Before the Technology Administration, Department of Commerce
Washington, DC 20230

In the Matter of Digital Entertainment and Rights Management

Comments of the Electronic Privacy Information Center
July 17, 2002

1. Existing digital rights management systems, designed to provide a more predictable and secure environment for the transmission of copyrighted material, are ineffective and do so at the expense of consumers' rights and innovation.

Existing digital rights management ("DRM") technologies designed to produce a more predictable and secure environment for transmission of copyrighted materials invariably do so at the expense of the consumers' rights: to privacy; to freedom of expression; to 'fair use' rights; and, the promotion of science and the useful arts generally. Far from creating positive conditions for commerce, DRM subsidizes inefficient channels of content-delivery in the face of more efficient and more equitable systems of distribution.

Existing DRM systems threaten consumers' privacy.

Today, individuals are free to explore different ideas presented in books, music, and movies anonymously. [1] Existing DRM systems weaken this right by allowing copyright owners to monitor private consumption of content. In an attempt to secure content, many DRM systems require the user to identify and authenticate a right of access to the protected media. In the case of Microsoft's eBook Reader, this means that the media software and users' choices in books are digitally linked to the hardware system and to the Passport profiling system. [2] Some systems, such as Microsoft's Windows Media Player, assign a Globally Unique Identifier (GUID) to the media device that facilitates tracking. [3] These systems create records that enable profiling and target marketing of individuals' tastes by the private sector. Law enforcement can also gain access to these records by subpoena or by simply purchasing them.

In February 2002, Sunncomm, Inc., a DRM systems developer, and Music City Records settled a lawsuit by a California woman who objected to their practice of tracking and disclosing personal information - including music consumption patterns - to third-parties with no opt-out scheme. The settlement agreement required the companies to provide notice to consumers of their information collection practices and to refrain from requiring consumers to disclose their personal information as a condition of downloading, playing, or listening to a CD. [4]

Linking personally-identifiable information to content may result in "price discrimination." Price discrimination is the practice of selling an item at different costs to different consumers. It can be facilitated where the seller knows the consumer's identity, and can associate the identity with a profile that includes financial information on the consumer. DRM systems may enable content owners to control access to content, but also to adjust the price of content based on the consumer's identity.

Alternative models exist that would provide copy protection while protecting privacy; they are discussed in more detail in the response to Question #3, below.

DRM systems cannot recognize consumers' "fair use" rights.

'Fair use' allows individuals to interact with content to promote cultural production, learning, innovation, and equity between content owners and consumers. 'Fair use' includes libraries' and educators' rights to provide content to users, the right to sell physical copies of certain content that one acquires lawfully (the "first sale" doctrine), and the ability to make a backup copy of software and music.

It is impossible for DRM systems to incorporate 'fair use' principles in code because they are difficult to define and evolve over time. No DRM standard developed affords users these rights. [5] Nor is it likely that any future DRM technology could do so, as engineers would need to be able to program a federal judge onto a computer chip." [6] Any attempt to enumerate the conditions of 'fair use' in code will necessarily give it an artificially rigid scope and shrink the rights and expectations Americans now enjoy in law.

DRM systems threaten consumers' freedom of expression and the public domain.

DRM restricts access to the public domain at the whim of copyright owners and creates obstacles to the free flow of information, even for legitimate purposes. The Constitution grants copyright to authors for limited terms, after which works are supposed to enter the public domain. However, even with authorization, an archivist cannot be confident in his or her ability to migrate and store content protected by DRM, particularly when limitations are placed on which devices can be used to access the content or when access is provided in conjunction with a pay-per-use system.

The unfortunate fact is that copyright holders have a commercial, albeit short-sighted, incentive to design DRM systems restrictively when it comes to protected uses. [7] Understandably, this has led many to worry that the architecture of cyberspace will create too much, rather than too little, control over the distribution of content.

