DISTRICT OF COLUMBIA
COURT OF APPEALS

No. 07-CV-000159

SOLERS, INC.,

Plaintiff-Appellant,

v.

JOHN DOE,

Defendant-Appellee,

and

SOFTWARE & INFORMATION INDUSTRY ASSOCIATION,

Intervenor-Appellee.

ON APPEAL FROM THE SUPERIOR COURT
OF THE DISTRICT OF COLUMBIA

BRIEF OF THE BUSINESS SOFTWARE ALLIANCE AS AMICUS CURIAE IN SUPPORT OF APPELLEES AND AFFIRMANCE

Robert A. Long, Jr.
Martin F. Hansen
Mark W. Mosier
Covington & Burling LLP
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2401
(202) 662-6000

Attorneys for Amicus Curiae
Business Software Alliance

September 26, 2007

CORPORATE DISCLOSURE STATEMENT

The Business Software Alliance is a non-profit association organized under the laws of the District of Columbia. It has no parent corporation and has issued no stock at least 10 percent of which is held by any publicly held corporation.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

INTEREST OF AMICUS CURIAE 1

SUMMARY OF ARGUMENT 3

ARGUMENT 5

I. THIS CASE IMPLICATES IMPORTANT FIRST AMENDMENT RIGHTS, INCLUDING RIGHTS OF SIIA AND ITS MEMBERS. 5

II. SIIA IS ENTITLED TO A QUALIFIED FIRST AMENDMENT PRIVILEGE BECAUSE COMPELLED DISCLOSURE OF THE SOURCE'S IDENTITY WOULD SEVERELY HARM ITS ENFORCEMENT PROGRAM 8

A. Software Piracy Poses A Serious Problem For The U.S. Economy. 8

B. SIIA Exercises Its First Amendment Rights in Seeking to Reduce Software Piracy 9

C. Private Enforcement of Copyright Laws Against Corporate End-User Pirates Depends on Information Provided by Sources Within the Corporation. 11

D. Individuals Are Less Likely To Expose Violators If They Believe Their Identities Will Be Disclosed And They Will Be Subjected To Retaliation 12

III. THE SUPERIOR COURT PROPERLY QUASHED THE THIRD-PARTY SUBPOENA BECAUSE SOLERS FAILED TO DEMONSTRATE A COMPELLING NEED TO OBTAIN DISCOVERY FROM SIIA. 14

CONCLUSION 16

TABLE OF AUTHORITIES

CASES

Management Information Tech., Inc. v. Alyeska Pipeline Serv., Co.,
151 F.R.D. 478 (D.D.C. 1993) 12

NAACP v. Alabama ex rel. Patterson,
357 U.S. 449 (1958) 5, 6

NAACP v. Button,
371 U.S. 415 (1963) 5, 6

In re Primus,
436 U.S. 412 (1978) 5, 6, 11

Rumsfeld v. Forum for Academic & Institutional Rights, Inc.,
547 U.S. 47 (2006) 5

**United States v. Garde*,
673 F. Supp. 604 (D.D.C. 1987) .... *passim*

STATUTES AND REGULATION

15 U.S.C. § 78j-1 13

17 U.S.C. § 501 10

17 U.S.C. § 502 10

17 U.S.C. § 504 10

18 U.S.C. § 1514A 13

26 C.F.R. § 301.7623-1 13

CONGRESSIONAL HEARINGS

Evaluating International Intellectual Property Piracy: Hearing Before the S. Comm. on Foreign Relations, 108th Cong. (2004) 2

Hearings Before the Subcomm. On Int'l Econ. Pol'y, Export and Trade Promotion of the Senate Comm. on Foreign Relations, 106th Cong. (1999) 10

Piracy of Intellectual Property: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary, 109th Cong. (2005) 2, 8, 9

OTHER SOURCES

2006 Roundup: BSA's Programs in Review, available at http://www.bsa.org 3

BSA and IDC Global Software Piracy Study 2006, available at http://www.bsa.org/globalstudy 8

BSA Raises the Stakes in Fight Against Software Piracy, available at http://www.bsa.org 2

Expanding the Frontiers of Our Digital Future: Reducing Software Piracy to Accelerate Global IT Benefits, available at http://w3.bsa.org/idcstudy/pdfs/White_Paper.pdf 9

