MEGAN E. GRAY (CSB No. 181204)
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. NW, Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Facsimile: (202) 483-1248

AMICI CURIAE
ELECTRONIC PRIVACY INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION, MEDIA ACCESS PROJECT, PUBLIC KNOWLEDGE, THE PRIVACY FOUNDATION, CENTER FOR DIGITAL DEMOCRACY, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, AND CONSUMER ACTION

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

PARAMOUNT PICTURES CORPORATION; DISNEY ENTERPRISES, INC.; NATIONAL BROADCASTING COMPANY, INC.; NBC STUDIOS, INC.; SHOWTIME NETWORKS INC.; THE UNITED PARAMOUNT NETWORK; ABC, INC.; VIACOM INTERNATIONAL INC.; CBS WORLDWIDE INC.; and CBS BROADCASTING INC.,

Plaintiffs,

v.

REPLAYTV, INC., and SONICBLUE INC.,

Defendants.

Case No. CV 01-09358 FMC

APPLICATION TO FILE BRIEF OF AMICI CURIAE CIVIL LIBERTIES AND CONSUMER GROUPS IN SUPPORT OF DEFENDANTS' OBJECTIONS TO MAGISTRATE JUDGE'S DISCOVERY ORDER

Hearing Date:	June 3, 2002
Hearing Time:	10:00 a.m.
Judge:	The Honorable Florence-Marie Cooper
Courtroom:	750
Discovery Cutoff:	October 25, 2002
Pretrial Conference:	Not set
Trial Date:	Not set

Amici request leave to file the accompanying amicus curiae brief. This brief is submitted in support of a reversal of Judge Eick's order mandating surveillance and disclosure of television-usage data. Defendants have consented to the filing of this brief. Plaintiffs refused to consider whether to consent without advance review of the final draft of the brief, which (given the short time frame involved in this matter) could not be provided to them.

The Electronic Privacy Information Center (EPIC) is a public interest research center that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

The Electronic Frontier Foundation is a nonprofit, membership-supported civil liberties organization working to protect civil rights and free expression in the digital world.

Media Access Project is a nonprofit public interest telecommunications law firm that has defended the public's First Amendment rights to receive information before federal agencies and in the courts for nearly thirty years.

Public Knowledge is a public interest advocacy organization dedicated to fortifying and defending a vibrant "information commons" – the shared information resources and cultural assets that we own as a people.

The Privacy Foundation exists to educate the public, in part by conducting research into communications technologies and services that may pose a threat to personal privacy.

The Center for Digital Democracy is a nonprofit organization working to ensure that the digital media systems serve the public interest.

Computer Professionals for Social Responsibility (CSPR) is a public interest alliance of computer scientists and other interested individuals concerned about the impact of computer technology on society.

Consumer Action is a nonprofit watchdog group with offices in San Francisco and Los Angeles that works through a national network of 6,500 community-based organizations.

The matter now before this Court, namely judicially ordered surveillance of third parties as part of a civil lawsuit alleging copyright violations, concerns First Amendment free expression and privacy rights. Amici have long held these rights to be core values protected by the First Amendment, essential to personal development, political liberty, and intellectual freedom. Accordingly, Amici respectfully request leave to file the accompanying amicus curiae brief in support of the objections filed by Defendants to the Magistrate Judge's Order of April 26, 2002.

DATED: May __, 2002

ELECTRONIC PRIVACY INFORMATION CENTER

MEGAN E. GRAY

By:_____
Megan E. Gray

On behalf of Amici Curiae the Electronic Privacy Information Center, Electronic Frontier Foundation, Media Access Project, Public Knowledge, The Privacy Foundation, Center for Digital Democracy, Computer Professionals for Social Responsibility, and Consumer Action

MEGAN E. GRAY (CSB No. 181204)
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. NW, Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Facsimile: (202) 483-1248

AMICI CURIAE
ELECTRONIC PRIVACY INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION, MEDIA ACCESS PROJECT, PUBLIC KNOWLEDGE, THE PRIVACY FOUNDATION, CENTER FOR DIGITAL DEMOCRACY, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, AND CONSUMER ACTION

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

PARAMOUNT PICTURES CORPORATION; DISNEY ENTERPRISES, INC.; NATIONAL BROADCASTING COMPANY, INC.; NBC STUDIOS, INC.; SHOWTIME NETWORKS INC.; THE UNITED PARAMOUNT NETWORK; ABC, INC.; VIACOM INTERNATIONAL INC.; CBS WORLDWIDE INC.; and CBS BROADCASTING INC.,

Plaintiffs,

v.

REPLAYTV, INC., and SONICBLUE INC.,

Defendants.

Case No. CV 01-09358 FMC

BRIEF OF AMICI CURIAE CIVIL LIBERTIES AND CONSUMER GROUPS IN SUPPORT OF DEFENDANTS' OBJECTIONS TO MAGISTRATE JUDGE'S DISCOVERY ORDER

Hearing Date:	June 3, 2002
Hearing Time:	10:00 a.m.
Judge:	The Honorable Florence-Marie Cooper
Courtroom:	750
Discovery Cutoff:	October 25, 2002
Pretrial Conference:	Not set
Trial Date:	Not set

I. INTRODUCTION

As this Court is well aware, SONICblue manufactures and sells a digital video recorder called the "ReplayTV 4000," which acts essentially like a digital VCR Plus, linking television shows to specific numbers for recording, viewing, etc. This device is marketed as *personal television* because it allows digital customization of television viewing. So noxious are some of these customization features to the television studios that they have sued Defendants on an assortment of copyright infringement theories.

