IN THE COURT OF APPEAL
OF THE STATE OF CALIFORNIA
SIXTH APPELLATE DISTRICT

JASON D. O'GRADY, MONISH BHATIA AND KASPER JADE, *Petitioners and Appellants*, vs. SUPERIOR COURT OF THE STATE OF CALIFORNIA, COUNTY OF SANTA CLARA, *Respondents* APPLE COMPUTER, INC. *Real Party in Interest*.	No. H028579 Santa Clara County Superior Court Trial Court Case No. 1-04-CV-032178 The Hon. James Kleinberg

REQUEST OF UNITED STATES INTERNET INDUSTRY ASSOCIATION AND NETCOALITION FOR LEAVE TO FILE BRIEF AS AMICUS CURIAE IN SUPPORT OF NON-PARTY JOURNALISTS' PETITION FOR A WRIT OF MANDATE OR PROHIBITION; AND

BRIEF OF UNITED STATES INTERNET INDUSTRY ASSOCIATION AND NETCOALITION AS AMICI CURIAE IN SUPPORT OF NON-PARTY JOURNALISTS' PETITION FOR A WRIT OF MANDATE OR PROHIBITION

Counsel of Record:
Elizabeth H. Rader (SBN 184963)
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto, CA 94303

Attorneys for Amici Curiae
United States Internet Industry
Association and NetCoalition

TABLE OF CONTENTS

TABLE OF AUTHORITIES……ii

APPLICATION FOR LEAVE TO FILE BRIEF AMICUS CURIAE IN SUPPORT OF THE ISSUANCE OF A WRIT OF MANDATE OR PROHIBITION……1

INTRODUCTION AND SUMMARY OF THE ARGUMENT……..4

ARGUMENT……...6

I. **THE TRIAL COURT FAILED TO ACCOUNT FOR THE PROHIBITIONS THE SCA IMPOSES ON ELECTRONIC COMMUNICATION SERVICE PROVIDERS**……....6

A. **The SCA Prohibits ECS Providers from Disclosing the Contents of Stored Communications to Private Parties**……..6

B. **The SCA's Limited Exceptions Do Not Permit the Disclosure of Stored Emails in this Case**……...7

C. **The SCA Reflects a Congressional Choice to Treat "Contents" and Other Consumer Information Differently**……...12

II. **THE COURT'S RULING DISCOUNTS IMPORTANT FIRST AMENDMENT GUARANTEES WITHOUT SUFFICIENT REGARD FOR THE DISCOVERY ORDER'S CHILLING EFFECT ON PROTECTED SPEECH**……14

III. **THE TRIAL COURT'S RULING UNIFORMLY COMPROMISES EMAIL USER PRIVACY AND IMPOSES SUBSTANTIAL BURDENS ON INTERNET SERVICE PROVIDERS**……17

CONCLUSION…..……..19

TABLE OF AUTHORITIES

FEDERAL CASES

Ameritech Corp. v. McCann,
297 F.3d 582 (7th Cir. 2002) 9
Bartnicki v. Vopper,
532 U.S. 514 (2001) 15
Brainsick v. Vosper,
532 U.S. 514 (2001) 4
In re Charter Communications, Inc., Subpoena Enforcement Matter,
393 F.3d 771 (8th Cir. 2005) 2
Columbia Ins. Co. v. Seescandy.com,
185 F.R.D. 573 (N.D. Cal. 1999) 14, 15, 16
Curtis v. United States,
511 U.S. 485 (1994) 13
Doe v. 2TheMart.com Inc.,
140 F. Supp. 2d 1088 (W.D. Wa. 2001) 14
Doe v. Ashcroft,
334 F. Supp. 2d 471 (S.D.N.Y. 2004) 9, 15
Federal Trade Comm'n v. Netscape Communications Corp.,
196 F.R.D. 559 (N.D. Cal. 2000) 10
Freedman v. Am. Online, Inc.,
325 F. Supp. 2d 638 (E.D. Va. 2004) 11
Hall v. Earthlink Network, Inc.,
396 F.3d 500 (2d Cir. 2005) 6
Jarecki v. G. D. Searle & Co.,
367 U.S. 303 (1961) 11
Jessup-Morgan v. America Online, Inc.,
20 F. Supp. 2d 1105 (E.D. Mich. 1998) 12
Katz v. United States,
389 U.S. 347 (1967) 15
Los Angeles Memorial Coliseum Comm. v. Nat'l Football League,
89 F.R.D. 489 (C.D. Cal. 1981) 14
McIntyre v. Ohio Elections Comm'n,
514 U.S. 334 (1995) 14
Mink v. Salazar,
344 F. Supp. 2d 1231 (D. Colo. 2004) 10
NAACP v. Alabama ex rel. Patterson,
357 U.S. 449, 461 (1958) 14
New York Times v. Sullivan,
376 U.S. 254 (1964) 14