> "[T]he technology of cyberspace, *in combination with the protections of law*, will produce greater control over the use of copyrighted material than the balance intended by the *Copyright Act*." [8] [Emphasis added]

The combination of DRM and legal remedies against circumvention of copyright protection or the altering of rights management information means that copyright holders could write, through code, their own copyright laws to put legal force behind any restrictions chosen by a copyright holder. Professor Charles Nesson of Harvard Law School recently described the problem as follows:

> "[W]ithout respect for time limits on copyright, the amount of uncopyrightable material within the 'protective envelope', or the doctrines of first sale and fair use… copyright holders are thus staking a claim far in excess of the exclusive rights explicitly granted them in existing copyright legislation." [9]

Professor Lawrence Lessig of Stanford Law School, perhaps the most outspoken critic of the negotiation of public law by private code, [10] suggests that we are entering an age in which "The problem will center not on copy-right but on copy-*duty*, - the duty of owners of protected property to make that property accessible." [11]

The Business Software Alliance, an industry watchdog, dismisses this objection, stating that

"such proposals are intended to preserve the existing balance [of interests established by the Berne Convention] between [creators'] rights and exceptions to those rights (including access to works in the public domain)." [12] But the road to copyright Hell is paved with such intentions and there is plenty of evidence that we are already on our way. [13]

DRM systems threaten consumers with criminal sanctions.

Criminal sanctions are blunt instruments and should be employed with great caution in the copyright context. Until recently, penalties were invoked only for serious, damaging infringers, and not against non-infringers or *de minimis* infringers. [14] Provisions in the *Digital Millennium Copyright Act* change this balance by prohibiting the circumvention of DRM technologies, even where there is no commercial copyright infringement or criminal intent to defraud copyright holders.

The Secure Digital Music Initiative ("SDMI"), an industry sponsored research effort, challenged scientists to break their industry encryption code for the purpose of determining if it was suitably secure. In return, the SDMI offered a reward, but only if researchers who broke the code promised not to publish their findings. [15]

Princeton University Professor Edward Felten and a team of researchers cracked the code but chose not to claim the reward. Instead, they decided to publish their results at a conference. In response, the SDMI threatened Felten and his team with possible litigation, claiming that the paper, which explained how the team had defeated watermarking technology meant to protect digital music, was a circumvention technology under the DMCA. Public pressure forced the SDMI to back down and Felten subsequently launched a counter-suit with help from the Electronic Frontier Foundation. The suit was dismissed, but the chilling effect on academic freedom had already been felt.

In July 2001, U.S. Federal agents arrested Dmitry Sklyarov at the "DEF CON" conference in Las Vegas, after he described a program he had written to export content from Adobe Systems' proprietary encrypted eBook format to its non-encrypted portable document format (PDF). The action Sklyarov had engaged in was not prohibited in his native country, Russia, where the program had been developed.In response to Sklyarov's arrest, Rep. Rick Boucher (D-VA), pointed out that Sklyarov's technology could be used for legitimate purposes such as copying a digital book to another device (i.e. a PDA) for personal use. He stated, "We now have seen the law being misused… this went too far." [16] Sklyarov was released in December 2001 in exchange for testifying against his employer, Elcomsoft, for whom he had written the decryption program.

Last August, a Dutch cryptographer, Neils Ferguson, reported that he had found a flaw in Intel's digital content protection technology, but has refused to publish it because he fears ending up in Dmitry Sklyarov's shoes the next time he lands in the U.S. [17] Intel has indicated that Ferguson is welcome to present his work, but if the FBI chooses to track him down, it's out of their hands. [18] This is not much incentive for Ferguson to publish his findings and Intel will suffer as a result.

DRM systems threaten consumers' ability to use free and open source software.

DRM schemes and laws that require embedding copy protection into devices endanger the development of free and open-source software. Free and open-source software developers rely on reverse engineering to write programs that can interact with hardware. This practice is illegal

under the DMCA. Additionally, some DRM standards require that software be "tamper-resistant." "Tamper-resistant" is defined in such a way that it makes open source implementations non-compliant.

Existing DRM systems threaten the innovation and the promotion of science and the useful arts.

The ability of intellectual property owners to misjudge the benefits of new information and communications technologies to the point of actual or potential self-inflicted harm can never be underestimated. [19] David Boies, a prominent attorney who represented Napster in its recent travails, reminds us that Hollywood has waged a kind of neo-Luddite battle against technology for over fifty years, "Cable television came along and copyright owners said, 'Oh, this is terrible. They're reproducing our copyrighted shows and not paying us.' They sued to stop it." [20]

In the 1954 Canadian case of *Canadian Admiral Corp.* v. *Rediffusion, Inc.*, [21] the court held that non-consensual cable-based retransmission infringed neither the then-existing 'public performance right', nor the then-existing 'communication right'. Fifty years later, the result is an explosion in cable-viewing and a demand for content that has tremendously enriched the very same copyright holders who fought against this technology. Today, some of the largest companies on Canada's national stock exchange are cable companies. The same story was repeated here in the U.S.

