FRED VON LOHMANN, SBN. 192657
fred@eff.org
CORYNNE MCSHERRY, SBN. 221504
corynne@eff.org
KEVIN BANKSTON, SBN. 217026
bankston@eff.org
LILA I. BAILEY, SBN. 238918
lila@eff.org
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, California 94110-1914
Telephone: (415) 436 9333 x122
Facsimile: (415) 436 9993

THOMAS E. MOORE III, SBN. 115107
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Ave. Third Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Facsimile: (650) 798-5001

Attorneys for *Amici Curiae*
ELECTRONIC FRONTIER
FOUNDATION AND CENTER FOR
DEMOCRACY & TECHNOLOGY

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES INDUSTRIES, INC., et al.

Plaintiff,

v.

JUSTIN BUNNELL, et al.,

Defendant.

CASE NO.: 06-01093 FMC

BRIEF OF *AMICI CURIAE* IN SUPPORT OF DEFENDANT'S OBJECTIONS TO AND MOTION FOR REVIEW OF ORDER RE SERVER LOG DATA

Date: July 16, 2007
Time: 10:00 a.m.
Courtroom: 750
Judge: Hon. Florence Marie Cooper

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

INTRODUCTION

The Order at issue here addresses an important question of first impression: does digital data that exists only temporarily in the random access memory (RAM) of a computer qualify as "electronically stored information" subject to preservation and production under Federal Rule of Civil Procedure 34? In its May 29, 2007 order granting in part and denying in part Plaintiffs' motion to require Defendants to preserve and produce server log data ("Order"), the Magistrate Judge mistakenly answered this question in the affirmative, ignoring both the text of the statute and the traditional limits that apply to federal discovery practice, and relying instead on an inapt analogy to copyright law.

The result is no standard discovery order. If allowed to stand, this Order would mark a radical expansion of the scope of federal electronic discovery obligations, far beyond anything contemplated by the drafters of Rule 34. Virtually every business in the United States relies on digital technologies for all kinds of communications. And virtually every function carried out by those technologies depends on and results in the temporary creation of RAM data that is not ordinarily retained. Thus, the Order threatens actual and potential litigants with the specter of having to capture and compile an avalanche of RAM data that would otherwise be automatically overwritten in the ordinary course of computer processing. Further, the court's expansive reading of Rule 34 undermines the right to read, speak and associate anonymously online by making it impossible for businesses to stand behind strong privacy policies intended to foster those constitutionally protected activities. As a result, the Order destabilizes the carefully crafted balance that Congress and the courts have erected in the discovery context over the past two decades. Finally, the Order unnecessarily puts federal discovery obligations on a collision course with federal electronic privacy laws.

Fortunately, Rule 34 does not require this outcome. The express language of the statute as well as legislative history make clear that Rule 34 applies only to

electronically *stored* information. As a factual matter, because information held only in RAM is not "stored," but rather exists only temporarily until overwritten, RAM data does not fall within the scope of Rule 34. Whether RAM data *could* be stored is irrelevant—Rule 34 does not obligate a litigant to create new documents solely in order to produce them to an adversary. Similarly, whether information in RAM might be relevant (or even necessary) to a litigant's case is also beside the point—Rule 34 cannot be read to conscript a litigant to serve as an investigator on behalf of its adversary.

Amici are organizations dedicated to fostering free speech and privacy rights on the Internet. Because the Order misunderstands the technology and misapplies the law, *amici* urge this court to reconsider the Order and reject Plaintiffs' invitation to radically expand Rule 34's reach in the digital realm. And, should the Court determine that its reconsideration requires it to reach the federal electronic privacy issues, *amici* also urge the Court to schedule further briefing on those complex questions.

INTERESTS OF AMICI

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or *amicus* in key cases addressing the First Amendment and electronic privacy issues as applied to the Internet and other new technologies. With more than 13,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

The Center for Democracy & Technology ("CDT") is a non-profit public interest group that seeks to promote free expression, individual liberty and technological innovation on the open, decentralized Internet. CDT advocates

balanced policies that support the democratizing potential of new digital technologies and media.

ARGUMENT

I. Treating Transient RAM Data as "Electronically Stored Information" Would Radically Expand the Scope of Discovery and Contravene the Express Language of Rule 34

It is well-established that "a party cannot be compelled to create, or cause to be created, new documents solely for their production." *See Paramount Pictures Corp. v. Replay TV*, CV 01-9358, 2002 WL 32151632, * 2 (C.D. Cal. May 30, 2002). The recent "e-discovery" amendments to Rule 34 were not intended to undermine this principle. Report of the Civil Rules Advisory Comm. App. at 28. Quite the contrary: they were intended to put electronic documents on "equal footing" with traditional documents. *Id.* Thus, as amended, Rule 34 simply provides that a party may request documents or "electronically *stored* information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations *stored* in any medium from which information can be obtained...and which are in the possession, custody or control of the party upon whom the request is served." Fed.R.Civ.P. 34 (emphasis added).