James M. Sellers, Comment, *The Black Market and Intellectual Property: A Potential Sherman Act Section Two Antitrust Defense?*, 14 Albany L. J. Sci. & Tech. 583 (2004) 11

SIIA Anti-Piracy 2006 Year in Review, available at http://www.siia.net/piracy/yir_2006.pdf 9, 12

Smart About Software, available at http://www.smartaboutsoftware.org 2

Treasury Inspector General for Tax Administration, *The Informants' Rewards Program Needs More Centralized Management Oversight* (2006) 13

Blane Warrene, *The US Copyright Office's Rob Kasunic on Internet Law* (Feb. 8, 2005), available at http://www.macnewsworld.com/story/40268.html 10

INTEREST OF AMICUS CURIAE

The Business Software Alliance ("BSA") respectfully submits this brief as an *amicus curiae* supporting Intervenor-Appellee Software & Information Industry Association ("SIIA").[1]

BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. BSA's programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA's members include Adobe, Autodesk, Avid, Bentley Systems, Borland, CA, Cisco Systems, CNC Software/Mastercam, Dell, EMC, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, SAP, SolidWorks, Sybase, Symantec, The MathWorks, and UGS.

BSA and its members have a strong interest in reducing software piracy. BSA members suffer enormous financial losses from software piracy and other forms of copyright infringement. BSA seeks to reduce software piracy through education, policy, and enforcement programs. BSA develops and makes available to software users information and tools to increase public awareness of copyright laws, encourage legal use of legitimate software and explain the consequences of software piracy. The goal of these programs is to demonstrate to organizations and consumers the legal and practical risks associated with software piracy.

To raise public awareness of software piracy in the workplace, BSA recently partnered with the U.S. Small Business Administration to educate businesses on proper software management. As part of this program, BSA and the Small Business Administration created a

[1] SIIA and Plaintiff-Appellant Solers, Inc. have consented to the filing of this brief. SIIA has consented to extend the time for filing Solers's reply brief by one week.

joint website, which provides educational material on software piracy for small business owners. *See Smart About Software*, available at http://www.smartaboutsoftware.org. In addition, BSA recently launched an advertising campaign to encourage employees to report software piracy at their workplace. *See BSA Raises the Stakes in Fight Against Software Piracy* (July 2, 2007), available at http://www.bsa.org (follow "News & Events" hyperlink; then follow "Piracy News" hyperlink) ("BSA is launching 'Blow the Whistle,' a national advertising campaign that encourages employees to report software piracy.").

BSA is also involved in efforts to reduce software piracy through legislative reform. The President of BSA regularly testifies before congressional committees to discuss the economic impact of software piracy. *See Piracy of Intellectual Property: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 109th Cong. (2005); *Evaluating International Intellectual Property Piracy: Hearing Before the S. Comm. on Foreign Relations*, 108th Cong. (2004).

BSA and its members combat software piracy by taking legal action against software resellers and end-user organizations that make unauthorized copies of software. BSA files actions on behalf of its members under the civil enforcement provisions of federal copyright law. It also works closely with law enforcement agencies to coordinate enforcement of criminal copyright laws. BSA's enforcement program has been instrumental in bringing thousands of organizations that use software into compliance with copyright law, in closing down pirate Internet sites, and in stopping the illegal sale of pirated software through Internet auction sites and retail outlets. In 2006, BSA received over 2000 leads and successfully settled with 56 companies in North America. *See 2006 Roundup: BSA's Programs in Review* 4 (Apr. 24, 2007), available at http://www.bsa.org (follow "Research & Statistics" hyperlink; then follow "Research

Papers" hyperlink). All money collected from settlements is used to fund BSA's education, policy, and enforcement programs.