In this lawsuit, the television studios asked SONICblue to turn over all data that the company has on its customers' usage of their Replay 4000 personal television machines. SONICblue frankly and under oath answered that it did not possess such data, and that it never had such data.[1] Under both common sense and the Federal Rules of Civil Procedure, that should have been the end of it.

Instead, using the rubric of a discovery dispute, perhaps in a conscious effort to avoid public outrage and a clear appellate route, the television studios marched into court to demand that SONICblue reengineer its product and install software on devices located in users' homes so that this data will be collected.

While SONICblue is certainly capable of pointing out to this Court the wrongness of this ruling, the order raises issues of such gravity and impact upon non-parties well beyond the borders of this litigation that amici participation is appropriate. Bursey v. United States, 466 F.2d 1059, 1083 (9th Cir. 1972) ("The First Amendment interests in this case are not confined to the personal rights of [plaintiffs]. Although their rights do not rest lightly in the balance, far weightier than they are the public interests in First Amendment freedoms that stand or fall with the rights that these witnesses advance for themselves."). Requiring disclosure of consumer viewing habits in the emerging digital environment raises far-reaching

[1] With a few minor exceptions (e.g., www.myreplay.com), which SONICblue agreed to deliver to the television studios.

privacy questions and implicates the design of new technology. See, e.g., EPIC, Digital Rights Management and Privacy, http://www.epic.org/privacy/drm.

II. ARGUMENT

A. Surveillance For The Purpose Of Collecting Prospective Evidence Is Not Permitted By Civil Discovery Procedure.

This Court is not confronted with the question of whether SONICblue should divulge information currently in its possession. Rather, the issue before the Court is whether SONICblue should be compelled to prospectively collect information using technological means at its disposal. The fundamental principles of civil discovery unequivocally reject such compulsion.

In a personal injury lawsuit, it is relevant to know whether a plaintiff who claimed to be wheelchair-bound in fact left his chair; yet, one would be hard-pressed to find a discovery ruling in which a judge ordered such a plaintiff to place an electronic sensor in his chair seat. In a defamation lawsuit, it would be helpful to know if in fact the defamatory comment had a wide circulation among plaintiff's neighbors; yet, it is unfathomable to think that a court would order a microphone to be placed in the local pub.[2]

Such hypothetical discovery rulings are non-existent for the simple reason that the discovery rules do not permit enforced surveillance, regardless of how useful such information might be to an accurate determination of fact from fiction. Amici present this brief in an effort to describe the constitutional underpinnings for why that is.

The bottom-line answer to that "why" question is not particularly complex. It is a matter of personal freedom – a matter of individual privacy. In this country, these principles are so highly valued that we are willing to accept some inefficiencies in other respects.

[2] In the case before this Court, the matter is more grave than even these examples suggest, because the case at bar involves data collection in one's home.

While the television studios try to characterize SONICblue's decision to forego collection of usage data as nefarious, SONICblue's explanation – cost considerations and an earlier public outcry against such surveillance – rings true, especially now, when the public is increasingly concerned about maintaining a realm of personal privacy.[3] This public concern is well-founded in light of the break-neck speed of technological advances. Indeed, if the television studios' proposition were to be adopted – the proposition that any computer producer, telecommunication provider, or electronics manufacturer must place sensors, chips, cameras, what-have-you in a device whenever that device might be used to commit a tort or a crime and such tort or crime might be easily detected if only a tracking mechanism had been built in – then soon all aspects of an individual's life will be recorded and monitored by others.[4]

In order to protect their copyrights, the television studios are willing to sacrifice individual privacy rights, even if it results in a de facto police state.[5] That

---

[3] See Freedom of Information in the Digital Age, American Society of Newspaper Editors Freedom of Information Committee and the First Amendment Center, April 3, 2001 (http://www.freedomforum.org/templates/document.asp?documentID=13597). In interviews with 1,005 adults, the poll found that 89% were concerned about their personal privacy. Privacy, among the respondents, was as important as concerns about crime, access to quality health care, and the future of the social security system. See also Wall Street Journal/NBC News Poll, September 23, 1999, a poll of 2,025 adults by phone found that the loss of personal privacy was the number one concern of Americans as twenty-first century approaches.

[4] For example, it is not far from the realm of possibility, even today, for a XEROX machine to be engineered to make a compressed digital file of the content of every piece of paper copied, and download that data to a diskette, to be gathered by the company during regular maintenance visits.

