, *United States v. Willis*, 890 F.2d 1099, 1102 (10th Cir. 1989) (". . . we are left with an approximate minimization effort of seventy per cent. We see nothing which indicates that these statistics are anything short of reasonable.") One court found that 25.6% minimization was sufficient, but the wiretapping in that case was an outlier. It involved only 84 calls subject to minimization—a dramatically smaller number than the 18,150 calls in present case. *United States v. Yarbrough*, 527 F.3d 1092, 1097–1099 (10th Cir. 2008).

B. Law Enforcement Wiretaps are Subject to Exclusion if They Violate Title III or the Fourth Amendment

Improper wiretaps are subject to a general exclusionary rule under the Fourth Amendment and also under Title III. 18 U.S.C. §§ 2515, 2518(10)(a) (2009). The Supreme Court has held that communications intercepted under an illegal wiretap order must be

suppressed, as well as any communications intercepted under a legal extension to that order, as derivative evidence. *United States v. Giordano*, 416 U.S. 505, 524–533 (1974).

Shortly after the Supreme Court established that suppression was a valid remedy to a violation of Title III's authorization requirements, this Court held that Title III's sealing and storage requirements are also of sufficient importance to merit suppression as a remedy. *United States v. Gigante*, 538 F.2d 502 (2d Cir. 1976). This Court also held that a trial court's error in denying a motion to suppress wiretap evidence for a violation of the authorization requirements was sufficiently prejudicial to merit reversal of a conviction. *United States v. Marion*, 535 F.2d 697 (2d Cir. 1976).

The principle of suppression for violations of Title III is still applied regularly in this Circuit. For example, in *United States v. Simels*, 2009 U.S. Dist. Lexis 56732 (E.D.N.Y. 2009), the district court upheld a motion to suppress wiretap evidence gained pursuant to an invalid authorization. In *United States v. Amanuel*, 418 F. Supp. 2d 244 (W.D.N.Y. 2005), the district court granted a motion to suppress wiretap evidence that was not properly sealed.

The rigid application of suppression remedies by the Supreme Court and this Circuit for violations of Title III and the Fourth Amendment is testament to the harm that arises from such violations.

C. Law Enforcement Wiretaps are Subject to Exclusion for Purposes of Relevance

In addition to exclusion under Title III and the Fourth Amendment, the contents of law enforcement wiretaps are subject to the Federal Rules of Evidence's relevancy requirements. "Evidence which is not relevant is not admissible." Fed. R. Evid. 402. Just as wiretap recordings are subject to pre-trial minimization when their contents are not related to the criminal investigation, a large percentage of them are either never introduced or excluded as irrelevant at trial.

The government's own statistics demonstrate that most wiretap recordings do not contain incriminating communications. In 2009, the government reported that only 19% of intercepted communications were incriminating, on average. 2009 Wiretap Report at 5. This percentage has been consistent over several years. In 2008, the rate of incriminating communications was 19%. In 2006, the rate was 20%. In

2005, the rate was 22%. In 2004, the rate was 21%. The highest rate came in 2007, at 30%. *See supra* notes 7 & 10 and accompanying text.

In addition to the government's own determination that a given intercepted communication is not relevant to an investigation, courts are required by Rule 402 to determine whether recordings that the government seeks to introduce as evidence meet the standard for relevance set forth in Fed. R. Evid. 401 ("'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.").

Under Rules 401 and 402, the court must determine relevance even before it applies the other rules of evidence. *See Janetka v. Dabe*, 892 F.2d 187, 191 (2d Cir. 1989); *see also Bonilla v. Jaronczyk*, 2009 U.S. App. LEXIS 26167 (2d. Cir. 2009), *Arlio v. Lively*, 474 F. 3d 46, 52–53 (2d Cir. 2007). In this case, the government has acknowledged that "[t]here are tons and tons of calls that at the end of the day when everybody has reviewed everything, every one of those calls isn't going to be played at this trial." Joint Appendix at A184.

III. The District Court's Decision is Contrary to Law and Violates the Privacy Interests of Individuals Whose Personal Communications are Completely Unrelated to the Investigation

As discussed above, government statistics indicate that hundreds of thousands of individuals are recorded on wiretaps every year. Approximately 80% of those personal communications are "not incriminating."[14] They are irrelevant to any alleged criminal activity. If we assume that incriminating communications are distributed evenly across all wiretapped communications and individuals, then 14,520 of the 18,150 intercepts in this case are irrelevant to alleged wrongdoing. And 440 of the more than 550 individuals recorded have nothing to do with the criminal investigation. Nationally, the projected statistics are even more staggering. In 2009 alone, 217,475 individuals' communications were wiretapped, yet had no relation to a crime.[15] Yet the District Court's order threatens to disclose these uninvolved individuals' personal communications.

---

[14] *Supra* note 11 and accompanying text.

[15] 268,488 wiretapped individuals less 19% who, assuming an even distribution, engaged in "incriminating" communications. *See supra* notes 9-11 and accompanying text.

As set forth in Appellants' Brief, The Wiretap Act prohibits disclosure of wiretapped communications "in all but a few instances." Appellants' Brief at 29 (*citing United States v. Marion*, 535 F.2d 697, 700 (2d Cir. 1976)). By ordering disclosure in the face of this prohibition, the District Court's decision in the present case poses a grave risk to individuals' privacy. It would expose more than 550 individuals' private communications to third parties through civil discovery before any court rules on the recordings' relevance, Constitutionality, or relation to criminal activity. Further, it could serve as precedent for even more widespread and damaging disclosures—exposure of the communications of hundreds of thousands of innocent, wiretapped individuals who are not charged with any crime, are not parties to any lawsuit, and are likely unaware that they were recorded.

Under the standard Title III paradigm, individuals' innocent communications are protected from disclosure. The Court will typically rule on a wiretap's Constitutionality, ensure that law enforcement agents minimized the amount of data recorded about innocent individuals and topics, and refuse to admit communications that are irrelevant to the criminal case. The District Court's ruling threatens to

eviscerate these privacy safeguards and improperly disclose sensitive, personal communications.

CONCLUSION

Amicus Curiae respectfully requests this Court to grant Appellants' motion to reverse the decision of the lower court.

Respectfully submitted,

/s/ Marc Rotenberg

MARC ROTENBERG
Counsel of Record
JOHN A. VERDI
JARED KAPROVE
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

April 30, 2010

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 3,161 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word 2007 in 14 point Century style.

Dated: April 30, 2010

/s/ John Verdi

MARC ROTENBERG
JOHN A. VERDI
JARED KAPROVE
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

ANTI-VIRUS CERTIFICATION

In the matter of *SEC v. Rajaratnam*, Docket No. 10-462-cv (L), I, John Verdi, certify that I used ZoneAlarm Anti-Virus 9.1.507.000, Scan Engine Version 8.0.2.48; Virus Definitions Version 1013548064 to scan for viruses the PDF version of the foregoing Brief of *Amicus Curiae* that was submitted in this case by electronic case filing. No viruses were detected.

Dated: April 30, 2010

/s/ John Verdi

MARC ROTENBERG
Counsel of Record
JOHN A. VERDI
JARED KAPROVE
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 30th day of April, 2010, the foregoing Brief of *Amicus Curiae* was electronically filed with the Clerk of the Court, and thereby electronically serve upon counsel for the parties *via* electronic delivery. In addition, six paper copies were shipped to the Clerk by U.S. Mail, postage prepaid, on May 3, 2010.

Dated: April 30, 2010

/s/ John Verdi

MARC ROTENBERG
JOHN A. VERDI
JARED KAPROVE
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-114