BSA has a substantial interest in the outcome of this appeal because the success of its enforcement program is largely dependent on leads provided by confidential sources. BSA, like SIIA, promises sources that their identities will not be disclosed unless required by law. The promise of confidentiality is important, because sources often are current or former employees of the pirating corporation and fear that the corporation will retaliate against them for reporting incidents of software piracy. Reversal of the Superior Court's order in this case would thus have an adverse effect on BSA's efforts to reduce software piracy.[2]

SUMMARY OF ARGUMENT

The third-party subpoena at issue in this case seeks to compel SIIA to disclose the identity of a confidential source. This subpoena implicates the First Amendment rights of SIIA and its members as well as those of the confidential source. An organization's First Amendment rights are burdened by a judicial order compelling it to reveal the identity of its members or others with whom it associates. This First Amendment protection extends to organizations that associate with whistleblowers, particularly when disclosure of the whistleblower's identity could subject that person to retaliation. Accordingly, organizations should not be forced to disclose the identity of a confidential source absent a showing that there is a compelling reason for such disclosure. Here, Solers has not come close to making such a showing.

[2] BSA has participated as an *amicus curiae* in other cases presenting issues of importance to BSA and its members, including *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

Software piracy is an extremely serious problem for copyright owners and the U.S. economy as a whole. SIIA and its members exercise their First Amendment rights by engaging in a wide variety of expressive activities intended to combat software piracy. These activities include civil actions to remedy copyright infringement by corporate end-user pirates. Such piracy is often difficult to detect, because it is often known only to individuals within the pirating corporation. In many cases, SIIA learns of corporate end-user piracy only through information provided by a confidential source with a connection to the pirating corporation. When these individuals are employees, they naturally are concerned that the corporation may retaliate against them, and thus their willingness to provide information often depends upon SIIA's ability to maintain their confidentiality. If a company can force SIIA to disclose a source's identity simply by filing a "John Doe" lawsuit and serving a third-party subpoena, SIIA's anti-piracy program will be severely harmed.

Solers failed to establish any compelling reason to require SIIA to disclose the identity of the confidential source in this case. The Superior Court found that Solers failed to show that it exhausted alternative methods of determining Doe's identity. In addition, Solers failed to show that it suffered a cognizable injury from the confidential communication between Doe and SIIA. Because a judicial order compelling disclosure of Doe's identity would infringe SIIA's First Amendment freedoms of speech and association, the Superior Court acted well within its broad discretion in quashing the third-party subpoena. The court's decision should be affirmed.

ARGUMENT

I. THIS CASE IMPLICATES IMPORTANT FIRST AMENDMENT RIGHTS, INCLUDING RIGHTS OF SIIA AND ITS MEMBERS.

SIIA's brief to this Court explains that the communication between Defendant-Appellee John Doe and SIIA implicates important First Amendment rights. These rights include the freedom of speech and the freedom of association of John Doe, SIIA, and its members. Solers's attempt to compel SIIA to disclose the identity of its source infringes upon these First Amendment interests.

The Supreme Court has long held that the First Amendment freedoms of speech and association apply to an organization's efforts to express its message. *See NAACP v. Button*, 371 U.S. 415, 428-29 (1963) ("[T]he activities of the NAACP, its affiliates and legal staff shown on this record are modes of expression and association protected by the First and Fourteenth Amendments."). The First Amendment applies whether the group's message concerns political or economic issues. *See NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958) ("[I]t is immaterial whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters."). These First Amendment rights extend to a group's efforts to advance its cause through litigation. *See In re Primus*, 436 U.S. 412, 426 (1978) ("Collective activity undertaken to obtain meaningful access to the courts is a fundamental right within the protection of the First Amendment.").[3]

---

[3] In discussing the First Amendment rights of an organization, courts do not always draw a sharp distinction between speech rights and associational rights. Often such a distinction is unnecessary. As the Supreme Court recently explained, these rights are intertwined because association facilitates speech. *See Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 68 (2006) ("The right to speak is often exercised most effectively by combining one's voice with the voices of others. If the government were free to restrict individuals' ability (continued…)

An organization's First Amendment rights are implicated by a judicial order compelling disclosure of the identities of individuals with whom it associates. In *Patterson*, the Supreme Court recognized that the NAACP's associational rights would be burdened if the organization were required to reveal its membership list. 357 U.S. at 462 ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association . . . ."). The Court concluded that compelled disclosure would create a risk of retaliation against NAACP members, which would make membership less appealing, thereby infringing on the freedom of association:

> [O]n past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility. Under these circumstances, we think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.

Id. at 462-463. Because the state had not shown a compelling interest in obtaining the membership list, the Court refused to order its disclosure. *Id.* at 464-65.