By reading "stored" out of the above definition and imposing a preservation requirement on ephemeral information that has no corollary in traditional discovery, the Order undermines the equal footing Rule 34 was intended to establish. The Order then compounds the problem by substituting "fixation," a concept drawn from copyright law, for Rule 34's express requirement that the information be "stored."

A. RAM Data is Transient Data Essential to the Functioning of Virtually Every Digital Device

To understand the implications of the Order, it is crucial to understand the role that RAM plays in digital devices. Virtually every computer and digital device employs transient RAM "buffers" to hold both data and applications while data processing is carried out. Those RAM buffers are generally not used to store or

record data; rather, they constitute a working area where data and applications are manipulated during a computing process.[1] *See, e.g., Apple Computer, Inc. v. Franklin Computer Corp.,* 545 F.Supp. 812, 813 (D.C. Pa. 1982) (explaining that information stored in RAM is an impermanent form of computer memory). For example, as a user types at her keyboard, every stroke (including those that are immediately deleted as "typos") is momentarily represented in RAM, where it is processed by word processing software that is also held in RAM, before being sent to the computer's display.

RAM is inherently transient: "It is a property of RAM that when the computer is turned off, the copy of the program recorded in RAM is lost." *Apple Computer, Inc. v. Formula International, Inc.*, 594 F. Supp. 617, 622 (C.D. Cal. 1984). Due to the sheer volume of data processed through RAM, that data is constantly overwritten by new data during the course of a computer system's operations, sometimes within fractions of a second. James Boyle, *Intellectual Property Policy Online: A Young Person's Guide*, 10 Harv. J. L. & Tech. 47, 90 (1996) ("RAM is volatile; it is constantly rewritten while the computer is being used").[2] Indeed, the very purpose of having RAM is so that data can exist temporarily for processing without being stored.

And, RAM is ubiquitous. *See* Note, Kristen J. Mathews, *Misunderstanding Ram: Digital Embodiments And Copyright*, 1997 BCIPTF 41501, 40 (1997) ("Any

---

[1] Technically speaking, the relevant distinction is whether the information in question has been "stored" by a computer in a manner intended for retrieval at a later time. This does not necessarily turn on the medium in which the information exists, but rather on whether the information is being held temporarily for processing, or stored for later retrieval. For example, certain specialized forms of RAM (known as "flash RAM" and used in the USB "memory sticks" that have largely replaced floppy disks) are intended for persistent storage of information. By the same token, many modern computers may use a portion of their internal hard drives (known as "virtual memory") to temporarily hold information intended for processing but not storage. Here, the parties agree that the information in question is ephemeral data held in RAM. Accordingly, for purposes of this discussion, the term "RAM" is used to describe internal RAM used by computers to hold ephemeral information for processing.

[2] This is precisely the case here. *See* the Declaration of Wes Parker In Support Of Defendants' Objections To And Motion For Review Of Order Re Server Log Data and Objections To Such Order, page 2 (referring to the Server Log Data sought by plaintiffs, stating that "http headers are stored in RAM for at most seconds and likely less than a second").

electronic device that has anything more than an on-off switch usually contains some form [sic] RAM.") Digital devices, including computers, cell phones, personal digital assistants (PDAs), compact disc players, fax machines, and digital televisions, could not function without creating and manipulating data in RAM for a transitory period of time. Niels Schaumann, *Copyright Class War*, 11 UCLAELR 247, 266 (2004) ("For it is not just software that is loaded into a computer's RAM: all content accessed digitally is transferred to RAM before it is made perceptible to humans.").

Given the ubiquity of transient RAM data in digital technologies, courts should treat with skepticism claims that such data is equivalent to a paper document and, therefore, subject to preservation and production under Rule 34. Information that exists solely in ephemeral form in RAM is simply not the same as information that is "stored" for later retrieval.

B. Rule 34 Does Not Contemplate the Preservation and Production of RAM Data

Rule 34 was never intended to reach ephemeral information. In the analog world, a wide array of such information exists beyond the reach of discovery. For example, Rule 34 does not require a civil litigant to record all telephone conversations, even if such conversations might be potentially relevant to the ongoing litigation. Similarly, Rule 34 does not require a corporate litigant to record or transcribe the face-to-face conversations among its employees, nor to take pictures of every scribbling that might appear on a whiteboard at a meeting. Forcing a litigant to preserve and produce these forms of ephemeral information would be impermissible because, in addition to interfering with a party's business routines and privacy, such an order would require the creation of new documents. *See Paramount Pictures Corp.*, 2002 WL 32151632 at * 2; *see also Universal Acupuncture Pain Services, P.C. v. State Farm Mut. Auto. Ins. Co.*, 01 Civ. 7677, 2002 WL 31309232, *4 (S.D.N.Y. 2002) ("It is well-established, however, that courts may not compel the creation of documents to comply with a discovery demand."); *Alexander v. FBI*, 194

F.R.D. 305, 310 (D.D.C. 2000); *Rockwell Int'l Corp. v. H. Wolfe Iron and Metal Co.*, 576 F. Supp. 511, 513 (W.D. Pa. 1983).