[5] Interview with Jamie Kellner, CEO of Turner Broadcasting: "Personal Video Recorders…., which I'm not sure is good for the cable industry or the broadcast industry or the networks… because of the ad skips…It's theft. Your contract with the network when you get the show is you're going to watch the spots. Otherwise you couldn't get the show on an ad-supported basis. Any time you skip a commercial or watch the button you're actually stealing the programming. [Question by Interviewer: "What if you have to go to the bathroom or get up and get a Coke?"] I guess there's a certain amount of tolerance for going to the bathroom." Content's King, Cableworld, Apr. 29, 2002 (http://www.inside.com/product/product.asp?entity=CableWorld&pf_ID=7A2ACA71-FAAD-41FC-A100-0B8A11C30373).

is the studios' prerogative. However, under the civil discovery rules, the television studios may not force their choice on third parties.[6] As the Supreme Court recently noted, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion [into this constitutionally protected area] constitutes a search [under the Fourth Amendment]." Kyllo v. United States, 533 U.S. 27, 34 (2001). "Reversing that approach would leave the homeowner at the mercy of advancing technology – including imaging technology that could discern all human activity in the home." Id. at 35-36.

B. The Television Studios Seek Greater Invasion Into Personal Lives Than The Federal Government Has In The War On Terrorism

This distinction between a requirement to produce data already in a party's actual possession versus a requirement to collect information that is not in a party's possession is a critical one.

Indeed, even in the much more serious context of public safety, network service providers are not required to collect data on their customers' activities. Service providers are only required to preserve data that they already collected for their own business purposes.

For example, under the federal wiretap statute, "[T]he authority to direct [service] providers to preserve records and other evidence is not prospective. That is, Section 2703(f) letters can order a provider to preserve records that have already been created, but cannot order providers to preserve records not yet made. Agents cannot use Section 2703(f) prospectively as an 'end run' around the electronic surveillance statutes. If agents want providers to record information about future

[6] It not only violates the civil procedure rules, but also arguably violates separation-of-powers considerations to give the studios what they have thus far been unable to obtain from Congress. See Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002), at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s.2048 (proposed legislation to require all digital media devices to include copyright controls) (no vote in Senate, no similar bill in House).

electronic communications, they must comply with the electronic surveillance statutes…."[7]

Official statements from the United States make this distinction, and the privacy considerations underlying it, clear: "Preservation [of electronic data] does not require a service provider to collect data prospectively. [This reflects a]….. general agreement that, for now, this preservation regime strikes the proper balance between the competing policy interests [privacy versus law enforcement]. With respect to Internet service providers choosing to retain data, the US has taken an approach that neither requires the destruction of critical data, nor mandates the general collection and retention of personal information. Rather, ISPs are permitted to retain or destroy the records they generate based upon individual assessments of resources, architectural limitations, security, and other business needs."[8]

The television studios are seeking, and have obtained from Judge Eick, a mandatory surveillance system even greater that what United States law enforcement, battling international terrorism, has obtained, or considers appropriate. A discovery order according greater surveillance powers to copyright owners, prior to any sort of liability being found, is nonsensical.

C. Personal Television Monitoring Implicates Privacy Rights In Core Arenas.

Judge Eick's data-collection order has caused such public outcry because the order strikes at two bastions of privacy – what happens in one's own home and what ideas one chooses to absorb.

///

///

[7] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Dept. of Justice Computer Crime and Intellectual Property Section, Jan. 2001 (www.cybercrime.gov/searchmanual.htm#lllg1); see also 18 U.S.C. § 2073(f) (wiretap statute).

[8] Prepared Statement of the United States of America, Presented at EU Forum on Cybercrime, November 27, 2001 (www.usdoj.gov/criminal/cybercrime/intl/MMR_Nov01_Forum.doc).

1. A Person's Home Is His Castle, Free From Unwarranted Intrusion.

The home has long enjoyed significant protection as a private place. According to William Blackstone, the law has "so particular and tender a regard to the immunity of a man's house that it stiles it his castle, and will never suffer it to be violated with impunity."[9] William Pitt declared: "The poorest man may in his cottage bid defiance to the Crown. It may be frail – its roof may shake – the wind may enter – the rain may enter – but the King of England cannot enter – all his force dare not cross the threshold of the ruined tenement!"[10]

In the US, the importance of privacy in the home has long been recognized. As far back as 1886, the Supreme Court recognized the importance of protecting "the sanctity of a man's home." Boyd v. United States, 116 U.S. 616, 630 (1886). As the Court later observed in Payton v. NY, 445 U.S. 573, 589 (1980), "In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home…"[11] As recently as Kyllo v. United States, 533 U.S. 27 (2001), the Court ruled that a person's home is such a core component of the right to privacy that the government may not use technological, but physically non-invasive, means to intrude there.

///

///

[9] Commentaries on the Laws of England, 4 William Blackstone, *223 (1765-1769).

[10] Charles J. Sykes, The End of Privacy 83 (1999).

[11] See also Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion"); Shulman v. Group W Productions, 18 Cal. 4th 200, 230-31 (1988) ("the tort of intrusion into private places, conversations or matter is perhaps the one that best captures the common understanding of 'invasion of privacy.' It encompasses unconsented-to physical intrusion into the home…or other place the privacy of which is legally recognized, as well as unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying….'He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant.'").

2. Monitoring An Individual's Content Choices In Expressive Ideas Is An Impermissible Abridgment Of The First Amendment.

While the First Amendment is most commonly thought of in terms of the right to speak freely, its necessary corollary is the right to freely *receive* information and ideas. This right, though not explicitly articulated in the Constitution, is necessary to the successful and uninhibited exercise of the specifically enumerated right to "freedom of speech."