Subsequent decisions have extended associational rights beyond an organization's "rank-and-file members" to cover non-members who associate with the group for a limited purpose. In *Button*, the Supreme Court held that the NAACP's associational rights protected its staff lawyers in advising both members and non-members on whether to pursue litigation and directing them to particular lawyers. *See* 371 U.S. at 437; *see also Primus*, 436 U.S. at 425 n.16

---

to join together and speak, it could essentially silence views that the First Amendment is intended to protect.").

(noting that in *Button*, "recommendations were made even to nonmembers") (internal quotation marks omitted); *United States v. Garde*, 673 F. Supp. 604 (D.D.C. 1987) (an organization's associational rights extend to "members, agents, contributors, or recipients of contributions").

These First Amendment protections extend to organizations that express their message by associating with whistleblowers. *See United States v. Garde*, 673 F. Supp. 604 (D.D.C. 1987). In *Garde*, the Nuclear Regulatory Commission ("NRC") sought to compel the Governmental Accountability Project ("GAP") to reveal the identity of its confidential sources. GAP was a private organization that advocated on behalf of whistleblowers on safety-related issues at nuclear power projects. The court found that compelling GAP to disclose the identity of its confidential sources would burden its First Amendment rights. If identities are disclosed, the court explained, "GAP will lose the confidence of some of its whistleblower informants and its efforts to gather and present safety allegations will suffer. This is the harm that GAP claims, and it is cognizable under the right to association." *Id.* NRC failed to show a compelling interest in discovering the identity of the sources, because it had "not satisfied this Court that it has explored alternatives to the use of compulsory process to obtain the information sought." *Id.* The court concluded that "NRC cannot cast with such a wide net when constitutional freedoms are at stake. Alternatives minimizing the intrusion on associational rights must be carefully and conscientiously explored before resort may be had to the court's process." *Id.* (internal citations omitted).

In this case, as in *Garde*, the First Amendment concerns extend beyond John Doe's right to speak anonymously. Whether an organization should be compelled to disclose the identity of its confidential source implicates the organization's First Amendment rights of speech and association. Absent a compelling reason for disclosure, the First Amendment permits an

organization to maintain the confidentiality of a source when disclosure could subject the source to retaliation.

II. SIIA IS ENTITLED TO A QUALIFIED FIRST AMENDMENT PRIVILEGE BECAUSE COMPELLED DISCLOSURE OF THE SOURCE'S IDENTITY WOULD SEVERELY HARM ITS ENFORCEMENT PROGRAM.

A. Software Piracy Poses A Serious Problem For The U.S. Economy.

Software piracy is an enormous problem for both the U.S. and the global economy. Pirated software accounts for roughly 35 percent of all software used worldwide. *BSA and IDC Global Software Piracy Study 2006* 1, available at http://www.bsa.org/globalstudy. If the current piracy rate remains unchanged, the software industry will suffer revenue losses of approximately $180 billion between 2007 and 2010. *Id.* at 4. In the United States alone, losses from software piracy exceed $7 billion annually. *Id.* at 12.

Members of Congress have recognized the scope and severity of the threat posed by software piracy. *See, e.g., Piracy of Intellectual Property: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 109th Cong. (2005) (statement of Sen. Hatch) ("Piracy and counterfeiting inflict significant and widespread harms on the American economy. Theft of intellectual property abroad disadvantages this country's entrepreneurs, innovators, and creative community. Ultimately, it also harms consumers, shareholders, and American workers and their families."); *id.* (statement of Sen. Leahy) ("piracy has blossomed into a global problem as well, and because the United States is the world leader in intellectual property, we are – or at least we ought to be – acutely aware of its impact on U.S. industries and our citizens' own creativity and innovation.").

Reducing software piracy would have significant economic benefits for the global economy. According to one recent study, "IT [Information Technology] growth due to piracy reduction would help every country create more jobs for its workforce, create more opportunities for entrepreneurs, create more value for consumers and add more government services with an expanded tax base." *Expanding the Frontiers of Our Digital Future: Reducing Software Piracy to Accelerate Global IT Benefits* 6, available at http://w3.bsa.org/idcstudy/pdfs/White_Paper.pdf. A 10 percent drop in the global piracy rate would create an estimated 2.4 million jobs, generate $400 billion in economic output, and produce $67 billion in tax revenues over the next four years. *Id.* The United States would be the primary beneficiary, gaining almost 120,000 jobs, $124 billion in economic output, and $21 billion in taxes. *Id.* at 22.