The scope of Rule 34 should not vary based on whether information was created using digital or analog technology. The history and text of the revisions to Rule 34 do not contemplate this type of discrimination. Rather, the revisions were designed to ensure that civil discovery would remain "media neutral," so that the discoverability of information would not turn on the way it was stored. *See* Note: Shannon M. Curreri, *Defining "Document" in the Digital Landscape of Electronic Discovery*, 38 LYLALR 1541, 1563 (2005).

In the instant case, upholding the objective of media-neutrality requires attention to Rule 34's express limitation to electronic information that is "stored." According to the Merriam-Webster dictionary, to store is "to lay away, to accumulate or to place or leave in a location (as a warehouse, library, or computer memory) for preservation or later use or disposal." Merriam-Webster's Collegiate Dictionary (Frederick C. Mish et al, eds., 10th Edition 1993). Thus, in choosing to limit Rule 34's scope to "electronically *stored* information," Congress ensured it would apply solely to information that had been laid away, accumulated or kept for future retrieval. Congress reinforced this concept by repeating the term "stored" twice in Rule 34(a), adding that data and data compilations "*stored* in any medium" are subject to discovery. Elsewhere, Rule 34 refers to the need to produce documents as they are "kept in the usual course of business" or "ordinarily maintained." Fed.R.Civ.P. 34(b)(i), 34(b)(ii). Accordingly, the unambiguous text of Rule 34 only permits discovery of *stored* information—information retained by a business in the normal course of its operations.[3]

[3] Moreover, key antecedents to the new electronic discovery rules further support the limitation of discovery of electronic information to only that which has been stored for later use. The influential Sedona Principles, formulated by a forum of judges, attorneys and technologists and consulted by several courts confronted with electronic discovery disputes, *see, Johnson v. Kraft Foods N. Am., Inc.*, 05-2093 2006 WL 3302684 (D. Kan. Nov. 14, 2006); *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005); *Williams v. Sprint/United Management*

Because information held temporarily in RAM is not laid away for future use—indeed it is ephemeral by nature, often immediately overwritten—the Order improperly reads the term "stored" out of the statute altogether. *See Boise Cascade Corp. v. United States EPA*, 942 F.2d 1427, 1432 (9th Cir.1991) ("Under accepted canons of statutory interpretation, we must interpret statutes as a whole, giving effect to each word and making every effort not to interpret a provision in a manner that renders other provisions of the same statute inconsistent, meaningless or superfluous.")

Moreover, a recurrent theme throughout the commentary by the Advisory Committee responsible for the electronic discovery amendments is that the "electronically stored information" not only be "stored" but also "recorded," "accessed," "searched" or "retrieved." Thus, the Advisory Committee stated:

> The volume of – and **ability to search** – much electronically stored information means that in many cases the responding party will be able to produce information from **reasonably accessible** sources that will fully satisfy the parties' discovery needs.
> * * *
> The decision whether to require a responding party **to search for** and produce information that is not **reasonably accessible** depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified.
> * * *
> The responding party has the burden as to one aspect of the inquiry – whether the identified sources are not **reasonably accessible** in light of the burdens and costs required **to search for, retrieve, and produce** whatever responsive information may be found.

Advisory Committee Comments Rule 26(b)(2) (emphasis added). And:

> The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be **retrieved and examined**.
> * * *
> The items listed in Rule 34(a) show different ways in which information may be recorded or stored.

Co., 230 F.R.D. 640 (D. Kan. 2005), describe the proper sources of electronic records for discovery purposes as information "*purposely stored in a manner that anticipates future business use* and permits efficient searching and retrieval." *See* The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Discovery at 9 (emphasis added). *Available at* http://www.thesedonaconference.org/dltForm?did=SedonaPrinciples200303.pdf.

Advisory Committee Comment Rule 34 (a) (emphasis added). Ephemeral RAM data is not "stored" or "recorded" for later "access" or "retrieval." Ephemeral RAM data cannot be "searched" in the normal course. Indeed, the examples of electronically stored information given in the comments all involve items saved in some form of persistent storage:

> Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spreadsheets, different image or sound files, and material from databases.

Advisory Committee Comment Rule 34(b).

