Testimony of

Mr. William Barr

September 9, 2003

Statement of William Barr
Executive Vice President and General Counsel
Verizon Communications
Before the United States Senate
Committee on The Judiciary
Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks
September 9, 2003

Mr. Chairman and members of the Committee, thank you for inviting me here today to discuss this important issue.

We at Verizon recognize the legitimate interests of copyright owners and the threats to those interests that are posed by the misuse of new technologies, including peer-to-peer software. Verizon remains committed to working with the copyright community to find solutions to these issues that result in effective protection for intellectual property, without placing substantial burdens on Internet service providers or violating the privacy and First Amendment interests of their subscribers. Back in 1998, Verizon and other service providers agreed in the Digital Millennium Copyright Act ("DMCA") to conduct voluntary industry negotiations aimed at developing "standard technical measures" (also known as digital rights management tools), to protect copyright works from online infringement.1 The copyright community has never accepted our offer to begin those negotiations and to work cooperatively toward a technical solution to this problem. In the end, as in the area of VHS recordings and cable television access to broadcast programming, Verizon believes that appropriate technical and legal solutions will be

1 17 U.S.C. 512(i)(1) & (2).

- 2 -

found. As discussed in detail below, the district court's misreading and misapplication of the Section 512(h) subpoena power is not that solution.

As an Internet service provider, Verizon promptly takes down infringing material that resides on our system or network in response to requests from copyright owners and we have strict policies against infringement of copyrights. Verizon also promotes legitimate pay music sites such as MP3.com and Rhapsody as part of its ISP service. We will continue to work with copyright owners to marry the power of the Internet with the creative genius of content providers through new business relationships and licensed websites that offer music, video, and other proprietary content to the over 100 million Internet users in this country. Verizon believes that lawful and licensed access to quality content is essential to the continuing development of the Internet in general and broadband in particular, and we are committed to exploring technological and other solutions so that copyright owners may enjoy the fruits of their labors and Internet users will have access to a rich array of digital content.

However, the answer to the copyright community's present business problems is not a radical new subpoena process, previously unknown in law, that un-tethers binding judicial process from constitutional and statutory protections that normally apply to the discovery of private data regarding electronic communications. Verizon believes that the district court was wrong in concluding that Congress authorized such a broad and promiscuous subpoena procedure in the DMCA--but whatever the courts ultimately conclude on this issue--the subpoena power endorsed by the district court is not an effective remedy for copyright holders and has great costs in terms of personal privacy, constitutional rights of free expression and association, and the continued growth of the Internet.

- 3 -

As interpreted by the district court, this subpoena provision grants copyright holders or

their agents the right to discover the name, address, and telephone number of any Internet user in this country without filing a lawsuit or making any substantive showing at all to a federal judge. This reading of the DMCA accords truly breathtaking powers to anyone who can claim to be or represent a copyright owner; powers that Congress has not even bestowed on law enforcement and national security personnel. It stands in marked contrast to the statutory protections that Congress has enacted in the context of video rentals, cable television viewing habits, and even the requirements for law enforcement officers to gain access confidential data associated with electronic communications.

All one need do is fill out a one-page form asserting a "good faith" belief that a copyright has been infringed and one can obtain identifying information about anyone using the Internet. There is no review by a judge or a magistrate; the clerk's office simply issues the subpoena in ministerial fashion. This identifying information can then be linked to particular material sent or received over the Internet, including e-mails, web browsing activity, chat room postings, and file-sharing activity. It is also important to remember that the threshold for a claim of copyright in any form of expression is extremely low. This subpoena power applies not just to sound recordings, it applies to the expression contained in an e-mail or posting in a newsgroup, digital photographs, and even pornographic materials. It has and will be used and abused by parties far less responsible than the recording or movie industries. In essence, any private party willing to assert a property right in any form of expression is constituted as their own roving grand jury, without any of the normal checks and protections that apply to governmental investigations.