As the Supreme Court put so eloquently, "[I]n the context of this case – a prosecution for mere possession of printed or filmed matter in the privacy of a person's own home – that right [to receive information] takes on an added dimension. For also fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy… [the defendant] is asserting the right to read or observe what he pleases – the right to satisfy his intellectual and emotional needs in the privacy of his own home. He is asserting the right to be free from state inquiry into the contents of his library… If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds." Stanley v. Georgia, 394 U.S. 557, 564-565 (1969).[12] The Supreme Court has recently reiterated the crucial role that the unfettered exchange of ideas plays in our society, stating, "The citizen is entitled to seek out or reject certain ideas or influences without government interference or control." United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 817 (2000); Winters v. New York, 333 U.S. 507, 510 (1948) ("What is one man's amusement, teaches another's doctrine").

[12] See also Grisworld v. Connecticut, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read…and freedom of inquiry…"); Bd. Of Education v. Pico, 457 U.S. 853, 867 (1982) (right to receive information is "an inherent corollary of the rights of free speech…").

As the television studios will correctly point out, Judge Eick's order does not outright prevent individuals from watching what they choose on their ReplayTV 4000 devices. But it is a self-evident truth that people will alter their behavior if they know they know such behavior is being monitored.

As one preeminent scholar notes, the First Amendment's "…zone of protection [covers] the entire series of intellectual transactions through which [people] formed the opinions they ultimately chose to express. Any less protection would chill inquiry, and as a result, public discourse, concerning politically and socially controversial issues – precisely those areas where vigorous public debate is most needed, and most sacrosanct." See, e.g., Julie Cohen, A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace, 28 CONN. L. REV. 981, 1007 (1996).

The Supreme Court has adopted this interpretation of the First Amendment in a series of cases. "The doctrinal groundwork for a right to read anonymously is discernible in the First Amendment jurisprudence of the McCarthy era. Even in cases that accepted some degree of government power to inquire into individual involvement with suspected communist organizations, the Supreme Court's opinions reflect a sense that individual freedom to read and think lie at the heart of the zone of activity that the First Amendment protects. Thus, for example, in Sweezy v. New Hampshire,[13] the Court held that New Hampshire's Attorney General could not, in the course of investigating alleged communist activities, inquire into the contents of a university professor's lectures…six Justices made clear their view that the line of questioning pursued by the state threatened a core First Amendment interest in freedom of intellectual inquiry. In other cases, such as Schneider v. Smith,[14] the Court construed statutes empowering legislative

[13] 354 U.S. 234 (1957).

[14] 390 U.S. 17 (1968).

investigation into 'subversive' activities narrowly, to preclude a broad authorization to 'probe the reading habits' of individuals."[15]

Indeed, the Supreme Court affirmed recently that it is unconstitutional to require adults to register in order to gain access to constitutionally protected speech. In particular, the Court struck down the statutory requirement that viewers provide written notice to cable operators if they wanted access to certain sexually oriented programs because the requirement "restrict[s] viewing by subscribers who fear for their reputations should the operator, *advertently or inadvertently*, disclose the list of those who wish to watch the 'patently offensive' channel." Denver Area Educational Television Consortium v. FCC, 518 U.S. 727, 754 (1996) (emphasis added).

In sum, compelled collection of an individual's television viewing – the modern era's "book list" – will certainly chill that individual's constitutionally protected rights. "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads…. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike…. [F]ear will take the place of freedom in the libraries, book stores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas, government will hold a club over speech…." United States v. Rumely, 345 U.S. 41, 57-58 (1953) (Douglas, J., concurring).

///

///

///

[15] Julie Cohen, A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace, 28 CONN. L. REV. 981, 1007-1008 (1996).

3. Television Viewing Data Is Prohibited From Disclosure In Closely Analogous Statutory Schemes.

Congress itself has recognized the danger of disclosing television usage information. Congress acted to expressly protect this kind of sensitive information even though, until very recently, it was not technologically possible to monitor specific details on an individual's television/cable/video usage. Only general patterns – like what channels were watched or what tapes were rented – could be collected. Nonetheless, society determined that even this limited data needed to be protected from prying eyes. Thus, in order to reassure a deeply concerned citizenry, a plethora of statutes were enacted to protect one's privacy interest in this data.[16]

The data sought by the television studios in this case is, for all intents and purposes, identical to the types of information protected by two acts of Congress. Repeated protection of viewing data – particularly in the civil discovery context – illustrates legislative intent and justifies a reasonable expectation of privacy in this information.

In 1984, Congress enacted the Cable Communications Policy Act ("CCPA"). 47 U.S.C. § 551. Congress, in formulating the Act, envisioned a day where it would be possible for content providers to monitor every minute of viewers' behavior. "Cable systems, particularly those with a 'two-way' capability, have an enormous capacity to collect and store personally identifiable information about each cable subscriber." H. Rep. No.934, 98th Cong., 2d Sess. at 29 (1984), quoted in Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874 (10th Cir. 1992). "Subscriber records from interactive systems," Congress noted, "can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions." Id.

[16] Several states, including California, enacted protections even greater than those created by Congress. However, Amici focus in this brief solely on the Federal laws.