Finally, sheer common sense demands that courts not elide the distinction between ephemeral and stored data. Any construction of the electronic discovery rules that would encompass transient RAM data could easily lead to absurd results. For example, calls made via Voice Over Internet Protocol (VoIP) technology, a method of routing voice signals over the Internet, necessarily pass temporarily through RAM and could be retained through the use of simple software designed to log them.[4] In fact, as more businesses turn to digital phone systems, every telephone conversation will be recorded, if only momentarily, in ephemeral RAM copies on computers housed in enterprise data centers.[5] Under the Order, telephone conversations taking place using VoIP or similar digital technologies would suddenly become subject to preservation and potential production, simply because they took place over a digital medium rather than an analog one.

Similarly, every keystroke entered into a computer exists temporarily in RAM, whether or not those keystrokes are ever reflected in any final document ever saved or sent. So, for example, if an employee types an email message, then rewrites it, and then ultimately decides not to send it, the message and its revisions all existed in

[4] The creation of RAM copies is integral to the operation of the sound equipment found in modern computers. *See, e.g.*, "VOIP: Frequently Asked Questions" *at* http://www.fcc.gov/voip. As digital representations of sound waves pass through and are manipulated by digital phone systems, they will be temporarily held in RAM.

[5] *See, e.g.,* Bernard Simon, *A Bright New Day for the Telecom Industry, if the Public Will Go Along*, N.Y. Times, Jan 12 2004 at C3 (describing investment in digital telephone systems that "sends phone calls as digital data like that used over the Internet").

RAM, if only for a short period. And, with the advent of video-conferencing, it is easily conceivable that the digital equivalent of whiteboard scribblings might be temporarily preserved in RAM as well. In many of these circumstances, it would be simple and inexpensive to divert all of this ephemeral RAM data to a more permanent storage medium—to "log" them, as the Order directs Defendants to do for the Server Log Data. Under the Magistrate Judge's reasoning, every one of these ephemeral documents could be subject to preservation and production, simply because it existed momentarily in RAM. Indeed, every digitally mediated communication or transaction, no matter how brief, could be subject to discovery obligations from the moment litigation is reasonably anticipated, thereby creating an extraordinary and unjustified new burden of preservation and production for litigants in federal litigation.[6] This outcome should not be endorsed by this Court.

C. The Order Improperly Substitutes Inapposite Copyright Law Analogies for Sound Federal Discovery Principles.

Lacking support from the text of Rule 34 or the precedents and policies under girding it, the Order relies instead on an inapposite analogy drawn from a controversial Ninth Circuit copyright opinion, *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993).[7] In *MAI*, the Ninth Circuit Court of Appeals suggested that software temporarily held in the RAM of a computer was sufficiently "fixed" to constitute a reproduction for copyright purposes because it could be "perceived, reproduced, or otherwise communicated for a period of more than

---

[6] One of the main flaws in the Magistrate Judge's reasoning is that she defined the term, "Server Log Data" in a way that glossed over the ephemeral nature of the RAM data. In the Order, "Server Log Data" is defined as "(a) the IP addresses of users of defendants' website who request 'dot-torrent" files; (b) the requests for 'dot-torrent files'; and (c) the dates and times of such requests." (Order at 3:15-4:3). In fact, however, this ephemeral data that passes through RAM would have to be processed by a server log program to exist in that form.

[7] *MAI v. Peak* has been widely criticized by copyright commentators. *See e.g.,* Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT § 8.08[A][1] (2005) (noting that the *MAI* court's holding that RAM copies are fixed for copyright purposes has been "contentious."); *see also*, R. Anthony Reese, *The Public Display Right: The Copyright Act's Neglected Solution to the Controversy Over RAM Copies*, 2001 U. OF ILL. L. REV. 83, 122-38 (2001). At least one Court of Appeals has also departed from its reasoning. *See Costar Group, Inc. v. LoopNet,* Inc., 373 F.3d 544, 550-51 (4th Cir. 2004).

transitory duration." Order at 13 (citing *MAI*, 991 F.2d at 518-19). Whatever the merits of the Ninth Circuit's reasoning in *MAI*, the opinion obscures rather than illuminates the central issues here.

In *MAI*, the court was interpreting the meaning of "fixed" as defined by Section 101 of the Copyright Act. That definition is distinct, and serves a very different purpose, from Rule 34's requirement that electronic information be "stored." Under the Copyright Act, a work is "fixed" when its "embodiment in a copy" is "sufficiently permanent or stable to permit it to be perceived, reproduced or otherwise communicated for a period of more than transitory duration." *See* 17 U.S.C. § 101. The concept of "storage" appears nowhere in the Copyright Act's definition.