Recording Industry Ass'n of America, Inc. v. Verizon Internet Servs., Inc.,
351 F.3d 1229 (D.C. Cir. 2003) 2
Reno v. ACLU
521 U.S. 844 (1997) 1, 15
Robinson v. Shell Oil Co.,
519 U.S. 337 (1997) 11
Shelley v. Kraemer,
334 U.S. 1 (1948) 14
Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004) 2, 6, 8
United States v. American Trucking Assn., Inc.,
310 U.S. 534 (1940) 13
United States v. Dauray,
215 F.3d 257 (2d Cir. 2000) 10
United States v. Morton,
467 U.S. 822 (1984) 11

STATE CASES

Kobzoff v. Los Angeles County Harbor/UCLA Med. Ctr.,
19 Cal. 4th 851 (1998) 11

STATUTES

17 U.S.C. § 512(m) 5
18 U.S.C. § 2510 10
18 U.S.C. § 2510(15) 6
18 U.S.C. § 2510(8) 6
18 U.S.C. § 2511(1) 10
18 U.S.C. § 2511(2) 10
18 U.S.C. § 2511(2)(a) 7
18 U.S.C. § 2511(2)(a)(i) 5
18 U.S.C. § 2517 7
18 U.S.C. § 2520 10
18 U.S.C. § 2701 ..... 2, 4
18 U.S.C. § 2702 2
18 U.S.C. § 2702(a)(1) 6, 12
18 U.S.C. § 2702(a)(2) 12
18 U.S.C. § 2702(b) 5, 7
18 U.S.C. § 2702(b)(2) 7
18 U.S.C. § 2702(b)(3) 7, 8
18 U.S.C. § 2702(b)(4) 7

18 U.S.C. § 2702(b)(5) 7
18 U.S.C. § 2702(b)(6) 7
18 U.S.C. § 2702(b)(7)(A) 7
18 U.S.C. § 2702(c)(6) 12
18 U.S.C. § 2703 ..... 7, 8
18 U.S.C. § 2703(b) 12
18 U.S.C. § 2703(b)(1)(B) 12
18 U.S.C. § 2703(c) 9
18 U.S.C. § 2703(c) 9
18 U.S.C. § 2703(d) 12
18 U.S.C. § 2703(e) 9
18 U.S.C. § 2703(f) 9
18 U.S.C. § 2705 12
18 U.S.C. § 2707 9
18 U.S.C. § 2707(a) 8
18 U.S.C. § 2707(e) 9, 10
18 U.S.C. § 2711(1) 6
18 U.S.C.§ 2703(a) 12
18 U.S.C.§ 2703(c)(1)(C) 10

FEDERAL RULES OF CIVIL PROCEDURE

Fed. R. Civ. Proc. 45 10

CALIFORNIA RULES OF COURT

Rule 13(c) 1

SECONDARY SOURCES

Joan Steinman, *Privacy of Association:A Burgeoning Privilege in Civil Discovery*, 17 HARV. C.R.-C.L. L. REV. 355 (1982) 14

Kent D. Stuckey, INTERNET AND ONLINE LAW (1996) § 5.03[1][a][ii] 7, 8

LEGISLATIVE MATERIALS

S. Rep. No. 99-541 (1986) 6

APPLICATION FOR LEAVE TO FILE BRIEF AMICUS CURIAE IN SUPPORT OF THE ISSUANCE OF A WRIT OF MANDATE OR PROHIBITION

TO THE HONORABLE PRESIDING JUSTICE, SIXTH DISTRICT COURT OF APPEAL, DIVISION:

Pursuant to California Rule of Court 13, subdivision (c), amici curiae United States Internet Industry Association ("USIIA") and NetCoalition respectfully request leave to file the accompanying brief amicus curiae in support of the petition of Jason O'Grady, Monish Bhatia and Kasper Jade for a permanent writ of mandate and/or prohibition directing the Superior Court to vacate its order denying petitioners' protective order and to issue a new order preventing enforcement of subpoenas against the non-party journalists or their communications service providers, including Nfox.com, Inc.

Amicus USIIA is a trade association with more than 200 members who provide the facilities and services that constitute the Internet as we know it today. USIIA members include Internet Service Providers ("ISPs"), who provide proprietary content, email capability, and web browsing functionalities to their subscribers. Many of USIIA's members transmit and store electronic communications that are protected by the First Amendment, the Fourth Amendment, and federal statutes from disclosure to third parties. Subscriber confidence in the security and privacy of their electronic communications is central to USIIA's mission and central to the success of the Internet as an effective medium of social, political, economic, and cultural exchange. *See Reno v. ACLU*, 521 U.S. 844, 863 (1997).