B. SIIA Exercises Its First Amendment Rights in Seeking to Reduce Software Piracy.

To address the pressing problem of software piracy, SIIA engages in expressive activities protected by the First Amendment. SIIA is actively involved in efforts to reduce software piracy through legislative reform. *See SIIA Anti-Piracy 2006 Year in Review* 4, available at http://www.siia.net/piracy/yir_2006.pdf. (SIIA "advocates legislation that would increase and/or improve funding, personnel, training, enforcement powers and other government resources to combat piracy."). SIIA also "works with government officials and other industry stakeholders on activities to combat piracy of software." *Id.*

SIIA focuses much of its attention on reducing corporate end-user piracy. This form of piracy occurs when a corporation pirates software by making unauthorized copies for its own use. Corporate end-user piracy is the "business software industry's worst piracy problem." *Piracy of Intellectual Property: Hearing Before the Subcomm. on Intellectual Property of the S.*

Comm. on the Judiciary, 109th Cong. (2005) (testimony of Robert Holleyman, President and Chief Executive Officer, Business Software Alliance). One of the reasons that corporate end-user piracy is such a serious problem is that some violators do not view it as equivalent to other forms of theft. *See, e.g., Hearings Before the Subcomm. On Int'l Econ. Pol'y, Export and Trade Promotion of the Senate Comm. on Foreign Relations*, 106th Cong. (1999) (statement of Colleen Pouliot, Chair, Business Software Alliance Board of Directors) ("Most of us would never think of shoplifting a box of software from the store, yet many people do not think twice about copying a CD-ROM from a friend or making multiple copies of a program for use in their business. Software piracy of the kind I have just described, so-called 'end user' piracy, is theft."). SIIA works to change this perception by speaking out against corporate end-user piracy in an attempt to increase public awareness of the problem.

In addition to raising public awareness, SIIA seeks to curb corporate end-user piracy through private enforcement of the copyright laws. The United States has recognized the important role that private-sector enforcement of the U.S. copyright laws plays in reducing piracy. *See, e.g.*, Blane Warrene, *The US Copyright Office's Rob Kasunic on Internet Law* (Feb. 8, 2005), available at http://www.macnewsworld.com/story/40268.html (quoting the principal legal advisor to the U.S. Copyright Office as saying, "[w]hile there are some criminal and international trade sanctions for copyright infringement that can be brought by the U.S. government in appropriate circumstances, most enforcement of copyright infringement is the responsibility of copyright owners themselves.") Federal law creates a civil cause of action that permits a copyright holder to bring suit against an infringer, and expressly authorizes courts to enjoin further infringement and to award the copyright holder its actual damages or liquidated damages of up to $150,000. 17 U.S.C. §§ 501(b), 502, 504. Because copyright holders

generally enforce their copyrights through civil complaints, and government enforcement agencies rarely seek criminal charges in corporate end-user piracy cases, enforcement programs like SIIA's are particularly important. SIIA's efforts to reduce corporate end-user piracy through the legal process are entitled to First Amendment protection. *See Primus*, 436 U.S. at 431 (First Amendment protects an organization that "engages in litigation as a vehicle for effective political expression and association, as well as a means of communicating useful information to the public.").

C. Private Enforcement of Copyright Laws Against Corporate End-User Pirates Depends on Information Provided by Sources Within the Corporation.

Uncovering corporate end-user piracy is difficult because the illegal activity is often impossible for those outside the corporation to detect. Unlike software counterfeiting, in which the pirate must disclose its illegal activities to some extent in order to attract purchasers of the pirated goods, end-user piracy can occur without anyone but the pirate knowing of it. *See* James M. Sellers, Comment, *The Black Market and Intellectual Property: A Potential Sherman Act Section Two Antitrust Defense?*, 14 Albany L. J. Sci. & Tech. 583, 594 (2004) ("End-user piracy is the most pervasive form of piracy. The number of end-users of IP products, the ease of duplication and storage mediums (including the Internet), and the low probability of detection allows many end-users to personally pirate and not risk detection.").