The definition of fixation, moreover, must be understood as part of the detailed statutory scheme created by the Copyright Act, which grants exclusive rights to copyright owners, balanced by an extensive array of statutory limitations and exceptions. *See* 17 U.S.C. §§ 106-23. The federal discovery system rests on very different premises—it does not convey to a litigant any "exclusive right" to an adversary's property, nor does it provide statutory "limitations and exceptions" to offset such an expansive grant of rights. Nowhere in the Advisory Committee Report is there any reference to copyright law, not any evidence that the drafters of Rule 34 or its recent amendments drew their conceptions of "electronically stored information" from the Copyright Act. *See generally*, The Report of the Civil Rules Advisory Comm. In short, the definition of "fixation" under the Copyright Act sheds no light on the meaning of "stored" under Rule 34.

II. The Magistrate Judge's Order Would Undermine the Right to Read and Speak Anonymously Online.

Unfortunately, the impact of the Order challenged here will be felt well beyond the discovery context. For two decades, Congress and the courts have struggled to balance strong protections for anonymous speech and privacy against

the right of litigants to pursue legitimate cases. One guiding objective has been to avoid chilling Internet speech—even at the cost, in some instances, of limiting a litigant's ability to pursue litigation. By making it impossible for a company to implement *and stand behind* strong privacy practices that further anonymous speech, the Magistrate's Order threatens to undermine that objective via an expansive interpretation of a federal rule of discovery.

A. The Magistrate's Order Would Chill Free Speech

It is well-established that citizens have a First Amendment right to read, speak and associate anonymously. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342, 357, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995) (an "author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment"); *Gibson v. Florida Legislative Investigative Comm'n*, 372 U.S. 539, 544, 83 S.Ct. 889, 9 L.Ed.2d 929 (1963) ("[I]t is ... clear that [free speech guarantees] . . . encompass[] protection of privacy association"); *Talley v. California*, 362 U.S. 60, 64, 80 S.Ct. 536, 4 L.Ed.2d 559 (1960) (finding a municipal ordinance requiring identification on hand-bills unconstitutional, and noting that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind"); Julie Cohen, *A Right to Read Anonymously*, 28 Conn. L. Rev. 981, 1003-19 (1996) (examining the First Amendment jurisprudence supporting the right to read anonymously).

Moreover, these fundamental rights enjoy the same protections whether the context for speech and association is an anonymous political leaflet or an Internet message board. *See Reno v. ACLU,* 521 U.S. 844, 870, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997) (there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to" the Internet"); *see also, e.g., Doe v. 2theMart.com, Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) ("The right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse,

and far ranging exchange of ideas.").

But these Constitutional safeguards mean little in the online world if a discovery rule can make it impossible for services to implement privacy practices that support online anonymity. In the analog world, individuals can read, speak, and associate anonymously with relative ease. They can browse in the stacks of libraries that do not demand identification from their patrons, visit medical clinics that do not record the names of every potential client who stops in to ask a question, and participate in political, social and religious organizations that do not record the names of people who come to meetings and services.[8] An individual may also walk into a copy shop, pay in cash, and print up a pamphlet expressing views on controversial issues, all without having to reveal his or her identity. *Cf.* THE FEDERALIST PAPERS, *reprinted in* THE FEDERALIST (Jacob E. Cooke ed., Wesleyan University Press 1961) (pseudonymous publication by Alexander Hamilton, James Madison, and John Jay).

In the digital world, that same ability to speak, read and participate anonymously depends on at least some service providers offering a comparable "no record" option to their users. Recognizing as much, a number of online entities have adopted policies protecting the constitutional anonymity interests of their users. For example, Indymedia.org, a collective of independent media organizations and journalists offering grassroots news coverage, specifically promises readers that it does not log Internet Protocol (IP) addresses "as a way of protecting the privacy of our visitors." *See* Privacy Policy, *available at* http://docs.indymedia.org/. Similarly, Riseup.net, an organization providing "mail, lists, and hosting for those working on liberatory social change," expressly promises users that it does not keep personally identifying information and does not log IP addresses. *See* Privacy Policy, *available at* http://help.riseup.net/policy/privacy/. Religious organizations have implemented

[8] Alcoholics Anonymous is just one example of an organization promising anonymity in order to provide valuable counseling services. AA explains the importance of anonymity at: http://www.aa.org.au/factfile/fact_file_anonymity.php?nav=mb.

similar policies: the Etz Hayyim Synagogue, for example, expressly declines to record IP addresses. *See* Privacy Policy, *available at* http://www.etz-hayyim-hania.org/_cont/privacy.html ("Etz Hyyim synagogue is **committed to protecting the privacy of visitors** to this Web site. You can visit our site without telling us who you are or revealing any personal information. We do **not** log IP addresses (the Internet address of a computer) or use "cookie" technology to track user sessions and page views on our site.") (emphasis in original).[9]

The Magistrate Judge's Order here jeopardizes these organizations' ability to stand behind these policies. Should they even *anticipate* litigation in which the IP addresses of readers or speakers could be relevant, these organizations would have to log that data or face potential discovery sanctions. *See, e.g., In re Napster, Inc. Copyright Litigation*, 462 F.Supp.2d 1060, 1069 (N.D. Cal. 2006) (litigants have an obligation to preserve relevant documents upon reasonable anticipation of litigation). The inevitable result would be to chill expression, as legitimate forums adjust their policies and individuals who value their anonymity withdraw from active participation.