USIIA President David P. McClure, a prominent Internet industry spokesperson, has testified before Congress on numerous occasions

regarding the intersection of Internet privacy and intellectual property. USIIA has participated in numerous federal and state court cases raising issues of ISP duties and subscriber privacy in the context of third-party discovery requests. *See, e.g., In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005); *Recording Industry Ass'n of America, Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003).

NetCoalition is a Washington, DC trade association that represents some of the world's most innovative Internet companies, including ISPs, search engines, portals and hosting companies. NetCoalition provides creative and effective solutions to the critical legal and technological issues facing the Internet. By enabling technology industry leaders, policymakers, and the public to engage directly in the consideration of these issues, NetCoalition has helped to ensure the integrity, usefulness and continued expansion of this dynamic medium.

Amici are particularly concerned with the burden that subpoenas for email content place on third-party ISPs in the discovery process. ISPs are not and should not be converted into "Internet policemen." They do not monitor their subscribers' private electronic communications or web browsing behaviors. Although their servers store the contents of private electronic communications, the First Amendment, the Fourth Amendment and, most importantly, federal statutes forbid access to stored electronic communications except in the most exigent of circumstances.

Crucially, the Electronic Communications Privacy Act of 1986 ("ECPA"), *codified at* 18 U.S.C. § 2701, *et seq*. forbids any electronic communications services ("ECS") provider from disclosing the contents of stored communications. *Id*. § 2702. An overbroad or otherwise invalid

civil subpoena or discovery order can violate the protections for stored communications contained in the ECPA. *See, e.g., Theofel v. Farey-Jones*, 359 F.3d 1066, 1073-75 (9th Cir. 2004).

Nevertheless, the trial court's opinion rejecting the motion for protective order completely fails to consider the limitations federal law places on disclosure of stored electronic communications to third parties. For these reasons, amici respectfully request that this Court grant them leave to file the attached brief *amicus curiae* in this proceeding. Amici submit that this Court should issue a writ of mandate or prohibition forbidding Apple from executing this overbroad, unlawful, and unconstitutional discovery request that the trial court sanctioned without adequate consideration of its conflict with the prohibitions contained in the ECPA and the protections afforded under the First Amendment.

April 8, 2005

Respectfully submitted

Elizabeth H. Rader (SBN 184963)
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto CA, 94303

Attorneys for Amici Curiae
United States Internet Industry
Association and NetCoalition

INTRODUCTION AND SUMMARY OF ARGUMENT

This writ proceeding raises several critical issues of law regarding the privacy of individual and otherwise confidential communication and association through the Internet. Over 100 million Americans use the Internet each day, sending and receiving personal and business emails, participating in chat rooms and news groups, purchasing items of every sort, and consulting web pages of every kind – from those containing medical advice (e.g., <www.webmd.com>) – to those fostering political views and association (e.g., <www.trueblueliberal.com>). The right to send and receive content over the Internet and associate electronically in a manner of one's choosing, without having one's identity and private communications revealed to third parties, is at the core of the protections of the First Amendment.

Those protections are as, or perhaps even more important, when private parties seek to use the judicial power to compel disclosure of anonymous speakers and the content of their speech. *See Brainsick v. Vosper*, 532 U.S. 514, 533 (2001). Because Nfox, the ISP that provided email service for Petitioner Jason O'Grady, did not object to the subpoena or participate in the motion for a protective order, *see* March 11, 2005 Order at 3 (Appendix Exhibit 34, p. NPJ00457) ("Trial Court Order"), the trial court was denied the critical perspective of the service provider in this discovery dispute.

This case involves attempted discovery of the most private and sensitive aspects of electronic communications – the full content and distribution information of Petitioner O'Grady's stored electronic communications. Yet the federal Stored Communications Act ("SCA"),

part of the ECPA, codified at 18 U.S.C. §§ 2701-11, categorically forbids disclosure of the email content sought in this case. Under the SCA, ECS providers must not disclose the contents of stored communications, such as stored email, unless expressly permitted by law. The narrow exceptions to the SCA, which principally apply to disclosure to the government in a criminal investigation or a showing of "immediate danger of death or serious physical injury to any person," do not apply to the civil discovery requests at issue here. *See* 18 U.S.C. § 2702(b) (listing limited exceptions to broad prohibition on disclosure of stored electronic communications).

These protections are critical to ISPs and their ability to provide safe, reliable, and secure communications channels to their subscribers. Congress has repeatedly affirmed that ISPs should not be placed in the position of "big brother" monitoring or scouring through private electronic communications for the benefit of civil litigants. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(i) (prohibiting random ISP checks or observation of email content except for mechanical or service quality control purposes); 17 U.S.C. § 512(m) (ISPs have no duty to monitor the contents of their subscribers' communications for potential copyright violations).