Under our constitutional scheme, the issuance and enforcement of judicial process in civil cases is generally confined to an actual case or controversy and is undertaken under judicial

supervision. The district court's reading of Section 512(h) departs from this constitutional tradition and thus eliminates many of the normal constraints on discovery by civil litigants. The statute lacks the most basic protections that are applied to the discovery of confidential and personal data connected with expressive activity. As noted above, the filing that need be made is truly minimal, and is below the notice pleading standard for the filing of a civil complaint in federal court. The normal duties to investigate and substantiate a civil claim that apply to the filing of a lawsuit under the Federal Rules of Civil Procedure do not apply. The clerk's office simply rubberstamps these subpoenas in ministerial fashion--with no inquiry into the bona fides of the party filing the request or the self-interested "belief" that a copyright has been violated. The individual subscriber, whose identity is at issue, is not even entitled to receive notice of the subpoena before his or her personal information is turned over to a third party. Thus, the subscriber, who may in fact be engaged in fully protected speech or association, will have his or her identity revealed without ever having an opportunity to be heard in court. There is no opportunity to assert the normal defenses to a claim of copyright infringement--fair use, the non-protection of ideas, or the fact that material resides in the public domain. Nor is there any provision for damages or other punishment for wrongfully obtaining or misusing the identity of a subscriber subject to such a subpoena. It is truly ironic that Congress has placed more substantial requirements and protections on law enforcement access to confidential information regarding electronic communications than apply to a private party under this statute.2 Given the substantial privacy protections that Congress built into the DMCA itself, see 17 U.S.C. § 1205 (savings clause for state and federal privacy laws); id. § 512(m) (protection of subscriber privacy

2 See, e.g., 18 U.S.C. § 3121, et seq. (pen registers and trap and trace devices limited to governmental personnel upon court order for valid criminal investigation); 18 U.S.C. § 2703 (limits on disclosure of records
pertaining to electronic communications services).

from monitoring of Internet communications) it is utterly implausible that Congress wished to create this substantial threat to personal privacy in the subpoena provision contained in the same statutory scheme.

This combination of unlimited scope, minimal substantive requirements, and lack of judicial supervision makes both mistakes and intentional abuses of this new power inevitable. Every time you send an e-mail, browse a website, or join a discussion in a chatroom or newsgroup, others gain access the numerical IP address that you are using. Armed with this IP

address, anyone to whom you have sent an e-mail, from whom you have received an e-mail, with whom you or your children have spoken in a chat room, or who operates a web site you have visited, no matter how sensitive the subject matter, can unlock the door to your identity.

This list is not limited to those with legitimate interests in enforcing copyrights. As safety and privacy groups like the National Coalition Against Domestic Violence and WiredSafety stated in our litigation, it opens the door to your identity to people with inappropriate or even dangerous motives, such as spammers, blackmailers, pornographers, pedophiles, stalkers, harassers, and identity thieves. In fact, over 92 diverse organizations, representing consumer and Internet interests, submitted letters to this Committee last week expressing serious concerns about the privacy, safety, and security of Internet users arising from the potential misuse of this subpoena process. These include the ACLU, the American Library Association, the Consumer Federation of America, and the National Coalition Against Domestic Violence. These groups do not condone copyright infringement rather, like Verizon, they are concerned that this subpoena provision will cause great harm to privacy, free expression, and even personal security of Internet users with little gain in copyright enforcement.

- 6 -

As Ms. Aftab, from WiredSafety states, "With one broad sweep, the DMCA subpoena power will frustrate the work of the entire online safety community to arm our children and their parents with cyber-street-smarts. It won't matter what they voluntarily or mistakenly give away. All the information predators need can be obtained far more easily with the assistance of the local Federal District Court Clerk." The potential for abuse of this new subpoena power is limited only by the deviousness of the criminal mind.