Further, the Order does, via the back door of discovery, precisely what Congress has refused to do when squarely addressing questions touching on privacy in the online context. For example, recognizing the profound importance of the Internet as a speech arena, in 1996 Congress immunized users and providers of "interactive computer services" from liability for republishing content authored by

[9] Other Internet services have also chosen not to log the IP addresses of their users, and have made express promises to that effect in their privacy policies, including, among others: SoulCast Blogging Services, available at http://www.soulcast.com/page/privacy ("We do not collect personal information, including email addresses. We do not collect or maintain logs of our users' IP addresses and information regarding our users' use of our website and services."); PlayerSnitch.com, a site a site that allows people to warn others of sex predators on online dating sites, available at http://www.playersnitch.com/info.php?page=privacy ("We do not use cookies to track you, and we do not log "IP addresses."); The Virus Tracking Center, available at http://www.resourcelinks.net/securitycenter.htm ("No personal files from your computer are ever sent back to Trend Micro's servers. All virus tracking information is anonymous. We do not log IP addresses or collect personal information about individual users in the Virus Tracking Center database.")

third parties. *See* 47 U.S.C. § 230 ("Communications Decency Act"); *see also Dimeo, v. Max*, 433 F. Supp. 2d 523, 528 (E.D. Pa 2006) (Congress enacted Section 230 "to promote the free exchange of information and ideas over the Internet. In specific statutory findings, Congress stressed that '[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.'") (*quoting* 47 U.S.C. § 230(a)(3)). As a result, federal immunity permits individuals to republish videos, articles or observations as part of the dialog carried on through newsgroups, blogs, email lists, and/or video hosting services, without fear of defamation or other state civil liability.

Put another way, Congress chose to limit an individual's ability to sue republishers of defamatory material, rather than allowing the threat of litigation, however meritorious, in order to encourage intermediaries to open and develop forums for free expression. As the Fourth Circuit put it in the seminal case interpreting Section 230, such liability would be, "for Congress, simply another form of intrusive government regulation of speech." *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998) ("Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum."). Congress thus recognized in Section 230 what the U.S. Supreme Court later confirmed in extending the highest level of First Amendment protection to the Internet: "[G]overnmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it." *Reno v. ACLU*, 521 U.S. at 885.

Moreover, Section 230 conspicuously avoids imposing any affirmative data retention obligations on those who provide online services, leaving room for services that provide a platform for anonymous inquiry, speech and association. Congress could have tied immunity from secondary liability for speech-related torts to an

obligation to affirmatively assist aggrieved litigants by logging users' IP addresses. It did not. Similarly, in the copyright context, Congress expressly declined to impose any data retention obligations on online service providers under the Digital Millennium Copyright Act, which creates safe harbors from copyright liability for service providers who comply with other statutory requirements. *See* 17 U.S.C. § 512. In fact, although Congress enacted specific discovery procedures to protect the interests of copyright holders, such as a streamlined subpoena process, *see* 17 U.S.C. § 512(h), it did not impose on service providers any obligation to gather data or otherwise seek facts indicating infringing activity, 17 U.S.C. § 512(m). In fact, despite enacting numerous laws addressing online activities in a variety of contexts, Congress has assiduously avoided imposing *any* general data retention obligations on U.S. online service providers. *See,* Catherine Crump, *Data Retention: Privacy, Anonymity and Accountability*, 56 Stan. L. Rev. 191, 194 (2003) (comparing United States and European data retention policy).

By making it impossible for online services to stand behind practices intended to protect anonymity, the Magistrate Judge here has rewritten the framework for Internet speech so as to effectively impose a logging requirement on online services, thereby accomplishing precisely the sort of regulation—and concomitant chilling effect—that Congress hoped to avoid when it passed Section 230 of the Communications Decency Act. Protecting private civil litigation interests should not come at the cost of chilling free speech and public participation. *Buckley v. Am. Constitutional Law Found.*, 525 U.S. 182, 192, 119 S.Ct. 636, 142 L.Ed.2d 599 (U.S. 1999) (Courts must "be vigilant . . . [and] guard against undue hindrances to . . . the exchange of ideas.") If Plaintiffs wish to rewrite the regulatory framework that has helped make the Internet into an extraordinary free speech forum, they should address their requests to the legislative process, rather than resorting to the back door of federal discovery.