Because the trial court completely overlooked the federal statutory prohibitions and First Amendment privacy protections that the discovery requests implicate, and because those federal laws prohibit Nfox from undertaking the very conduct that the Apple discovery request would require, this Court should issue a permanent writ of mandate or prohibition in this matter.

ARGUMENT

I. THE TRIAL COURT FAILED TO ACCOUNT FOR THE PROHIBITIONS THE SCA IMPOSES ON ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

A. The SCA Prohibits ECS Providers from Disclosing the Contents of Stored Communications to Private Parties.

The SCA imposes a number of obligations on an ECS provider such as Nfox.[1] Foremost, the SCA mandates that a "person or entity providing an electronic communication service to the public shall not knowingly divulge to *any* person or entity the *contents* of a communication while in electronic storage by that service[.]" 18 U.S.C. § 2702(a)(1) (emphasis added); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.").[2] The "contents" of an electronic communication, under the SCA, "includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The trial court's discovery order, which requires Fox to "knowingly divulge . . . the contents" of stored electronic communications squarely conflicts with the SCA's general prohibition.

---

[1] There is no question that Nfox is an ECS provider within the meaning of the SCA. *See* 18 U.S.C. § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); 18 U.S.C. § 2711(1) (generally providing that the definitions in 18 U.S.C. § 2510 apply to the SCA); *see also Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 504 n.2 (2d Cir. 2005) ("It is not disputed that ISPs are a type of electronic communication service provider."); O'Grady Decl. ¶ 23 (Appendix, Exhibit 18, p. NPJ00131:6-7).

[2] Congress passed the SCA to prohibit an ECS provider "from knowingly divulging the contents of any communication while in electronic storage by that service to any person other then the addressee or intended recipient." S. Rep. No. 99-541, 97th Cong. 2nd Sess. 37, 1986 U.S.C.C.A.N. 3555, 3591.

B. The SCA's Limited Exceptions Do Not Permit the Disclosure of Stored Emails in this Case.

The SCA, pursuant to § 2702(b), provides for certain limited exceptions to this general prohibition against knowingly divulging stored electronic communications. The statutory exceptions fall into three general categories. *See* Kent D. Stuckey, INTERNET AND ONLINE LAW § 5.03[1][a][ii] (1996). The first category includes disclosures that are authorized by either the sender or the receiver of the communication.[3] The second category permits disclosures necessary to maintain the efficient system operations.[4] The third category is strictly limited to disclosures to a governmental entity. *Id.*[5] "All other disclosures – including disclosures to a third party subpoena in civil litigation – are prohibited." *Id.*

[3] *See* 18 U.S.C. § 2702(b)(1) (authorizing disclosures "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient"); 18 U.S.C. § 2702(b)(3) (authorizing disclosure "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service").

[4] *See* 18 U.S.C. § 2702(b)(4) (authorizing disclosures "to a person employed or authorized or whose facilities are used to forward such communication to its destination"); 18 U.S.C. § 2702(b)(5) (authorizing disclosures "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service").

[5] *See* 18 U.S.C. § 2702(b)(2) (authorizing disclosures "as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title"); 18 U.S.C. § 2517 (authorizing disclosure by a law enforcement officer for investigative purposes); 18 U.S.C. § 2511(2)(a) (exceptions to ban on interception of electronic communications); 18 U.S.C. § 2703 (listing circumstances under which disclosure to a government entity is required); 18 U.S.C. § 2702(b)(6) (authorizing disclosures "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990"); 18 U.S.C. § 2702(b)(7)(A) (authorizing disclosures "to a law enforcement agency . . . if the contents . . . (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime"); 18 U.S.C. § 2702(b)(2) (authorizing disclosures "to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency").

Apple's civil discovery request does not fall within any of these statutory exceptions. Neither Petitioner O'Grady nor any of his correspondents have "authorized" Nfox to disclose the contents of their communications, to Apple or any other private third-party litigants. Furthermore, both Apple and Nfox are aware of Petitioners' writ request and the SCA prohibitions outlined therein. If Nfox were to now authorize disclosure without O'Grady's consent based on Apple's faulty subpoena, both Nfox and Apple could face SCA liability for accessing those electronic communications. *See* 18 U.S.C. § 2707(a) (authorizing civil action against private parties for SCA violations); *see also Theofel*, 359 F.3d at 1073 ("Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances"); Stuckey, INTERNET AND ONLINE LAW § 5.03[1][a][ii] ("Although the [SCA] allows "authorized" access to stored communications, analogy to trespass law can limit the scope of an authorization and support liability where the plaintiff was mistaken as to the nature and quality of the invasion intended."). Neither O'Grady nor any other anonymous Nfox subscriber could have foreseen the nature and quality of Apple's invasion into their protected email content. The invasion is thus unauthorized under section 2702(b)(3).