In the late seventies and early eighties, the battle between copyright and technology once again grew heated. In *Sony* v. *Universal City Studios*, [22] copyright holders sought to enjoin the sale of video tape recorders, declaring that "the VCR is… to the American film producer and the American public as the Boston Strangler is to the woman alone…." [23] Luckily for the public, equipment manufacturers *and* for the motion picture industry, the Supreme Court did not agree with this analogy nor with the argument generally that manufacturers should be held liable for unauthorized copying by the public. The court held that where a technology functioned as a tool for infringement, but was capable of significant non-infringing uses, supplying the technology to consumers did not violate the law. Justice Stevens, delivering the opinion of the court, declared that "audiences may increase and, given market practices, this should aid plaintiffs rather than harm them." [24] Allowing an injunction to issue in such a case would disserve the public interest.

Copyright holders can often be heard to argue that what matters is which *use* of the technology *predominates*. That has never been the law, and, indeed, in the *Sony* case, it was absolutely clear that more than 80 percent of the use was copyright infringement. The issue is not which is the predominant use, but rather, is there any substantial non-infringing use? And in fact, in *Sony*, the Supreme Court did not say there had to be any actual substantial non-infringing uses - it said that the technology merely had to be capable of substantial non-infringing uses.

DRM systems threaten consumers' expectations and set the stage for a pay-per-use business model.

DRM systems can limit users' interaction with media. Through limiting interaction, DRM technologies can change users' over time expectations about control and use of digital content. [25] DRM developers also may be attempting to acclimate consumers to a pay-per-use business model, one where consumers lose rights to access content that has been purchased.

2. Existing DRM standards and systems create major obstacles to the open commercial exchange of digital content.

Consumers are the ultimate arbiters of any DRM system. [26] In order for a standard to be useful, it must be adopted by a critical mass of consumers. Any framework that does not take into account the public interest in privacy, freedom of speech, and 'fair use' in copyright is doomed to alienate the very individuals at which it is aimed and will thus fail. This is the primary weakness of all current DRM systems: they do not take into account the public interest.

Further, as has already been discussed at length in response to Question #1, existing DRM standards call for proprietary systems which impinge on the neutrality of the network, making it more difficult to innovate future, unforeseen uses - not only for DRM, but for all applications.

Finally, as will be discussed in the responses to Questions #3 and #4, DRM standards that do not take adequate account of the public interest will fail.

3. A future framework for success will recognize public interests.

At a recent Congressional hearing on the consumer benefits of DRM, the Vice-President of Microsoft's Windows New Media Platform Division recognized that DRM systems cannot alone solve the piracy problem.

> "Microsoft and others in the industry learned from their technical protection efforts in the 1980s, using DRM protections as an anti-piracy club, without adequate regard for consumer convenience and expectations, risks alienating lawful consumers and impeding the growth of legitimate distribution channels. Instead, content owners must combine the effective use of DRM tools with new business models that give consumers realistic and attractive alternatives to piracy." [27]

A successful DRM technology will protect consumer privacy

Traditionally, copyright and privacy were compatible because copyright controls *public* distribution, performance and communications. [28] DRM technologies change this equation to include the surveillance and control of *private* use of digital content online. Many existing DRM technology facilitate the profiling of consumers' preferences and consumption patterns. While this is not a new phenomenon, profiling in the digital age is more problematic because it is often more invasive and less transparent to the consumer.

A successful DRM system will not force a consumer to *identify* himself or herself for the benefit of accessing online entertainment. Instead, a successful system will only *confirm the eligibility* of a particular consumer to perform certain actions (i.e. receive a subscription, fill a prescription, make a bill payment, etc.). [29]

A successful DRM system will not impinge 'fair use' rights.

At the Congressional hearing on the consumer benefits of today's DRM systems, Rep. Howard Berman (D-CA), ranking minority member of the Subcommittee on Courts, the Internet and Intellectual Property, noted that "consumers are understandably concerned about how DRM systems may restrict their expectation to be able to make fair uses of copyrighted works…" and that Congress must "give serious consideration to how today's DRM-protected products and services affect the fair use expectations of consumers." [30]

At the same meeting Rep. Zoe Lofgren (D-CA) argued that "DRM technology will ultimately fail if it prevents [fair use] and other consumer expectations in the name of outdated business

models. Put simply, the rights of the copyright owner to control their work must be balanced with the rights of the consumer. Traditionally, copyright law has aspired to do just that. The great challenge today is to maintain that balance in the digital world by finding ways to prevent and punish digital pirates without treating every consumer as one." [31]

A successful DRM system will not impinge consumers' freedom of expression or the public domain.