Indeed, just since the district court's ruling went into effect in June, the evidence of mistakes, potential abuses, and troubling uses of this subpoena power has continued to mount. SBC recently filed a suit in California against the Recording Industry, a copyright bounty hunter called "MediaForce" and an entity called Titan Media Group. Titan Media, a purveyor of pornographic videos over the Internet, sent one subpoena to SBC seeking the names, addresses and phone numbers of 59 individual subscribers who Titan asserted were infringing its copyrights in gay pornographic videos by exchanging them over the Internet. Titan eventually withdrew the subpoena when SBC threatened a court challenge, but the episode highlights the fact that this new subpoena power applies to anyone who can claim an interest in any form of expression. In a similar vein, ALS Scan, a purveyor of graphic Internet pornography, has also used the DMCA notice and takedown process and in fact submitted a declaration in favor of RIAA's broad interpretation of the subpoena power in the litigation with Verizon. The potential for abuse, for invasion of personal privacy, for reputational harm, and even for blackmail is highlighted by these examples.

The statute does not even require the copyright owner itself to obtain the subpoena, it may be obtained by an agent of the copyright holder. A whole industry of copyright "bounty hunters" has sprung up, enterprises that search the Internet for possible instances of copyright

- 7 -

infringement spurred on by economic incentives. The use of automated robots, known as "bots" or "spiders" has also led to a significant number of mistaken claims of copyright infringement. These bots operate much like the spiders that crawled through buildings in the movie Minority Report, scouring the Internet in search of file names that look like they match the names of copyrighted works or artists. Bots are far from perfect. Typing words such as "Madonna" or "the police" in an e-mail may earn you a DMCA subpoena, because the "bots" cannot distinguish the legitimate comment or discourse from copyright infringement. In 2001,Warner Bros. sent a letter to UUNet demanding that they terminate the Internet account of someone allegedly sharing a Harry Potter movie online. The small text file was entitled "Harry Potter Book Report.rtf., with a file size of 1k. The file was not an unauthorized copy of the movie, it was a child's book report, but the bot could not tell the difference and such an "investigation" can quickly form the basis for a DMCA subpoena.

In the past few months, RIAA has already admitted numerous cases of "mistaken identity." In one case, RIAA demanded the take down of Penn State University's astronomy department's servers during finals week, based on a claim that it contained infringing songs by the artist Usher. In fact, "Usher" is a professor's last name and the file at issue was his own

creation. RIAA later admitted sending at least two dozen other mistaken notices to Internet users as part of its campaign to warn peer-to-peer file-sharers. And this was before RIAA began its new campaign sending hundreds of subpoenas for subscriber identity to ISPs across the country. These chilling examples all sound like excerpts from the book "1984," except in this case, "Big Brother" isn't the Government, it is interested parties armed with their own private search warrants.

- 8 -

RIAA's most recent campaign began in July of this year after the district court's ruling went into effect. Despite the pending appeal on this issue, the Recording Industry has chosen to unleash numerous subpoenas on Internet service providers. Verizon has already received nearly 200 subpoenas, with which we have been required to comply. The Recording Industry alone has sent well over 1000 subpoenas to service providers across the country, placing a significant strain on the resources of the clerk's office of the district court in D.C. and on the subpoena compliance units at many Internet service providers, including Verizon.3

RIAA now claims that it is entitled to discover subscriber's e-mail addresses through these subpoenas and further claims that it may issue these subpoenas from the district court in Washington D.C., regardless of the location of the service provider or the customer. Obviously, obtaining the subpoena in a distant forum makes it a practical impossibility for many service providers and most customers to ever raise any objection to the subpoena. Indeed, Boston College and MIT successfully fought to quash subpoenas issued out of Washington, D.C. that were aimed at their students in Massachusetts. SBC has filed a lawsuit in the Northern District of California seeking to have the entire process declared unconstitutional. Columbia University is also seeking to quash subpoenas that RIAA has attempted to serve on it issued by the District of Columbia courts.4

3 Indeed, press accounts indicate that the clerk's office of the district court in D.C. has been overwhelmed with subpoena requests and has been forced to reassign staff from other judicial duties. See Ted Bridis, Music Industry Wins Approval of 871 Subpoenas Against Internet Users, Associated Press (July 19, 2003) at 2 ("The RIAA's subpoenas are so prolific that the U.S. District Court in Washington, already suffering staff shortages, has been forced to reassign employees from elsewhere in the clerk's office to help process the paperwork, said Angela Caesar-Mobley, the clerk's operations manager.").