Apple's request also does not qualify for any of the relevant law enforcement exceptions. In particular, any reliance on section 2703 is entirely misplaced.[6] Section 2703(c) permits disclosure of content under

[6] **(c) Records concerning electronic communication service or remote computing service – (1)** *A governmental entity* may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such

certain circumstances – but only *to the government*. *See Ameritech Corp. v. McCann*, 297 F.3d 582, 583-584 (7th Cir. 2002) (section 2703 "sets forth the requirements for *government access* to private communications and [that] electronic communications providers . . . shall furnish certain electronic records to governmental entities *only under specific circumstances*.") (emphasis added); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 487 (S.D.N.Y. 2004) (the ECPA "sets forth an intricate framework by which electronic communications providers, such as ISPs and phone companies, may be compelled to disclose stored electronic information *to the Government*.") (emphasis added). Section 2703(e) , which provides for a defense to civil liability where the ISP made the disclosure "in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter," is also of no aid. Section 2703(e) is

---

> service (not including the contents of communications) only when the governmental entity –
>
> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
>
> **(B)** obtains a court order for such disclosure under subsection (d) of this section;
>
> **(C)** has the consent of the subscriber or customer to such disclosure; or;
>
> **(D)** submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
>
> **(E)** seeks information under paragraph (2).

18 U.S.C. § 2703(c) (emphasis added).

strictly limited to compliance "under this chapter" – which by definition excludes civil discovery requests made by private litigants.

Last, Apple cannot rely on section 2707's good-faith defense to support its otherwise unsustainable position. Section 2707(e) provides that reliance on a "court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f))" constitutes a good-faith defense to a civil action brought by an aggrieved subscriber. 18 U.S.C. § 2707(e). Apple mistakenly contends that a defense to a civil action somehow provides a lawful basis for the brand of civil discovery at issue here. It plainly does not.

First, a defense to a civil action initiated by an aggrieved subscriber cannot be converted into a positive grant of authority for Apple to obtain Petitioner O'Grady's federally protected stored electronic communications. A comparison to the SCA's legislative sibling, the Wiretap Act, makes this point clear. Section 2707 mirrors section 2520, which applies the same good-faith exception to the "interception" of electronic communications under the Wiretap Act, codified at 18 U.S.C. § 2510, *et seq*. *See* 18 U.S.C. § 2520; *see also* 18 U.S.C. § 2511(1) (prohibiting the "interception" of electronic communications). It would strain credibility to contend that the Wiretap Act allows private parties engaged in civil litigation to "intercept" electronic communications for the purpose of civil discovery. *See* 18 U.S.C. § 2511(2) (listing exceptions to the prohibition against "intercepting" electronic communications). Nevertheless, Apple's reliance on the "court order" language of the section 2707 good-faith exception as a positive grant of authority to obtain stored electronic communications would necessarily apply equally to the interception of these same electronic

communications. *See Mink v. Salazar*, 344 F. Supp. 2d 1231, 1239 (D. Colo. 2004) ("the only difference between 'intercept,' as that term is used in the Wire Tape[sic] Act, and 'access,' as that term is used in Section 2701 of the ECPA, is temporal; interception is acquisition simultaneous with transmission while access is acquisition of material already stored.") Such a reading would turn the statutory language on its head. *See United States v. Dauray*, 215 F.3d 257, 264 (2d Cir. 2000) ("A statute should be interpreted in a way that avoids absurd results.").

Second, section 2707's reference to "court order or warrant" was intended by Congress to apply to either a court order or warrant in a criminal action or, perhaps, a court order in a government-initiated civil action.[7] *See* 18 U.S.C. § 2707(e); *see also Jarecki v. G. D. Searle & Co.*, 367 U.S. 303, 307 (1961) ("The maxim *noscitur a sociis*, that a word is known by the company it keeps, while not an inescapable rule, is often wisely applied where a word is capable of many meanings in order to avoid the giving of unintended breadth to the Acts of Congress.") Apple's efforts to isolate "court order" from the surrounding language and context should