SIIA takes action against organizations that make unauthorized copies of software. These copyright enforcement programs have been instrumental in bringing thousands of organizations into software compliance. SIIA reports that in 2006 it received 523 reports of alleged piracy; investigated 106 infringement claims and settled 49 such claims. *See SIIA Anti-Piracy 2006 Year in Review* 1, available at http://www.siia.net/piracy/yir_2006.pdf. SIIA's

enforcement program relies on individuals to report companies using pirated software. Without these leads, SIIA would often have no effective means to detect end-user piracy by corporations. Thus, the success of SIIA's enforcement program depends on the willingness of sources to alert it to end-user software pirating.

D. Individuals Are Less Likely To Expose Violators If They Believe Their Identities Will Be Disclosed And They Will Be Subjected To Retaliation.

Sources who report software piracy, like other whistleblowers, fear retaliation from pirating companies, which are often their current or former employers. As one court has explained:

> The case law, academic studies, and newspaper accounts well document the kind of treatment that is usually visited upon public and private employees who speak out as a matter of conscience on issues of public concern. For example, a six-year study on whistleblowers . . . details the full spectrum of management retaliation against ethical resistors who speak out against company or government policy and the long-term adverse consequences such employees can face. . . . The retaliation that occurs may not be so obvious as to involve the termination or transfer of whistleblowing employees but may nonetheless have negative impact on the whistleblowers' careers.

Mgmt. Info. Tech., Inc. v. Alyeska Pipeline Serv., Co., 151 F.R.D. 478, 481-83 (D.D.C. 1993) (internal citations omitted). Because of this threat, the court held that a party would not be required to identify its confidential sources "until the Court is satisfied that the sources will be adequately protected against retaliation." *Id.* at 481. *See also Garde*, 673 F.Supp. at 607 (unless an organization can promise to keep its sources confidential, it "will lose the confidence of some of its whistleblower informants and its efforts to gather and present [their] allegations will suffer").

Congress has also recognized that confidentiality is vital to the success of whistleblower programs. In enacting the Sarbanes-Oxley Act to address corporate accounting fraud, Congress acknowledged that encouraging confidential disclosures from employees was an important method for exposing accounting irregularities. The Act requires publicly traded companies to create procedures for whistleblowing. *See* 15 U.S.C. § 78j-1(m)(4)(b) (requiring the audit committee of a publicly traded corporation to "establish procedures for . . . the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters."). The Sarbanes-Oxley Act further protects whistleblowers through an anti-retaliation provision. 18 U.S.C. § 1514A.

Similarly, Congress has sought to encourage reporting of tax evasion by enacting a whistleblower program to supplement the auditing efforts of the IRS. To encourage sources to come forward, the IRS regulations protect a source's confidentiality. *See* 26 C.F.R. § 301.7623-1(e) ("No unauthorized person will be advised of the identity of an informant."). A recent report to Congress notes the success of this program: "[E]xaminations initiated based on informant information were often more effective and efficient than returns initiated using the IRS' primary method for selecting returns for examination." Treasury Inspector General for Tax Administration, *The Informants' Rewards Program Needs More Centralized Management Oversight* 1-2 (2006).

Unlike the government, a private organization such as SIIA has no authority to prohibit corporations from retaliating against sources who report software piracy. Thus, SIIA places even more reliance than government agencies on their ability to protect the confidentiality of their sources. SIIA promises its sources that their identities will not be revealed unless required by law. Because maintaining a source's confidentiality is essential to an enforcement

program's success, SIIA's associational rights would be impaired if it were required to reveal a source's identity. The First Amendment therefore permits SIIA to keep Doe's identity confidential unless the court finds a compelling reason for disclosure. *Garde*, 673 F. Supp. at 605.

III. THE SUPERIOR COURT PROPERLY QUASHED THE THIRD-PARTY SUBPOENA BECAUSE SOLERS FAILED TO DEMONSTRATE A COMPELLING NEED TO OBTAIN DISCOVERY FROM SIIA.