Copyright is a critical part of the process of creativity. While a great deal of creativity would not exist without the protections of the law, the same can be said of the existence of a meaningful public domain. The goal of law should be to push cultural products quickly into a public-domain "commons" where they can be enjoyed by all - and, perhaps, transformed into something new. [32] Any successful DRM system will need to recognize and facilitate this goal.

A successful DRM system will not render free or open source software non-compliant.

DRM systems are used, by copyright holders, to retain market share and protect copyright, by constraining what consumers can do with digital content, devices to access that content and by making it expensive to switch from one proprietary product or standard to another. [33] The architecture of digital rights management facilitates and expands monopolies of market power and allows copyright holders and technology developers to control not only users' present behavior, but more importantly, their future options and choices.

Successful DRM standards and systems must give consumers the greatest amount of individual choice, including the choice to use free or open-source software systems.

A successful DRM system will not impact network neutrality or discourage legitimate unintended uses of content or infrastructure.

To take just a few examples, Internet telephony, peer-to-peer, and electronic commerce are all applications far outside the range of expectations of those who designed the Internet (or even those who, much later, created the World-Wide Web). Indeed, e-mail itself, the first true "killer app" of the Internet, was an unintended by-product hacked by early users of the network, not the point of the network itself. [34] By keeping the cost of innovation low in the future - especially in the context of broadband media - the design of the successful DRM standards should respect the neutrality of networks and will facilitate innovation not dreamed of by those who design the standards.

4. Current consumer attitudes towards online entertainment demonstrate the failures in current digital rights management systems.

Our transactions in cyberspace - commercial and otherwise - are mediated more by private code than public law or by public laws giving legal force to private code. If copyright is a bargain - a relationship between equal stakeholders - then the subsuming of accountability in the relationship is a betrayal of that relationship. When individuals feel betrayed in relationships, they often begin to act outside of them; we see this manifesting in the widespread piracy on the Internet. [35]

The continued growth of broadband penetration indicates clear consumer demand for rich-media content: music, movies, and other forms of online entertainment. According to the U.S. Department of Commerce's February 2002 report on national internet use, "The rate of growth of internet use in the United States is currently two million new internet users per month. [36]

Consumers enjoy online entertainment because it is convenient and easy to access and share digital content. Consumers enjoy the freedom of listening, reading or watching from the comfort and privacy of their own home. Unfortunately, in the absence of legitimate services the online demand is manifested largely through piracy. [37]

According to online polls, consumers consider anonymity of consumption of content to be vital to their online activities. Most consumers are concerned with corporate profiling and marketing strategies and want legislation protecting their right to privacy online. According to the Wall Street Journal/NBC News Poll in the Fall of 1999 of 2,025 adults by phone found that the loss of personal privacy was the number one risk of Americans as twenty-first century approaches. 29% of respondents reported that the "loss of personal privacy" was a top concern. Privacy outranked other high-profile concerns such as overpopulation (23%), terrorist acts (23%), racial tensions (17%), world war (16%), and global warming (14%). [38]

A more recent poll by BusinessWeek/Harris Poll: A Growing Threat, BusinessWeek Magazine, March 2000 conducted by phone of 1,014 adults found that 89% were uncomfortable with schemes that merged tracking of browsing habits with an individual's identity, 95% were uncomfortable with profiles that included tracking of browsing habits, identity, and other data, such as income and credit data, 63% were uncomfortable with tracking users' movements on the Internet, even when the clickstream was not linked to personally-identifiable information, 92% were uncomfortable with web sites that shared user information with other organization, 93% were uncomfortable with web sites that sold user information to other organizations and finally 91% were uncomfortable with information sharing that allow tracking users across multiple web sites. [39] In a series of surveys conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability (GVU) Center repeatedly demonstrated strong support for Internet Anonymity. In the GVU surveys, individuals expressed "strong agreement" with the statement that anonymity on the Internet is valuable [40]

This means that individuals want accountability and security when online and want to know when information is being collected, its purposes, and whether it is being sold to other entities. A successful DRM system must take into account these consumer demand for privacy and anonymity of access.