In particular, the Cable Act requires prior notice to affected individuals when disclosure is pursuant to a court order. 47 U.S.C. § 551(c)(2)(B). Usage data is recognized as being so sensitive that the cable company cannot release it even with the user's consent. 47 U.S.C. § 551(c)(2)(C).

Congress acted again in 1988 to protect the same type of records that the television studios have demanded that Defendants surveil and collect. The Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, was enacted shortly after Supreme Court Nominee Judge Robert Bork's video rental records were disclosed, without consent, to a journalist, resulting in massive public shock and outrage.[17]

Under the VPPA, the disclosure standard in civil discovery is particularly protective of privacy rights. A party is prohibited from disclosing data in response to a court order unless there is a compelling need that cannot be accommodated by any other means – and, even then, the individual must be given advance notice of the contemplated disclosure and have an opportunity to oppose it. 18 U.S.C. § 2710(b)(2)(F). If the data is disclosed, the court is required to "impose appropriate safeguards against unauthorized disclosure." Id.

These acts of Congress were intended to protect the privacy of viewers' personal information.[18] Although Defendants are not technically within these statutes, that is only because technology develops faster than legislation can be amended. Nonetheless, the statutes evince unambiguous privacy expectations in television-usage data.

///

///

[17] S. Rep. No. 100-599, 100th Cong., 2d Sess. at 5 (1988); *The News That's Not Fit to Print*, Christian Science Monitor, Feb. 24, 1988, at 12; *Personal but Not Confidential: A New Debate Over Privacy*, N. Y. Times, Feb. 27, 1988, at 56; *Senators Seek 'Bork Bill' on Privacy*, L.A. Times, May 11, 1988, at 17.

[18] Of note, the Cable Act defines personally identifiable information to include everything except "aggregate data." 47 U.S.C. § 551(a)(2)(A). The VPPA's definition is non-exclusive, but extends at a minimum to actual identification. 18 U.S.C. § 2710(a)(3).

D. Both Plaintiffs And Defendants Have Recognized The Privacy Interest In Television-Usage Data.

Because of the fundamental bastions of privacy (home and intellectual freedom), a statutory landscape recognizing privacy interests in television-usage data, and international consensus that data collection is intrinsically more invasive than data preservation, ReplayTV 4000 users have a reasonable expectation that they will not be monitored in their own homes while watching television. Moreover, both the television studios and Defendants have independently recognized this privacy interest.

For example, TiVo, SONICblue's competitor in which some of the Plaintiffs have invested, expressly acknowledges this privacy expectation, stating in the risks section of its 2000 Annual Report: "consumers may be concerned about the use of personal information gathered by the TiVo service and personal video recorder. Under our current policy, we do not access this data or release it to third parties. Privacy concerns, however, could create uncertainty in the marketplace for personal television and our products and services." TiVo Form 10-K Annual Report, Sec. No. 000-27141, March 30, 2000, p. 34.

The television studios cannot credibly contest that, as a general matter, users reasonably expect that they will be free from surveillance in their television-viewing patterns.[19] However, the television studios assert that, in this particular instance, SONICblue's "privacy policy" utterly extinguishes any such expectation. But, contrary to the television studios' assertion, the SONICblue privacy policy does not notify users that they will be subject to the kind of electronic tentacles mandated by the Magistrate Judge's order.

Collection: Indeed, SONICblue's privacy policy generally reinforces a user's sense of privacy – it repeatedly assures consumers that privacy of their

[19] In fact, the public has coined a specific term for those individuals that do expect their television viewing to be monitored – those individuals are called "Nielsen families."

viewing information is "a right, not a privilege." No less than five times, the privacy policy assures users that, if any anonymous viewing information is collected about them, it will never, without their express permission, be linked to or associated with personal identifying information. The policy further provides that "when sending a show from one ReplayTV 4000 to another, the ReplayTV Service does not track or receive notification of which show is being sent or which shows you record."

Disclosure: The policy states that "SONICblue will not share your Personal Information with third parties without your consent, except in *the very limited circumstances* outlined in the next question and answer below." (Emphasis added.) In stating that SONICblue may disclose information pursuant to legal process, the Privacy Policy speaks of disclosure (i) to protect the rights and property of SONICblue, (ii) to protect the safety of SONICblue and its users, or (iii) to assist law enforcement in investigating violations of the SONICblue terms of service or the law generally. The average layperson would not extrapolate from that form legalese to conclude that "legal process" is without judicial gatekeepers to scrutinize subpoenas and discovery demands and thereby ensure that constitutional values, like privacy interests, are given due deference.