[7] It remains doubtful that even the government proceeding in a civil action can obtain subscriber information, let alone email content, through a discovery subpoena. *See Federal Trade Comm'n v. Netscape Communications Corp.*, 196 F.R.D. 559, 560-61 (N.D. Cal. 2000). There, the FTC sought subscriber information through a discovery subpoena issued pursuant to Federal Rule of Civil Procedure 45. The FTC argued that a discovery subpoena qualified as a "trial subpoena" under section 2703(c)(1)(C). The court rejected this argument because "[t]o decide otherwise would effectively allow the FTC to use Rule 45 to circumvent the precautions and protections built into the ECPA to protect subscriber privacy from governmental entities." *Id.* at 561. "*There [was] no reason for the court to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to.*" *Id.* (emphasis added). Importantly, the court did not look to section 2707's good-faith exception as a source of authority to permit the divulgence of ECPA-protected information during civil discovery.

be rejected. *See United States v. Morton*, 467 U.S. 822, 828 (1984) ("We do not . . . construe statutory phrases in isolation; we read statutes as a whole.").

Consequently, the SCA, by its terms, forbids ISPs from divulging the contents of users' emails unless the request satisfies one of the discrete statutory exceptions to this general rule. Here, the limited exceptions do not permit ECS providers to divulge the contents of electronic communications pursuant to civil discovery order for the benefit of a private litigant. The Court's inquiry can therefore proceed no further. *See Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997) (the "inquiry must cease if the statutory language is unambiguous"); *Kobzoff v. Los Angeles County Harbor/UCLA Med. Ctr.*, 19 Cal. 4th 851, 861 (1998) ("If the plain language of a statute is unambiguous, no court need, or should, go beyond that pure expression of legislative intent.").

C. The SCA Reflects a Congressional Choice to Treat "Contents" and Other Consumer Information Differently.

The SCA reflects a congressional choice to afford superior protection for electronic communication content. The SCA distinguishes between content and other subscriber information. *See Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638, 644 n.3 (E.D. Va. 2004) ("The discussion in this Memorandum Opinion focuses solely on the disclosure of plaintiff's subscriber record and information and not the contents of his communications). An ISP's disclosure of the contents of a subscriber's communications is subject to different rules set forth in §§ 2702(a)(1)-(2) and 2703(a)-(b)."); *see also In re United States for an Order Pursuant to 18 U.S.C. 2703(d)*, 36 F. Supp. 2d 430, 432 (D. Mass. 1999) and *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich.

1998) (noting differing treatment of communications content and non-content subscriber records). The SCA thus provides for the disclosure of some subscriber information – other than content – to private parties. *See* 18 U.S.C. § 2702(c)(6) ("A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) – to any person other than a governmental entity."). As already discussed, however, the statute does not authorize disclosure of content to private parties.

Furthermore, the SCA's scheme for ECS provider disclosure of stored communications content to governmental entities includes a general requirement that – absent a search – warrant subscribers must receive notice and opportunity to challenge disclosure requests, reflects the congressional concern for Internet privacy. *See* 18 U.S.C. § 2703(a) (contents stored for 180 days or less may only be obtained via a search warrant); 18 U.S.C. § 2703(b)(1)(B) (contents stored for more than 180 days may be obtained via either a search warrant or a governmental subpoena "with prior notice to the subscriber or customer."); 18 U.S.C. § 2705 (detailing "delayed notice" procedures). There is no comparable provision for notice to subscribers of non-government civil subpoenas for the content of their communications, however – not because Congress disregarded it, but because it was unnecessary considering the statute's lack of allowance for such subpoenas. If Apple wishes to obtain Petitioner O'Grady's emails, its only option under the SCA is to subpoena him directly. Such a subpoena to O'Grady would provide the notice that Congress was so concerned about while allowing him to timely assert any applicable privileges or shields.

In the end, had Congress intended to permit litigants to obtain email contents directly from ISPs via civil discovery, "it knew how to do so." *Curtis v. United States*, 511 U.S. 485, 492 (1994). Congress took no such action. The differing treatment afforded stored communication content and subscriber information evinces Congress's desire to provide the former greater protection. The discovery subpoena, which seeks civil discovery of email content for the benefit of a private litigant, violates this unmistakable congressional directive. *See United States v. American Trucking Assn., Inc.*, 310 U.S. 534, 542-545 (1940) ("In the interpretation of statutes, the function of the courts is easily stated. It is to construe the language so as to give effect to the intent of Congress.").

II. THE COURT'S RULING DISCOUNTS IMPORTANT FIRST AMENDMENT GUARANTEES WITHOUT SUFFICIENT REGARD FOR THE DISCOVERY ORDER'S CHILLING EFFECT ON PROTECTED SPEECH.

