Richard R. Wiebe (SBN 121156)
Law Office of Richard R. Wiebe
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382
wiebe@pacbell.net

Attorney for Amicus Curiae
Center For Democracy and Technology

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ALBERTO R. GONZALES, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES,

Movant,

v.

GOOGLE INC.,

Respondent.

Case No. CV 06-80006 MISC JW

AMICUS BRIEF OF

CENTER FOR DEMOCRACY & TECHNOLOGY

IN SUPPORT OF GOOGLE'S OPPOSITION TO THE MOTION TO COMPEL OF ATTORNEY GENERAL GONZALES

DATE: March 13, 2006
TIME: 9:00 a.m.
COURTROOM: 8, 4th Floor

The Hon. James Ware

TABLE OF CONTENTS

INTEREST OF AMICUS 1

ARGUMENT 2

I. The Electronic Communications Privacy Act Prohibits Disclosure Of The User Data The Government Seeks 2

A. The Electronic Communications Privacy Act 2

B. Google Is A "Remote Computing Service" Covered By ECPA With Respect To The Search Terms Created And Transmitted By Users For Further Processing By Google 3

C. The Search Terms That A Google User Transmits To Google Are The "Contents Of A Communication" Under ECPA 5

D. Because Google Is A Remote Computing Service, The Government Cannot Use A Civil Subpoena To Obtain The Content Of Search Terms Created And Transmitted By Users For Further Processing By Google 6

II. The Global Nature Of The Internet And The Global Nature Of Google's Search Results Render The Subpoenaed Information Irrelevant To The COPA Litigation 11

CONCLUSION 13

TABLE OF AUTHORITIES

Cases

American Civil Liberties Union v. Reno, 31 F.Supp.2d 473 (E.D. Pa. 1999) 13
Ashcroft v. ACLU, 542 U.S. 656 (2004) 12
Crowley v. Cybersource Corp., 166 F.Supp.2d 1263 (N.D. Cal. 2001) 5
Custis v. United States, 511 U.S. 485 (1994) 11
Federal Trade Comm'n v. Netscape Communications Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) 10
Freedman v. America Online, Inc., 303 F.Supp.2d 121 (D. Conn. 2004) 2, 11
Freedman v. America Online, Inc., 325 F.Supp.2d 638 (E.D. Va. 2004) 2
In re JetBlue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005) 5
In re United States for an Order Authorizing the Use of a Pen Register & Trap, 396 F.Supp.2d 45 (D. Mass. 2005) 6
Rodriguez v. United States, 480 U.S. 522 (1987) 11
Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) 7

Statutes

18 U.S.C. § 2510 ..... 3, 6
18 U.S.C. § 2702 ..... 7, 8, 11
18 U.S.C. § 2703 ..... 8, 10, 11
18 U.S.C. § 2711 3

Other Authorities

H.R. Rep. No. 99-647 (1986) 3
Prepared Statement of P. Michael Nugent, "Electronic Communications Privacy Act," Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary, 99th Cong., 1st and 2nd Sess, Serial No. 50 (1985-86) 4
S. Rep. No. 99-541, *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555 3

Amicus curiae the Center for Democracy & Technology respectfully submits this brief to assist the Court in resolving the novel and significant issues posed by this proceeding. In particular, this brief addresses issues under the federal Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 to 2712, that are squarely raised by this proceeding but that the parties have incompletely addressed.

INTEREST OF AMICUS

The Center for Democracy & Technology ("CDT") works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies.

CDT has been at the forefront of Internet free speech cases for as long as there have been such cases. CDT organized one of the two constitutional challenges that were consolidated in the landmark Supreme Court decision in *Reno v. ACLU*, 521 U.S. 844 (1997), striking down the Communications Decency Act. CDT has also been a leader in the effort to promote the use of filtering technology by parents and others to protect children online, because filtering technology is by far the most effective way to protect kids online, and because such technology offers a less restrictive alternative to governmental attempts to directly burden lawful speech online. *See* Berman and Weitzner, "Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media," 104 Yale L.J. 1619 (1995). CDT President Jerry Berman served as a Commissioner on the Child Online Protection Act ("COPA") Commission, an expert panel created by Congress in COPA to address how best to protect children online. Over the lengthy course of the litigation over COPA that underlies this matter, CDT has participated in five amicus briefs before the district court, the court of appeals, and the Supreme Court.