B. Provisional Masking of IP Addresses in Produced Documents Will Not Adequately Protect Privacy Interests.

The Order provides some initial protection for anonymity by requiring that Defendants produce IP addresses in a manner that will obscure the identities of TorrentSpy users. That requirement is an incomplete solution to the privacy problems created by the Order.

First, the Order itself suggests that the Server Log Data could be disclosed in an unmasked form at a later time. *See* Order at 34 ("defendant (sic) are not, *at least at this juncture*, ordered to produce such IP addresses in an unmasked/unencrypted form") (emphasis added). Accordingly, the requirement that IP addresses be encrypted when produced *today* may be little consolation for users worried about their privacy *tomorrow*. Further, this Order opens the door for future courts to require IP addresses to be recorded and disclosed in an unencrypted manner.

Indeed, the very fact that IP addresses are being recorded, whether or not the addresses are ever required to be produced, could be chilling to perfectly legitimate users.[10] An analogy drawn from the analog world makes this chilling effect plain. Imagine that a copy shop is sued for facilitating copyright infringements on the part of its customers. In the course of the litigation, the court orders the copy shop to record the names and addresses of every customer, even those that pay cash to use the self-service copiers. Were such an order to issue (and, as noted above, such an order in the analog world would plainly run beyond the scope of Rule 34), an individual intent on making copies of an entirely noninfringing pamphlet on a controversial or sensitive topic could well forego making those copies. The individual's trepidation would not be dispelled simply because the copy shop owner

[10] It has been widely reported that the entertainment industry's national litigation campaign against suspected online infringers has netted individuals who have turned out to be innocent. For example, in 2003, the RIAA sued a 66 year-old grandmother, Sarah Ward, for allegedly downloading hundreds of hip-hops songs. *See* Benny Evangelista, *Download Lawsuit Dismissed*, SAN FRANCISCO CHRONICLE, September 25, 2003, at B-1. The RIAA later dismissed the suit with prejudice. *Id.* Consequently, even those who use TorrentSpy for entirely noninfringing purposes have reason to fear having their identities revealed to Plaintiffs here.

tells her that her name and address might be masked, at least initially, if the record ever had to be produced in litigation. If she is truly worried about her privacy, she is likely to leave the shop and never make the copies she had planned rather than put herself at risk—and our public discourse would be the poorer for it.

The implications of such an order could be even more far-reaching. Keeping in mind that businesses must preserve potentially relevant information from the moment litigation is reasonably anticipated, other copy shop owners anticipating similar infringement claims might feel obligated to begin logging the same information. As a result, the world of anonymous copying options available to our hypothetical speaker would shrink, and along with it the likelihood that she will ever share her message with a broader audience.

III. The Magistrate's Electronic Privacy Rulings Misread Federal Electronic Privacy Law and Must be Rejected

In the course of charting a new and dangerous path through the jungle of electronic discovery, the Order makes an equally dangerous detour into the confused thicket of federal electronic privacy law. This area of law is dominated by three statutes that were created or heavily amended by the Electronic Communications Privacy Act ("ECPA") of 1986[11] namely: (1) the Wiretap Act (18 U.S.C. §§ 2510-22), (2) the Pen Register Statute ("PRS") (18 U.S.C. §§ 3121-27), and (3) the Stored Communications Act ("SCA") (18 U.S.C. §§ 2701-2712). This tripartite regime, which comprehensively regulates electronic privacy subject to a raft of narrowly crafted exceptions, is notoriously complex.[12] Indeed, the appeals courts have often

[11] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[12] *See, e.g., U.S. v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1988) (characterizing intersection of Stored Communications Act and Wiretap Act as a "complex, often convoluted, area of the law."); *Konop v. Hawaiian Airlines*, 302 F.3d 868, 878-79 (9th Cir. 2002), *cert denied* 537 U.S. 1193 (2003) (citing *U.S. v. Smith* and noting that "the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . ."). *See also* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 820-21 (2003) (citations omitted) ("The law of electronic surveillance is famously complex, if not entirely impenetrable. Even before Congress added the Internet to the surveillance laws in 1986 [with ECPA], the Fifth Circuit described the Wiretap Act as "a fog of inclusions and exclusions" that frustrated the judicial search for "lightning

struggled in applying its core terms to new technologies, with an unusually high frequency of amended or withdrawn panel opinions[13] and en banc hearings.[14] The Magistrate Judge's superficial analysis, based on unfounded assumptions regarding critical issues of first impression, further muddies the field by flatly contradicting the most recent ECPA case law and, at some points, even contradicting itself.