Apple's subpoena to Nfox would further violate the anonymity of other Internet subscribers in violation of their First Amendment rights. The First Amendment guarantees the right to free speech and freedom of association. U.S. CONST. AMEND. I.[8] Importantly, the First Amendment protects the right to speak and associate anonymously. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) ("Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent

[8] "A court order, even when issued at the request of a private party in a civil lawsuit, constitutes state action and as such is subject to constitutional limitations." *Doe v. 2TheMart.com*, 140 F. Supp. 2d 1088, 1091-92 (W.D. Wa. 2001) (citing *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964)); *Shelley v. Kraemer*, 334 U.S. 1 (1948)); *see also NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 461 (1958); *Los Angeles Memorial Coliseum Comm'n v. Nat'l Football League*, 89 F.R.D. 489 (C.D. Cal. 1981).

practice, but an honorable tradition of advocacy and dissent. Anonymity is a shield from the tyranny of the majority."); *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) ("[W]e acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself."); *see also* Joan Steinman, *Privacy of Association: A Burgeoning Privilege in Civil Discovery*, 17 HARV. C.R.-C.L. L. REV. 355, 375 (1982) ("The need to protect associational privacy is no less powerful in litigation.").

This fundamental right to anonymity applies with equal force to speech via the Internet. *See Reno v. ACLU*, 521 U.S. 844, 870 (1997) ("Through the use of Web pages, mail exploders and newsgroups, [any person] can become a pamphleteer."); *2TheMart.com Inc.*, 140 F. Supp. 2d at 1092 ("Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas."); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (The "ability to speak one's mind" on the Internet "without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate.").[9]

---

[9] As one court explained:

> A person who signs onto an anonymous forum under a pseudonym, for example, is essentially 'shut[ting] the door behind him,' . . . and is surely entitled to a reasonable expectation that his speech, whatever form the expression assumes, will not be accessible to the Government to be broadcast to the world absent appropriate legal process. To hold otherwise would ignore the role of the internet as a remarkably powerful forum for private communication and association.

Doe v. Ashcroft, 334 F. Supp. 2d 471, 510 (S.D.N.Y. 2004) (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967)).

Accordingly, "[i]f Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights." *2TheMart.com*, 140 F. Supp. 2d at 1093.[10]

Civil discovery requests seeking to unmask anonymous Internet users "are subjected to careful scrutiny by the courts." *See id*. at 1093 ("[N]on-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker."). Thus, even where a discovery request seeks only the identity of an anonymous Internet user, a far more focused request than the sweeping demand for email content at issue here, courts must undertake a rigorous inquiry before granting the discovery request. *See, e.g.*, *Seescandy.com*, 185 F.R.D. at 578-79; *2TheMart.com*, 140 F. Supp. 2d at 1095. In *Seescandy.com*, for example, the court required that the party seeking discovery of subscriber identities must (1) identify the individual with some specificity; (2) identify the past actions taken to uncover this information through less intrusive means; (3) establish that the case would withstand a motion to dismiss; and (4) justify the need for the information. *Id*.

The trial court failed to even engage in this review – let alone the more demanding First Amendment inquiry that would be required to sustain a request for email content.[11] Instead, the trial court gave short

[10] Indeed, the prospect of a subpoena for O'Grady's email has already had a chilling effect on his email correspondents. (O'Grady Supp. Decl., ¶¶ 2-4 (Appendix, Exhibit 31, NPJ00429:1-14).

[11] Apple's contention that its discovery requests seek information limited to potential defendants is inaccurate. The request is, in fact, quite broad and

shrift to the important First Amendment questions at issue, primarily relying on California's "strong commitment to the protection of proprietary business information" as the basis for its decision.[12] *See* Trial Court Order at 6 (Appendix, Exhibit 34, p. NPJ00460:10-11). The trial court's failure to take account of the factors necessary to resolve this important First Amendment question and engage in the requisite inquiry is reason alone to reject its decision.

III. THE TRIAL COURT'S RULING UNIFORMLY COMPROMISES EMAIL USER PRIVACY AND IMPOSES SUBSTANTIAL BURDENS ON INTERNET SERVICE PROVIDERS.

Amici believe strongly in protecting their members' customers' privacy to the maximum extent consistent with the needs of ongoing law enforcement investigations or the threat of terrorism. *See, e.g.*, http://www.usiia.org/legis/dataret.html ("Internet service providers are subject to subscriber agreements, contracts and laws related to the privacy rights of their subscribers, as well as more general Constitutional and legal rights with regard to protection of data. These rights cannot in principle be violated without a court order to do so for each individual subscriber without substantial liability risk to the Internet service provider.").

In its effort to protect customer privacy, the USIIA adopted a uniform practice of objecting to private civil subpoenas that seek customer

---

will capture protected content well beyond any potential wrongdoing. In reality, the request is a fishing expedition that is not targeted at specific individuals; instead, the request seeks to obtain the content of emails that is otherwise shielded from discovery under federal law. The discovery request at issue thus blatantly fails the First Amendment inquiry.