ARGUMENT

I. The Electronic Communications Privacy Act Prohibits Disclosure Of The User Data The Government Seeks

A. The Electronic Communications Privacy Act

The Attorney General's motion to compel production of search term data that users transmit to Google to be processed into search results must be denied. The plain language of the federal Electronic Communications Privacy Act prohibits government entities from obtaining, and prohibits Google from disclosing, the contents of its users' communications except pursuant to certain specified forms of compulsory process, which do not include civil pretrial discovery subpoenas.

Congress enacted the Electronic Communications Privacy Act ("ECPA"), codified at 18 U.S.C. §§ 2510 to 2712, to protect the privacy of electronic data and communications transmitted by users of electronic communication systems like the Internet. "Congress enacted the ECPA in 1986 to protect against the interception and disclosure of information related to electronic communications. The Act's paramount objective is to protect the privacy of persons in connection with the use of electronic and wire communications." *Freedman v. America Online, Inc*., 325 F.Supp.2d 638, 643 (E.D. Va. 2004).

ECPA was a groundbreaking statute. To achieve its goal of protecting privacy, Congress strictly limited the conditions under which electronic data and communications may be disclosed to the government and others. In particular, EPCA establishes clear and strict procedures for governmental access. *See Freedman v. America Online, Inc*., 303 F.Supp.2d 121, 127 (D. Conn. 2004) ("Congress designed such procedures to both (1) protect personal privacy against unwarranted government searches and (2) preserve the legitimate needs of law enforcement.").

While ECPA is a complex and multifaceted statute, on the narrow issue before the court, it provides a clear and straightforward answer: The government cannot obtain the user information its seeks from Google by means of a civil pretrial discovery subpoena.

B. Google Is A "Remote Computing Service" Covered By ECPA With Respect To The Search Terms Created And Transmitted By Users For Further Processing By Google

EPCA's protections against disclosure encompass two types of entities providing services related to electronic communications systems: "Remote computing services" ("RCS") providers and "electronic communication service" ("ECS") providers.

A " 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711, subd. (2). (Hereafter, all statutory references are to 18 U.S.C. unless otherwise noted.) An " 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." § 2510, subd. (15).

It is the limitations on disclosure by an RCS provider that will be of relevance here, because Google is an RCS provider. The RCS provisions of ECPA were drafted to cover companies like Electronic Data Systems Corporation (EDS), which received data from their customers by electronic transmission, processed that data, and then sent the results of that processed and transformed data back to the customer with added value. The RCS provisions of ECPA were intended to protect and foster the earliest forms of data processing "outsourcing." See S. Rep. No. 99-541 at 10-11 (describing RCS as data processing "accomplished by the service provider on the basis of information supplied by the subscriber or customer"), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3564-65; H.R. Rep. No. 99-647, at 23 (1986) (discussing the definition of an RCS). At the hearings leading up to enactment of ECPA, the government affairs counsel of EDS testified as to the need to extend clear privacy protection not only to communications in transit but also to data held by remote processing companies performing services like Google's: "There are other examples of remote computer services which involve electronic transmission of customer data to and from the venders [sic] computer center. These include interactive data services. Such interactive services includes [sic] (1) remote access

to databases . . . (3) inquiry/response activities between customer terminals and central computer locations . . . ." Prepared Statement of P. Michael Nugent, "Electronic Communications Privacy Act," Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary, 99th Cong., 1st and 2nd Sess., Serial No. 50 (1985-86) at 77-78.

Google is a provider of a "remote computing service." It serves as an outsourcer of search functions for its users. Internet users could, with considerable effort, maintain their own lists of URLs and send out their own robots or spiders to scour the Web looking for what they want. Instead, Google has taken on that processing function for users, via remote electronic transmission. Users transmit certain data—their search terms—to Google by means of electronic communications. Google takes that data and processes it with its proprietary data processing techniques and returns the results of that data processing—a list of search results—to the user.

A user outsourcing search to Google is no different than a company outsourcing its payroll operations to a data processing company like EDS. In each case, the user provides input data to the company, the company then processes the data and provides the value-added results of that data processing to the user. Users could build their own search engines to crawl the web, just as a company could do its own payroll in-house, but entities like Google have sprung up to do that data processing at a remote point. Transmitting input data by means of an electronic communications systems like the Internet to a remote processor and receiving in return the old data together with new and useful data derived from it is the very definition of an RCS, and that is what Google does. Declaration of Matthew Cutts at ¶ 6; Google Opposition at 20. And, as explained above, in EPCA Congress recognized the importance of protecting the privacy of a user's data when it is transmitted for remote processing from disclosure to the government.