For example, when considering the Pen Register Statute, the Magistrate implicitly held without analysis that Defendants' provide "electronic communications service" ("ECS"), by applying to Defendants' a statutory exception that is reserved for such providers. *See* Order at 26, citing 18 U.S.C. § 3121(b). Yet the issue of whether providers of internet search services are providers of ECS is a controversial question of first impression. The unsettled nature of this question—whether search engines are ECSs—is reflected in the range of briefing submitted in the case of *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006). In that case, Google argued that its search engine was an ECS and/or a remote computing service ("RCS");[15] *amicus* the Center for Democracy and Technology argued that Google was an RCS;[16] the Department of Justice argued that it was neither an ECS nor an RCS;[17] and a coalition of law professor *amici* sensibly urged caution, arguing that the court should avoid the question altogether until it solicited additional briefing on the

---

bolts of comprehension." The same court has since explained that that "construction of the Wiretap Act [as amended by ECPA] is fraught with trip wires," and in a case involving the intersection between the Wiretap Act [as amended by the ECPA] and the Stored Communications Act, that the law is 'famous (if not infamous) for its lack of clarity.'")

[13] *See, e.g.*, *Theofel v. Farey Jones*, 341 F.3d 978 (9th Cir. 2003), *withdrawn and amended by* 359 F.3d 1066 (9th Cir. 2004).

[14] *See, e.g., United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), *vacated and superseded by* 418 F.3d 67 (1st Cir. 2004) (en banc).

[15] *See* Google's Opposition to the Government's Motion to Compel at 18-21, *Gonzales v. Google Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW), available at http://www.cdt.org/security/20060217google.pdf.

[16] *See* Amicus Brief of Center For Democracy & Technology In Support Of Google's Opposition to the Government's Motion to Compel, at 3-5, *Gonzales v. Google Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW), available at http://www.cdt.org/security/20062024cdt-google-brief.pdf.

[17] *See* Reply Memorandum In Support Of Motion To Compel Compliance With Subpoena Duces Tecum at 17-21, *Gonzales v. Google Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006). (No. 5:06-mc-80006-JW), available at http://www.cdt.org/security/20060224doj-reply-google.pdf.

issue.[18] The court ultimately did not request more briefing, but it also managed to resolve the controversy without ever reaching this difficult ECPA issue. *See Gonzales*, 234 F.R.D. at 688.

The Order also holds, without analysis, that the requests by defendants' users to download torrent files are "electronic communications" in "electronic storage" with defendants (again, apparently assuming that defendants' provide ECS), and therefore that defendants' disclosure of the Server Log Data would not implicate the Wiretap Act because that statute "only prohibits interceptions during transmission (not while in electronic storage, *i.e.*, RAM)." Order at 24. Yet that conclusion flatly contradicts the most recent and well-reasoned decision on that issue. *See United States v. Councilman*, 418 F.3d 67, 85 (1st Cir. 2004) (en banc) (concluding after lengthy analysis "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of [a communication] in such storage is an offense under the Wiretap Act"). Furthermore, if the Order is correct in holding that the Server Log Data includes communications in "electronic storage" with an ECS, a holding on which its Wiretap Act holding relies, then its additional conclusion that the SCA does not forbid disclosure here flatly contradicts another recent and well-reasoned opinion. *Compare* Order at 23 (holding that defendants may disclose contents of communications in electronic storage to Plaintiffs) and *O'Grady v. Superior Court*, 139 Cal.App.4th 1423, 1440-47, 44 Cal.Rptr.3d 72 (2006) (concluding after extended analysis that "the [SCA] makes no exception for civil discovery" and therefore "render[s] unenforceable" civil discovery subpoenas seeking to compel ECS providers to disclose the electronic communications stored in their facilities).

Considering the intricacy of these ECPA issues and the limited space and time

[18] *See generally* Brief of *Amici Curiae* Law Professors Requesting Additional Briefing If This Court Addresses Google's ECPA Defense, *Gonzales v. Google Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006). (No. 5:06-mc-80006-JW), available at http://www.cdt.org/security/20060224law-profs-amicus.pdf.

available, *amici* cannot fully brief this Court on the Order's ECPA deficiencies, or offer a full analysis of how the Court should resolve these knotty problems. Therefore, in light of the complexity of this area of law and a number of serious problems and contradictions within the Order's short analysis, *amici* here urge what the law professors urged in *Gonzales v. Google*: that this Court should avoid reaching the ECPA issues if at all possible, and if that proves impossible, should solicit an additional round of briefing that specifically addresses those issues.

CONCLUSION

For the aforementioned reasons, *amici* respectfully urge this Court to reject the Magistrate's Order.

Respectfully submitted,

DATED: June 22, 2007

By _____

Corynne McSherry, Esq., SBN. 221504
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x122
Facsimile: (415) 436-9993

Thomas E. Moore III, SBN. 115107
THE MOORE LAW GROUP
228 Hamilton Ave. Third Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Facsimile: (650) 798-5001

Attorneys for *Amici Curiae*
ELECTRONIC FRONTIER FOUNDATION AND CENTER FOR DEMOCRACY & TECHNOLOGY