Both EPIC [41] and EFF [42] maintain extensive online resources on DRM technologies. We encourage the Department to draw upon these resources, as you go forward. We also request to meet with you or your staff to discuss these issues.

Sincerely,

Chris Hoofnagle
Legislative Counsel
Electronic Privacy Information Center

Jason Young
IPIOP Clerk
Electronic Privacy Information Center

Nicole Anastasopoulos
IPIOP Clerk
Electronic Privacy Information Center

---

[1] See Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management in Cyberspace*, 28 Conn. L. Rev. 981 (1996).
[2] Russel Kay, *Copy Protection: Just Say No*, Computerworld, (Sept. 4, 2000); Chris Jay Hoofnagle, *Overview of Consumer Privacy 2002*, 701 Practising Law Institute 1339 (2002), at http://www.epic.org/epic/staff/hoofnagle/plidraft2002.pdf; Chris Jay Hoofnagle, *Digital Rights Management and Privacy,* Presentation to the Santa Clara University Law School Symposium on Information Insecurity, February 8, 2002, at http://www.epic.org/epic/staff/hoofnagle/drm.ppt.
[3] Richard Smith, *Serious Privacy Problems in Windows Media Player for Windows XP*, Computerbytesman, Feb. 20, 2002, at http://www.computerbytesman.com/privacy/wmp8dvd.htm.
[4] Press Release, SunnComm, Inc., Sunncomm and Music City Records Agree to Resolve Consumer Music Cloqueing Law Suit by Providing Better Notice and Enhancing Consumer Privacy (February 22, 2002), at http://www.xenoclast.org/free-sklyarov-uk/2002-February/001580.html.
[5] Fred Von Lohmann, Reconciling DRM and Fair Use: Preserving Future Fair Uses?, Address at the Conference on Computers, Freedom, and Privacy 2002 (April 19, 2002), at http://www.cfp2002.org/fairuse/lohmann.pdf.
[6] Electronic Privacy Information Center, Digital Rights Management and Privacy, at http://www.epic.org/privacy/drm/.
[7] John P. Barlow, *Selling Wine Without Bottles: The Economy of Mind on the Global Net*, http://www.eff.org/Publications/John_Perry_Barlow/HTML/idea_economy_article.html.
[8] *A&M Records Inc*. v. *Napster Inc*., 2000 U.S. Dist. LEXIS 6243 at 30-31.
[9] *Universal City Studios, Inc*. v. *Reimerdes,* 111 F.Supp.2d 346 (S.D.N.Y. 2000) (*sub*. *nom*. *Universal City Studios, et*. *al*. v. *Corley et*. *al*.), aff'd 273 F.3d 429 (2d Cir. 2001), Nesson Br. at 2.
[10] See Lawrence Lessig, *Code and Other Law of Cyberspace* (2000); Lawrence Lessig, *The Future of Ideas: the future of the commons in a connected world,* (2001).
[11] *Id*. *Code and Other Laws*.
[12] A. Dixon and M. Hansen, *The Berne Convention Enters the Digital Age*, 18(11) E.I.P.R. at 605, 611 (1996).
[13] For an frank discussion of the bluntness of DMCA provisions see *e.g*. Mike Godwin, *Technology vs*. *Technology: Should Code-breakers Go To Jail? The Limits of Anti-circumvention* (5th Annual Technology & Society Conference, Cato Institute, 14 November 2001) [unpublished], online: Cato Institute http://www.cato.org/events/futureip/ (date accessed: 4 December 2001) at 6-7.
[14] *Id*. at 8.
[15] 3 Melvin B. Nimmer and David Nimmer, *Nimmer on Copyright*, c. 12A §2A.04 (2000), Identification and analysis of flaws in encryption technology for the purpose of advancing the state of knowledge in the field is an exception to the prohibition on anti-circumvention under §201.
[16] Lisa Bowman, *Hacker arrest may spur review of digital rules* CNET NEWS.COM, July 27, 2001, http://news.cnet.com/news/0-1005-200-6699001.html.
[17] Neil Ferguson, *Censorship in action: Why I don't publish my HDCP results*, August 16, 2001, http://www.macfergus.com/niels/dmca/cia.html.
[18] Steve Kettmann, *Dutch Cryptographer Cries Foul*, WIRED, August 16, 2001, http://www.wired.com/news/politics/0,1283,46091,00.html; Jen Muehlbauer, *Princeton Professor Bares All*, THE INDUSTRY STANDARD, August 16, 2001, http://www.thestandard.com/article/0,1902,28734,00.html.
[19] Howard Knopf, *Parallel Imports and the Internet: Bits, Borders, Barriers and Exhaustion*, Address to the 8th Annual Conference on Intellectual Property Law and Policy, Fordham