In this respect, Google's processing of user data and retransmittal to the user of the transformed results is quite different than e-commerce websites like Jetblue.com or

Amazon.com. In those cases, the user is not sending its data to be transformed and returned as new, different, and useful data, but is sending data to procure a service (a flight on an airplane) or a product (a book) quite separate from the processing of the data. The incidental transformations the e-commerce company makes to the data the user inputs (e.g., by triggering a command to the warehouse to ship a book, or a command to the credit card company to debit an account) are not transmitted back to the user but are retained and used by the e-commerce company for its own purposes. *Cf. In re JetBlue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299, 310 (E.D.N.Y. 2005) ("Plaintiffs have also failed to establish that JetBlue is a remote computing service."); *Crowley v. Cybersource Corp.*, 166 F.Supp.2d 1263, 1270 (N.D. Cal. 2001) ("Therefore, for Amazon to be liable for improper disclosure of electronic communications under the ECPA, it must provide either electronic communication service or remote computing service. The amended complaint makes clear that it does neither.").

C. The Search Terms That A Google User Transmits To Google Are The "Contents Of A Communication" Under ECPA

The search terms that a Google user transmits to Google are the "contents of a communication." EPCA defines an "electronic communication" very broadly: " 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature." § 2510, subd. (12). It defines the "contents" of a communication equally broadly: " 'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." § 2510, subd. (8).

Under these statutory definitions, there can be no doubt that the search terms a user transmits to Google to be processed into search results are the contents of a communication. The search terms have intelligible "substance," "purport," and "meaning," and they are electronically communicated as a transfer of "signs," "writing," and "data." The user transmits those contents to Google, which processes them using its proprietary

techniques and returns the search terms back to the user with additional valuable information whose content is determined by the search terms.

Indeed, at least one district court has already held that Google search terms are "content" within the meaning of ECPA. "A user may visit the Google site. . . . [I]f the user then enters a search phrase, ... [t]his would reveal content—that is, it would reveal, in the words of the statute, '. . . information concerning the substance, purport or meaning of that communication.' Title18 U.S.C. § 2510 (8). The 'substance' and 'meaning' of the communication is that the user is conducting a search for information on a particular topic." *In re United States for an Order Authorizing the Use of a Pen Register & Trap*, 396 F.Supp.2d 45, 49 (D. Mass. 2005).

D. Because Google Is A Remote Computing Service, The Government Cannot Use A Civil Subpoena To Obtain The Content Of Search Terms Created And Transmitted By Users For Further Processing By Google

In the case of either an RCS or an ECS, subdivision (a) of section 2702 creates a general prohibition against disclosures by the service provider of the contents of user communications.[1] With respect to an RCS, subdivision (a)(2) provides:

> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the *contents of any communication* which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not

[1] The portion of ECPA at issue here that limits disclosure of communications after transmission by the user is completed, 18 U.S.C. §§ 2701 to 2712, is also sometimes referred to as the "Stored Communications Act," or "SCA." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004).

> authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing;

§ 2702 (a)(2) (emphasis added). Thus, an RCS provider cannot disclose to a governmental entity the contents of customer communications except as otherwise expressly authorized by ECPA.

Subdivision (b) of section 2702 then sets forth exceptions to the prohibitions of subdivision (a)(2) against disclosure by an RCS of the contents of communication. Subdivision (b) has seven exceptions permitting disclosure of "the contents of a communication," all but one of which are clearly inapplicable here.[2] The only one that merits further discussion is subdivision (b)(2), which authorizes an RCS provider to disclose the "contents of a communication" "as otherwise authorized in section 2517,

---

[2] Subdivision (b) of section 2702 sets forth seven exceptions:

> (b) Exceptions for disclosure of communications.—A provider described in subsection (a) may divulge the contents of a communication—
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
> (2) *as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title*;
> (3) 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) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
> (5) 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;
> (6) to a law enforcement agency—
> (A) if the contents—
> (i) were inadvertently obtained by the service provider; and
> (ii) appear to pertain to the commission of a crime; or
> (B) if required by section 227 of the Crime Control Act of 1990; or
> (7) 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.

§ 2702, subd. (b) (emphasis added).

2511(2)(a), or 2703 of this title." Sections 2517 and 2511(2)(a) address criminal and foreign intelligence investigations and incidental disclosures in the course of operating an electronic communication service, none of which is present here, leaving the analysis at section 2703.