In any event, the television studios cannot toss aside, like so much rubbish, a societal expectation that has taken firm root in the public mind, based on Supreme Court precedent and legislative initiatives. Even if the SONICblue privacy policy unambiguously and expressly told users that every aspect of the TV shows they watched would be recorded and disclosed to Plaintiffs, individuals would not necessarily deprived of their reasonable expectation of privacy. Privacy policies are often placed in obscure locations and are not read by users. According to one important study, a majority of Internet users only "sometimes" or "rarely" read online privacy notices. See BusinessWeek/Harris Poll: A Growing Threat,

BusinessWeek Magazine, March 2000.[20] Given the incentive that commercial enterprises have to covertly collect and sell sensitive consumer data, it would be abhorrent to constitutional principals to think that every individual's privacy rights could be extinguished automatically by fine print in self-serving "policies."[21]

SONICblue's actual practice and direct statements to the public – as opposed to what its privacy policy claims – also need to be taken into account in this analysis. It is uncontroverted by any party in this proceeding that SONICblue's actual practice – is now, and has always been – to not collect usage data from ReplayTV 4000 users. Moreover, SONICblue positioned its personal television recorder as an alternative to the privacy-invasive competitive TiVo product.[22] In a multitude of interviews with journalists, resulting in widely published news articles, SONICblue championed its privacy protection. See *Making Television Searchable,* The New York Times, April 22, 1999 ("Unlike the Tivo system, which relays a 'personal profile' of the owner's viewing habits back to Tivo and then to advertisers, **the ReplayTV phone call each night gathers program listing information but does not report on what the owner has been watching. For privacy reasons alone, I would choose [ReplayTV] over the Tivo.**") (emphasis added); *Personal Video Recorders Give Viewers the Latest in Options,* The Dallas Morning News, June 2, 1999 (**"ReplayTV has no plans to monitor viewing habits, [ReplayTV] says. 'That's just unacceptable.'"**) (emphasis added); *Great*

[20] Available at http://www.businessweek.com/2000/00_12/b3673010.htm.

[21] Privacy policies are also not necessarily contractually binding on individuals, because of failure to assent, contract adhesion, unconscionability, etc. Vault Corp. v. Quaid Software Ltd., 655 F.Supp. 750 (E.D. La. 1987), *aff'd* 847 F.2d 255 (5th Cir. 1988); Specht v. Netscape Communications Corp., 150 F.Supp. 2d 585 (S.D.N.Y. 2001); America Online, Inc. v. Superior Court (Mendoza), 90 Cal. App. 4th 1 (2001).

[22] A 2001 report performed by the Privacy Foundation revealed that TiVo's collection practice could facilitate the tracking of users. *TiVo's Data Collection and Privacy Practices*, Privacy Foundation, Mar. 26, 2001 (http://www.privacyfoundation.org/privacywatch/report.asp?id=62&action=0).

Advice You Can Trust, PC World, March 27, 2001 ("TiVo rival ReplayTV does not collect viewer information, a spokesperson says.").[23]

Given SONICblue's effort to distinguish itself from TiVo, it is quite possible that some consumers chose the ReplayTV 4000 unit in specific reliance on these privacy assurances. Neither those individuals' reasonable expectation of privacy, nor those of the public at large, should be simply disregarded.

E. Users Have A Reasonable Expectation Of Privacy In Their Usage Data Separate And Apart From Name Identification.

The television studios are emphatic that Judge Eick's order does not implicate any individual's privacy rights because the individual's name will be masked. The studios are playing a semantics game – "personal" information means 'pertaining to or concerning a particular person.' Personal information is not limited to that which is "explicitly labeled with a subscriber identity." A TV viewer will reasonably believe that no record exists of the fact that he watched a dogmatic, controversial, or sexually explicit show, regardless of whether his actual name is known. It is not difficult to understand that a young woman who explores questions she has about her sexual orientation by watching particular television programs will not want a strange person to collect that scandalous tidbit on her personal life, even if the stranger does not actually know her name.

A more grave concern is the fact that the individual's name, albeit under a *nom de plume*, will be linked to his television-usage data profile. The television studios are simply willing to have the true name redacted for right now; nothing prevents the television studios, or some other third party, from later issuing a subpoena or discovery demand for that one last missing data point. The pseudonym

[23] Available at http://www.pcworld.com/news/article/0,aid,45589,00.asp. See also *Voice News Feature*, Net4TV, December 20, 1998 ("[Unlike TiVo,] ReplayTV has no plans to use customer profiling, but totes a larger price tag, giving consumers a choice between privacy and cost.") (http://net4tv.com/voice/Story.cfm?storyID=424); *Anthony Wood [ReplayTV] and Mike Ramsay [TiVo] Are at War*, Success, March 1, 1999 ("[with] Replay…there's privacy – you don't have to worry about anybody's monitoring your viewing habits.") (available on LEXIS).

proposal advocated by the television studios is but a temporary wall that will collapse with the next dispute or economic shake-up.[24]

In any event, merely redacting a specific individual's name does nothing to address the problem of data "re-identification." Re-identification is the practice of linking an individual's identity to an aggregate database stripped of personally identifying information. That linkage can result in a personally revealing and identifying profile.[25] For example, re-identification might be accomplished by combining hospital-discharge data (publicly released with the patient's name deleted) and any number of private databases (such as consumer warranty databases) – by overlaying these two lists, one could establish the actual identity of individuals in the aggregate database that was originally stripped of identifying information (e.g., the hospital database). In the hospital-discharge database and consumer-warranty database hypothetical, using re-identification procedures, one could determine the identity of the woman who had an abortion last year at the local hospital.

Similarly, given the massive databases already possessed by the plaintiff media conglomerates, using overlaying techniques, they could extract an enormous amount of commercially valuable yet sensitive information (separate and apart from

[24] This ominous prediction is hardly far-fetched. For example, in 2000, EPIC filed a complaint against DoubleClick with the Federal Trade Commission because DoubleClick widely represented to users that it would collect only anonymous data, but it later changed its business model to create detailed profiles on users, including sensitive personal details as well as actual name identification. See Complaint and Request for Injunctive Relief, In the Matter of Doubleclick (http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf).