[12] The trial court did examine the First Amendment question with respect to Mr. O'Grady's journalistic privilege argument in greater detail. The question of journalistic privilege, however, raises fundamentally different concerns than the right of a private speaker to remain anonymous.

information from Internet Service Providers. The USIIA has relied on the ECPA to support these objections. Through its consistent and diligent efforts, the USIIA seeks to preserve the general, overarching privacy of personal subscriber information and has ensured that parties seeking customer data, including email content, must satisfy the stringent requirements of the statute.

Indeed, amici are troubled by the possibility that non-party Nfox may have already been induced to violate the SCA by informing Apple that the word "Asteroid" appeared in petitioner's stored communications. (Appendix, Exhibit 20, p. NPJ00242:16-22).

As a policy matter, upholding the trial court's ruling would not only harm email users' privacy but also impose significant additional burdens on ECS providers. Amici's members already receive many subpoenas from private parties for non-content information such as subscriber identity and billing records. These non-content subpoenas intrude upon subscribers' privacy and are costly to process. Requiring ECS providers to provide content information would expose far more and far more sensitive information to private parties, raising serious liability concerns for providers and privacy concerns for subscribers.

In addition, selectively gathering the contents of emails or other electronic communications and securely storing and delivering them in response to private-party subpoenas would disrupt normal business operations and require additional physical and electronic storage space as well as employee time and effort. Such uncompensated costs would threaten the industry's financial health. Congress recognized this financial reality by providing that ECS providers shall be reimbursed for the costs of providing communications contents and other data to the government. 18

U.S.C. § 2706. Such reimbursement costs include both the direct costs of "searching for, assembling, reproducing, or otherwise providing such information" and "any costs due to necessary disruption of normal operations." 18 U.S.C. § 2706 (a). Yet there is no provision for reimbursement for complying with civil subpoenas for non-government litigants, for the simple reason that such subpoenas are not allowed under the statute.

CONCLUSION

The SCA was intended to protect the privacy of the contents of ordinary people's stored electronic communications, while allowing government access to those contents under a carefully crafted statutory scheme of subpoenas, court orders, and search warrants. Nothing in the SCA, however, allows private parties like Apple to gain unconsented access to users' stored communications directly from ECS providers. Rather, the plain text and structure of the SCA compels the conclusion that Congress neither created nor intended to create any "civil litigant" disclosure provision. Furthermore, the trial court failed to consider the First Amendment implications of its decision with respect to the anonymous email content of private individuals.

For all of these reasons, Amici respectfully request that this honorable Court reverse the judgment of the trial court and remand with instructions that the trial court grant the relief prayed for by Appellants.

April 8, 2005

Respectfully submitted

Counsel of Record:
Elizabeth H. Rader (SBN 184963)
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto CA, 94303

Attorneys for Amici Curiae
United States Internet Industry
Association and NetCoalition

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that the attached brief complies with the form, size and length requirements of Cal. R. App. Pro. 14(b) and (c) because it was prepared in a proportionally spaced type using Word 10 in Times Roman 13-point font double spaced and contains 6,827 words, excluding the portions of the brief exempted by Cal. R. App. Pro. 14(c)

Counsel of Record:
Elizabeth H. Rader (SBN 184963)
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto CA, 94303

Attorneys for Amici Curiae
United States Internet Industry
Association and NetCoalition

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 8th day of April, 2005 I caused an original and four copies of the foregoing brief to be manually filed with the clerk of the Court of Appeals. I also caused a copy to be mailed via First-Class Mail to the following recipients, four copies to be mailed to the clerk of the Supreme Court and one copy mailed to the clerk of the Superior Court in compliance with Cal. R. App. Pro. 40.1 (a) , and Cal. R. App. Pro. 44(b)(2):

Thomas Moore III
Tomlinson Zisko LLP
200 Page Mill Road, 2nd Floor
Palo Alto, CA 94306

George A. Riley, Esq.
David A. Eberhart, Esq.
O'Melveny & Myers LLP
Embarcadero Center West
275 Battery Street
San Francisco, CA 94111

Kurt B. Opsahl
Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Attorneys for Real party in Interest Apple Computer Inc.

Richard R. Weibe
425 California Street, Suite 2025
San Francisco, CA 94104

Nfox.com, Inc.
C/o Charles F. Catania
3187 East Rochelle Avenue
Las Vegas, NV 89121

Attorneys for Petitioners Jason O'Grady, Monish Bhatia and Kasper Jade

Registered Agent for Nfox.com, Inc.

Counsel of Record:
Elizabeth H. Rader (SBN 184963)
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto CA, 94303

Attorneys for Amici Curiae
United States Internet Industry
Association and NetCoalition