University, (April 27-28, 2000), at 75 (forthcoming 2002) (notes on file with the author).
[20] John Heileman, *David Boies: The Wired Interview* WIRED, (October 2000), http://www.wired.com/wired/archive/8.10/boies.html.
[21] *Canadian Admiral Corp*. v. *Rediffusion, Inc*., [1954] Ex. C.R. 382, 20 C.P.R. 75.
[22] *Sony Corp*. v. *Universal City Studios, Inc*., 464 U.S. 417 at 431 (1984).
[23] Home Recording of Copyrighted Works, Hearings, Subcommittee of the Judiciary Committee, 97th Cong., 2d Sess., No. 97, Pt. 1, at 8, comments by Jack Valenti.
[24] *See note 22*.
[25] See Richard Stallman, *The Right to Read* (1996), at http://www.gnu.org/philosophy/right-to-read.html.
[26] Zoe Lofgren, *Prepared Statement Consumer Benefits of Today's Digital Rights Management (DRM) Solutions Hearings Before the Subcomm. On Courts, the Internet, and Intellectual Property,* 107th Cong. 5 (2002).
[27] William Poole, *Prepared Statement Consumer Benefits of Today's Digital Rights Management (DRM) Solutions Hearings Before the Subcomm. On Courts, the Internet, and Intellectual Property,* 107th Cong. 16 (2002).
[28] Pamela Samuelson, Copyright and Censorship, Keynote address at the Censorship & Privacy Conference, Faculty of Law, University of Toronto, (January 25, 2002), in Jason Young *Conference Notes*, January 30, 2002, at http://www.lexinformatica.org/dox/censorship.pdf at 4.
[29] Stefan Brands, Rethinking *Public Key Infrastructures and Digital Certificates; Building in Privacy* (Cambridge: MIT Press, 2000) at 5.
[30] Howard L.Berman, *Prepared Statement Consumer Benefits of Today's Digital Rights Management (DRM) Solutions Hearings Before the Subcomm. On Courts, the Internet, and Intellectual Property,* 107th Cong. 3 (2002).
[31] Zoe Lofgren, *Prepared Statement Consumer Benefits of Today's Digital Rights Management (DRM) Solutions Hearings Before the Subcomm. On Courts, the Internet, and Intellectual Property,* 107th Cong. 5 (2002).
[32] Dale Zalewski, "'The Future of Ideas': Protecting the Old With Copyright Law" *New York Times*, January 6, 2002.
[33] *Id*.
[34] Mark Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era* 48 UCLA L. R. 925, 932 (2001).
[35] Jason Young, *Digital Copyright Reform in Canada: Reflections on WIPO and the DMCA* LEX INFORMATICA, 30 (2002), at http://www.lexinformatica.org/dox/copyright/digitalcopyright.pdf.
[36] Economics and Statistics Administration and National Telelcommunications and Information Administration, U.S. Dep't of Commerce, Pub. A Nation Online: How Americans Are Expanding Their Use of the Internet (2002).
[37] Howard Coble, *Prepared Statement Consumer Benefits of Today's Digital Rights Management (DRM) Solutions Hearings Before the Subcomm. On Courts, the Internet, and Intellectual Property,* 107th Cong. 2 (2002).
[38] Electronic Privacy Information Center, *Reported in Report Slams Privacy Policies; Poll Finds Privacy is Top Concern* (September 23, 1999) at http://www.epic.org/privacy/survey/default.html.
[39] Electronic Privacy Information Center, *A Growing Threat* (March 2000) at http://www.epic.org/privacy/survey/default.html.
[40] Electronic Privacy Information Center. *Graphic, Visualization, & Usability Center 10th WWW User Survey* (October 1998.) at http://www.epic.org/privacy/survey/default.html
[41] Electronic Privacy Information Center, *Digital Rights Management and Privacy*, at

http://www.epic.org/privacy/drm/.
[42] Electronic Frontier Foundation, *Campaign for Audiovisual Free Expression*, at http://www.eff.org/cafe/.