[25] "It was found that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}. About half of the U.S. population (132 million of 248 million or 53%) are likely to be uniquely identified by only {place, gender, date of birth}, where place is basically the city, town, or municipality in which the person resides. And even at the county level, {county, gender, date of birth} are likely to uniquely identify 18% of the U.S. population. In general, few characteristics are needed to uniquely identify a person." L. Sweeney, Uniqueness of Simple Demographics in the U.S. Population, LIDAP-WP4, Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA (2000).

evidentiary value for this lawsuit) from data received pursuant to Judge Eick's order.

F. Although Judge Eick's Order Should Be Reversed In Its Entirety, If This Court Disagrees, At A Minimum The Privacy Intrusion Should Be Greatly Reduced.

Because of the strong privacy interests that users have in being free from surveillance, especially in their own home, and especially vis-à-vis collection of behavioral data like television-viewing usage details, this Court should not permit Judge Eick's order to stand.

Consumers' privacy interests are shaped by their reasonable expectations. When a legitimate privacy interest of a third party will be invaded during discovery, the presumptive rule is that discovery should not be allowed. As the Supreme Court has held, a court order compelling production of information under circumstances that would threaten the exercise of a fundamental right is "subject to the closest scrutiny." NAACP v. Alabama, 357 U.S. 449, 461 (1958).

It must be emphasized that, without mandatory surveillance, the television studios can still establish their case. The data that the studios will need to collect is still available for collection (data regarding use of the ReplayTV 4000). As in the Sony case, consumer-usage information may be fully developed by less intrusive and invasive means – for example, by a joint survey of users. Sony v. Universal City Studios, 464 U.S. 417 (1984). Understandably, the studios do not find this alternative as attractive as electronic surveillance. No doubt the defendant in the hypothetical posed in the beginning of this brief would not find cross-examination of the personal injury plaintiff as attractive as an electronic sensor in plaintiff's wheelchair, either. However, a party is not entitled, under the civil discovery rules, to the most attractive or effective information-gathering technique. As with most aspects of litigation, competing interests are involved, and in this context, product re-design for enforced surveillance of end-users is not permissible under the

discovery statutes. Moreover, in this case, a consumer survey will be equally effective – if not more effective – at gathering the information that the studios seek.

Even if a discovery judge had authority under the Federal Rules of Civil Procedure to order prospective collection of private third-party data, Judge Eick's order is overly broad.[26]

Feature and Time Limitation: The order currently requires monitoring of all aspects of television usage even though only a few functions of the ReplayTV 4000 are at issue in this lawsuit. Any data-collection order should be limited to Replay 4000 features that are at issue, like Commercial Advance or Send Show. In addition, any data collection should be of limited duration, e.g., thirty days.

Aggregate Information: The data collected should be strictly aggregate information, completely disassociated from any information identifying users. Despite assertions to the contrary, the television studios requested surveillance does *not* ensure such anonymity. Rather, it would require that information be collected with third-party users identified "by unique identification numbers." This mechanism does not prevent the disassociation of use information from user identity, which is so crucial to user privacy.[27] The *potential to correlate* individual use with an identity of the user is *exactly* what caused the outcry over TiVo's actions and over other highly publicized data-collection practices.[28]

Notice and Opt-In: Viewers reasonably expect information only to be released where there is a legitimate and compelling need. Additionally, viewers reasonably expect to be notified of the purpose, uses, and intended recipients of

---

[26] When fundamental expressive rights are implicated, courts require that government action be no broader than necessary to advance its compelling interest. See Shelton v. Tucker, 364 U.S. 479, 488 (1960); Buckley v. Cleo, 424 U.S. 1, 68 (1976) (least restrictive means test).

[27] For example, under SONICblue's privacy policy, the company assured users that it would use "one way encoding" to prevent linking of identifying information to anonymous information.

[28] See, e.g., *Doubleclick Enters New Marketing Territory*, CNET News, Dec. 1, 1999; *Privacy Fears Raised by DoubleClick Database Plans*, CNET News, Jan. 25, 2000; *Internet Marketer DoubleClick in Hot Water*, San Francisco Chronicle, Jan. 27, 2000.

personal information before it is released. Thus, the surveillance should only occur after adequate notice to consumers and a right to opt-in. Opt-in is particularly important in a situation where privacy practices change after the user first purchases the information-collecting device.

Other Limitations: The collected data should be subject to standard protective-order provisions, such as destruction at the conclusion of litigation, "solely for use in this litigation" limitation, and attorneys' eyes only categorization.

III. CONCLUSION

Through the unusual procedure of a motion to compel, the television studios demand that Defendants deploy in users' home personal-television recorders new software that would first collect detailed viewing data on consumers' ReplayTV 4000 devices, then transmit that data to SONICblue servers, and store it there indefinitely. All this in a discovery order, even though this consumer data had never previously been known by, recorded by, or transmitted to SONICblue. All this, even though neither Defendants nor the individual users have been held liable, or likely to be liable, for the torts alleged. It is especially inappropriate to breach privacy rights based on mere allegations of wrongdoing, or otherwise privacy will be too easily shattered based on spurious claims. And once privacy has been breached, effective remedies are difficult to devise (the "cat out of the bag" syndrome).