Thus, disclosure to the government of the information protected under section 2702 is permissible here only if it is authorized by section 2703. Turning to section 2703, subdivision (b) establishes the requirements the government must meet to compel disclosure of the "contents" of communications held by an RCS provider:

> (b) Contents of wire or electronic communications in a remote computing service.
>
> (1) A governmental entity may require a provider of remote computing service to disclose the *contents of any wire or electronic communication* to which this paragraph is made applicable by paragraph (2) of this subsection—
>
> (A) without required notice to the subscriber or customer, if the governmental entity 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; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> (i) uses an *administrative subpoena* authorized by a Federal or State statute or a Federal or State *grand jury or trial subpoena*; or
>
> (ii) obtains a *court order* for such disclosure *under subsection (d)* of this section;
>
> except that delayed notice may be given pursuant to section 2705 of this title.
>
> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

§ 2703(b) (emphasis added).

Thus, under subdivision (b) of section 2703, the government may only compel an RCS to disclose the contents of a communication by one of five specified means: 1) a criminal search warrant; 2) an administrative subpoena; 3) a grand jury subpoena; 4) a trial subpoena; or 5) a court order issued under subdivision (d) of section 2703 (subdivision (d) orders can issue only on a showing that the information sought is "relevant and material to an ongoing criminal investigation," § 2703(d), and thus are not relevant here).

Here, the government has not sought to use any of the five methods authorized by subdivision (b) of section 2703 to compel disclosure by Google. A civil pretrial discovery subpoena under Rule 45 of the Federal Rule of Civil Procedure, the process the government seeks to use in this proceeding, is not an authorized means of compelling disclosure under section 2703, as Judge Patel of this Court has held: "There is no reason for the court to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to. [¶] To decide otherwise would effectively allow the [government] to use Rule 45 to circumvent the precautions and protections built into the ECPA to protect subscriber privacy from government entities. The court cannot believe that Congress intended the phrase 'trial subpoena' to apply to discovery subpoenas in civil cases, thus permitting government entities to make an end-run around the statute's protections through the use of a Rule 45 subpoena." *Federal Trade Comm'n v. Netscape*

Communications Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) (citations omitted) (construing a former version of section 2703(c) with operative language parallel to the current version of section 2703(b)); *accord*, *Freedman v. America Online, Inc*., 303 F.Supp.2d at 127 ("The ECPA imposes an obligation on governmental entities to follow specific legal processes when seeking such information.").[3]

Had Congress intended instead to permit the government to use civil pretrial discovery subpoenas to compel RCS providers to disclose the contents of communications, "it knew how to do so." *Custis v. United States*, 511 U.S. 485, 492 (1994). Congress specifically identified administrative, grand jury, and trial subpoenas as methods by which the government might seek disclosure, but pointedly refused to authorize civil pretrial discovery subpoenas as an additional method. This Court need look no further, because "where the language of a provision is sufficiently clear in its context, there is no occasion to examine the additional considerations of policy . . . that may have influenced the lawmakers in their formulation of the statute." *Rodriguez v. United States*, 480 U.S. 522, 526 (1987).

Accordingly, because section 2702 forbids disclosure absent an exception, and because section 2703 does not authorize the government to seek disclosure by means of civil pretrial discovery subpoenas, the Attorney General's motion to compel must be denied.[4]

---

[3] Even if the search terms transmitted by the user to Google were not the "contents of a communication," it would not avail the Attorney General. In addition to protecting the contents of communications, EPCA also prohibits the unauthorized disclosure by an RCS of "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . .)." § 2702(a)(3). The government may not obtain customer records from an RCS by a civil pretrial discovery subpoena, but only by the same five methods as are set forth in subdivision (b) of section 2703 for obtaining the contents of communications, plus a telemarketing fraud exception not relevant here. §2703(c); *see also* § 2702(c).

[4] Although other companies with search engines reportedly have complied in good faith with similar subpoenas from the Attorney General, the understandable fact of their innocent but

II. The Global Nature Of The Internet And The Global Nature Of Google's Search Results Render The Subpoenaed Information Irrelevant To The COPA Litigation

Although CDT submits this amicus brief principally to address the application of ECPA to this case, CDT believes that it is ultimately not necessary for the Court to reach the ECPA issue, because, as Google correctly argues, the subpoena is not seeking information that is likely to lead to relevant information and should be denied on that basis alone. The relevance argument has been extensively briefed by Google; CDT, however, wishes to note one fact not highlighted in Google's brief: the government's subpoena to Google suffers from the same flaw found in the COPA statute itself—both ignore the global nature of the Internet.