The third-party subpoena at issue in this case poses a threat to SIIA's First Amendment rights. SIIA seeks to reduce software piracy – a matter of serious public concern – through public education, legislative reform, and civil actions seeking to enforce federal copyright law. SIIA's anti-piracy campaign involves the exercise of rights of speech and association that are protected by the First Amendment. In particular, a critical component of SIIA's anti-piracy program is its association with confidential sources for the purpose of obtaining information about software piracy. SIIA uses the information it receives from confidential sources to pursue enforcement of copyright law. If SIIA is unable to protect the confidentiality of its sources, its associational rights will be harmed because sources will be less likely to associate with SIIA for the purpose of providing it with information. *See Garde*, 673 F. Supp. at 605. Consequently, SIIA should be required to disclose the source's identity only upon a showing of compelling need for disclosure. *Id.* The Superior Court correctly held that Solers made no such showing in this case.[4]

---

[4] Because Solers did not come close to making a compelling showing of need, the Superior Court would have acted within its discretion in quashing the subpoena even if a less demanding standard, such as "substantial need," applied to this case.

Solers failed to establish a compelling need for SIIA to disclose the source's identity for two reasons. *First*, Solers failed to demonstrate that SIIA is the only possible source for the information it seeks. When First Amendment rights are implicated, an order to compel disclosure should be the last option, not the first. *Id.* ("Alternatives minimizing the intrusion on associational rights must be carefully and conscientiously explored before resort may be had to the court's process."). The Superior Court found that "Solers has failed to demonstrate that it exhausted alternative methods of obtaining Doe's identity," and that "Solers could have searched other computer records besides the email server or it could have interviewed current and former employees." Solers does not challenge these factual findings, which are sufficient to affirm the Superior Court's decision to quash the subpoena.

Second, even if Solers had shown that SIIA was the only source for the information it is seeking, it still would have failed to demonstrate a compelling need for disclosure. Solers cannot claim that John Doe harmed its reputation by publicly accusing the company of software piracy in a newspaper Internet posting. Nor can Solers claim that it was injured by accusations John Doe made to Solers's customers or other business partners, because John Doe made no such accusations. Instead, John Doe communicated only with SIIA. SIIA, in turn, did not publicly accuse Solers of software piracy; it communicated only with Solers. These carefully limited communications cannot be said to have caused cognizable harm to Solers. As the Superior Court found, "[e]ven if Solers only had to demonstrate harm to its reputation regardless of lost profit, it has not done so." App. 26.

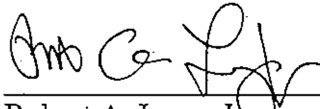
At a minimum, Solers has failed to demonstrate that its need for disclosure of the source's identity overcomes the interests of SIIA, its source, and society at large in preserving the source's confidentiality. As explained in Part II above, confidential sources frequently are

essential to detecting corporate end-user piracy, and sources facing a threat of retaliation frequently are unwilling to provide information without a promise of confidentiality. Compelling SIIA to disclose John Doe's identity would not allow Solers to remedy harm to its reputation, because Solers has suffered no harm. Compelled disclosure would, however, chill communications between SIIA and confidential sources, thus infringing rights of speech and association protected by the First Amendment.

CONCLUSION

For the foregoing reasons, as well as those stated in SIIA's brief, the Superior Court's decision should be affirmed.

Respectfully submitted,



Robert A. Long, Jr.
Martin F. Hansen
Mark W. Mosier
Covington & Burling LLP
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2401
(202) 662-6000

Attorneys for Amicus Curiae
Business Software Alliance

September 26, 2007

CERTIFICATE OF SERVICE

I hereby certify that on September 26, 2007, I served the brief of the Business Software Alliance as *amicus curiae* by sending one copy of the brief by Federal Express (overnight delivery) to each of the following:

Daniel J. Tobin
Ballard Spahr Andrews & Ingersoll, LLP
4800 Montgomery Lane, 7th Floor
Bethesda, MD 20814-3401

Attorney for Plaintiff-Appellant Solers, Inc.

Charles D. Tobin
Leo G. Rydzewski
Holland & Knight LLP
2099 Pennsylvania Ave., NW, #100
Washington, DC 20006

Attorneys for Intervenor-Appellee Software & Information Industry Association

Mark W. Mosier