"Our secrets, great or small, can now without our knowledge hurtle around the globe at the speed of light, preserved indefinitely for future recall in the electronic limbo of computer memories. These technological and economic changes in turn have made legal barriers more essential to the preservation of our privacy." Shulman v. Group W, 18 Cal. 4th 200, 243-244 (1998) (J. Kennard, concurring).

///

///

Because the data that the television studios request does not exist in any currently retrievable form, and cannot be collected consistent with user privacy expectations in their home and about their behavior, the Court should deny the television studios' requested surveillance.[29] If the Court insists on permitting the surveillance, it should proceed in drastically reduced form, as outlined above.

DATED: May __, 2002

ELECTRONIC PRIVACY INFORMATION CENTER

MEGAN E. GRAY

By: _____
Megan E. Gray

On behalf of Amici Curiae the Electronic Privacy Information Center, Electronic Frontier Foundation, Media Access Project, Public Knowledge, The Privacy Foundation, Center for Digital Democracy, Computer Professionals for Social Responsibility, and Consumer Action

[29] Amici note that a separate component of the parties' discovery dispute centers on production of documents already in existence, namely disclosure of SONICblue's customer list. Although privacy issues may be present in this disclosure as well, Amici do not address that issue at this time.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. ARGUMENT 2

A. Surveillance For The Purpose Of Collecting Prospective Evidence Is Not Permitted By Civil Discovery Procedure 2

B. The Television Studios Seek Greater Invasion Into Personal Lives Than The Federal Government Has In The War On Terrorism 4

C. Personal Television Monitoring Implicates Privacy Rights In Core Arenas. 5

1. A Person's Home Is His Castle, Free From Unwarranted Intrusion 6

2. Monitoring An Individual's Content Choices In Expressive Ideas Is An Impermissible Abridgment Of The First Amendment. 7

3. Television Viewing Data Is Prohibited From Disclosure In Closely Analogous Statutory Schemes. 10

D. Both Plaintiffs And Defendants Have Recognized The Privacy Interest In Television-Usage Data. 12

E. Users Have A Reasonable Expectation Of Privacy In Their Usage Data Separate And Apart From Name Identification. 15

F. Although Judge Eick's Order Should Be Reversed In Its Entirety, If This Court Disagrees, At A Minimum The Privacy Intrusion Should Be Greatly Reduced. 17

III. CONCLUSION 19

TABLE OF AUTHORITIES

Page(s)

CASES

America Online, Inc. v. Superior Court (Mendoza),
90 Cal. App. 4th 1 (2001) 14

Bd. of Education v. Pico,
457 U.S. 853 (1982) 7

Boyd v. United States,
116 U.S. 616 (1886) 6

Buckley v. Cleo,
424 U.S. 1 (1976) 18

Bursey v. United States,
466 F.2d 1059 (9th Cir. 1972) 1

Denver Area Educational Television Consortium v. FCC,
518 U.S. 727 (1996) 9

Grisworld v. Connecticut,
381 U.S. 479, 482 (1965) 7

Kyllo v. United States,
533 U.S. 27 (2001) 4, 6

NAACP v. Alabama,
357 U.S. 449 (1958) 17

Payton v. NY,
445 U.S. 573 (1980) 6

Schneider v. Smith,
390 U.S. 17 (1968) 8

Shelton v. Tucker,
364 U.S. 479 (1960) 18

Shulman v. Group W Productions,
18 Cal. 4th 200 (1988) 6, 19

Silverman v. United States,
365 U.S. 505 (1961) 6

Sony v. Universal City Studios,
464 U.S. 417 (1984) 17

TABLE OF AUTHORITIES
(continued)

Page(s)

Specht v. Netscape Communications Corp.,
150 F.Supp. 2d 585 (SDNY 2001) 14

Stanley v. Georgia,
394 U.S. 557 (1969) 7

Sweezy v. New Hampshire,
354 U.S. 234 (1957) 8

United States v. Playboy Entm't Group, Inc.,
529 U.S. 803 (2000) 7

United States v. Rumely,
345 U.S. 41 (1953) 9

Vault Corp. v. Quaid Software Ltd.,
655 F.Supp. 750 (E.D. La. 1987), aff'd 847 F.2d 255 (5th Cir. 1988) 14

Winters v. New York,
333 U.S. 507 (1948) 7

STATUTES

Cable Communications Policy Act, 47 U.S.C. § 551 ..... 10, 11

Consumer Broadband and Digital Television Promotion Act,
S. 2048, 107th Cong. (2002) 4

H. Rep. No. 934, 98th Cong., 2d Sess. (1984) 10

S. Rep. No. 100-599, 100th Cong., 2d Sess. (1988) 11

The Video Privacy Protection Act, 18 U.S.C. § 2710 11

OTHER AUTHORITIES

Charles J. Sykes, The End of Privacy 83 (1999) 6

Julie Cohen, A Right to Read Anonymously: A Closer Look at
Copyright Management in Cyberspace, 28 CONN. L. REV. 981,
1007-1008 (1996) 3