For jurisdictional reasons, COPA is necessarily territorial in effect—it can regulate only content created and hosted inside the United States. "COPA does not prevent minors from having access to those foreign harmful materials." *Ashcroft v. ACLU*, 542 U.S. 656, 667 (2004). The Internet, however, is a global communications medium. The search terms in Google's database come from all over the world and seek information from websites all over the world. Google's "bots" and other techniques index websites globally. Thus, reviewing a random worldwide selection of search terms and URLs from Google will not lead to any valid conclusions about websites with sexual content that are hosted in the United States—the only websites that as a practical matter COPA can reach.

Similarly, Google's users are spread around the entire world. Thus, analyzing a snapshot of search terms entered will not lead to any valid conclusions about how minors

---

mistaken compliance with a superficially lawful subpoena does nothing to bolster the meritlessness of the Attorney General's legal position. That companies that receive subpoenas from the government routinely comply with even broad requests for information further demonstrates why the government must be required to show a sufficiently specific reason for demanding the information and why it must comply with the statutorily mandated procedures of ECPA. As explained in Google's brief and in the underlying plaintiffs' brief, the Attorney General has failed to make an adequate showing of relevance. As explained in this brief, under ECPA the civil pretrial discovery subpoena served by the Attorney General is not an authorized method for compelling disclosure in any event.

in the United States—the class of people that COPA is intended to protect—gain access to sexual content or what sexual content might be available to them.

More broadly, as with the COPA statute itself, the government's subpoena totally ignores the fact that COPA will have no significant impact on online sexual content outside of the United States. The global nature of the Internet—and more particularly of sexual content on the Internet—make very clear that the COPA statute is wholly ineffective at protecting minors located in the United States.

The importance of the global nature of the Internet was made clear by the original district court decision in the underlying COPA litigation. There, the court found that minors could access sexual content on foreign web sites, and that this was one of the "problems [COPA] has with efficaciously meeting its goal." *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 496 (E.D. Pa. 1999). A subsequent study by the National Academy of Sciences released in 2002 confirms the importance of the fact that a majority of sexual content is hosted overseas.[5]

The National Academy determined that approximately three-quarters of the commercial sites offering sexually explicit material are located outside the United States. *See Nat'l Acad. of Sciences*, at 4. This enormous number of sexually explicit sites outside of the United States means that COPA will be ineffectual in protecting minors from sexual content on the Internet. Simply put, even if COPA somehow made all U.S.-based sites completely inaccessible to minors, minors would still have innumerable foreign sexual sites available to them. The National Academy report speaks bluntly about the significance

[5] *See* Nat'l Research Council of the Nat'l Academy of Sciences, "Youth, Pornography, and the Internet" (2002). The full report is also available online in HTML format at http://books.nap.edu/html/youth_internet/ and in PDF format at http://books.nap.edu/books/0309082749/html/index.html. The study was undertaken at the behest of Congress, Pub. L. No. 105-314, Title IX, § 901, 112 Stat. 2991 (1998), and looked at "computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet."

of sexual content on foreign websites on the likely effectiveness of COPA in furthering a governmental interest:

> For jurisdictional reasons, federal legislation cannot readily govern Web sites outside the United States, even though they are accessible within the United States. Because a substantial percentage of sexually explicit Web sites exist outside the United States, *even the strict enforcement of COPA will likely have only a marginal effect on the availability of such material on the Internet in the United States.* Thus, even if the Supreme Court upholds COPA, COPA is not a panacea, illustrating the real limitations of policy and legal approaches to this issue. The committee also notes that, even if COPA is constitutional, this does not necessarily mean it is good public policy. The concerns raised against COPA could at least arguably lead to the conclusion that it is insufficiently effective to justify its costs, whether or not it is consistent with the First Amendment.

Nat'l Acad. of Sciences, at 207 (emphasis added).

Because the information sought by the government is global in nature, any findings based on that information will of necessity be global in nature, and thus will say very little if anything about the impact of the underlying COPA statute on the ability of minors located in the United States to access pornography.

CONCLUSION

The motion to compel of Attorney General Gonzales should be denied.

DATED: February 24, 2006

Respectfully submitted,

__s/ Richard R. Wiebe____

Richard R. Wiebe

Attorney for Amicus Curiae
Center for Democracy and Technology