4 The Federal Rules of Civil Procedure generally provide for the issuance and service of subpoenas in the district where the party in possession of the material resides to protect the rights of third parties to contest the subpoena. See Fed. R. Civ. P. 45(a)(2) & 45(b)(2) (placing jurisdictional and service limitations on district court subpoenas for the protection of those from whom production is sought). Despite the fact that Congress expressly provided that the protections of Rule 45 should apply to Section 512(h) subpoenas, see 17 U.S.C. § 512(h)(6), RIAA has taken the position that it may obtain and serve a Section 512(h) subpoena from any district court in the country.

- 9 -

In Verizon's view, Congress never intended to unleash a massive wave of subpoenas on public and private Internet service providers and their customers. This is not an effective solution to the very real problems faced by copyright owners, it only creates an additional level of problems for Internet service providers and chills the free exchange of protected content over the Internet. The use of the subpoena power in an attempt to create an in terrorem effect over the entire Internet is both improper and disserves the long-term interests of both copyright owners and Internet service providers. When Congress enacted the DMCA in 1998, it outlined a set of carefully crafted take-down duties for material hosted by service providers. Service provider duties were carefully calibrated to the service providers' involvement with and control over the particular material asserted to be infringing. Congress created a subpoena power to identify only

those individuals who were directly linked to specific material residing on the service provider's network that could be "taken down." The language of the of the statute addressing the subpoena power makes three separate cross-references to notices and procedures that only apply in the context of material residing on a service provider's system or network.5 The subpoena provision was never intended to apply to materials residing on the user's hard drive, such as e-mails, instant messages, or shared files i.e., situations where the ISP is serving in a pure transmission or "conduit" role as described in the statute. By stretching the subpoena power to address a problem that was not before the Congress that enacted the DMCA, the district court has created a Frankenstein monster that Congress never contemplated and that has the potential to cause
(Continued . . .)
Thus, in its view, it could seek a subpoena from the district court in Guam targeting a small service provider in New
England.
5 See 17 U.S.C. § 512(h)(2),(4) & (5). Indeed, the statute provides that a subpoena may only issue if "the notification filed satisfies the provisions of subsection (c)(3)(A)," id. § 512(h)(4), a provision that only applies in the
context of material residing on a service provider's system or network. This limitation makes perfect sense in light
of the fact that infringing material available on websites was the principal problem before the Congress that passed
the DMCA in 1998.

irreparable damage to public confidence in the privacy of Internet communications. Given the concerns the Congress expressed throughout the DMCA regarding the protection of the privacy rights of individual Internet users,6 Verizon submits this is a clear perversion of Congressional intent.
Title II of the DMCA was designed to protect Internet service providers from copyright liability in order to promote the growth of the Internet as a medium of political, social, and economic exchange. But like the telephone itself, that medium depends upon the confidence of users in the privacy of their communications and communications habits. Every person in this room believes that his or her private e-mail or web browsing habits can and should remain private--yet the district court's erroneous decision in the RIAA matter has turned the DMCA into a direct threat to that privacy. It has also burdened Internet service providers with responding to thousands of subpoenas. From our own experience, we can tell you that RIAA's barrage of subpoenas has diverted and strained our internal resources. This new burden on service providers--responding to thousands of subpoenas issued in the conduit context--was never part of the statutory compromise embodied in the DMCA. It also threatens the limited resources of subpoena compliance units to satisfy legitimate law enforcement requests--as RIAA bombards service providers with dozens of subpoenas and purports to require responses on seven days or less notice. The protection of copyright, however legitimate a cause, should
6 See 17 U.S.C. §§ 512(m), 1205. See also S. Rep. No. 105-190, at 18 (1998) ("[T]he committee concluded that it was prudent to rule out any scenario in which section 1201 might be relied upon to make it harder, rather than
easier, to protect personal privacy on the Internet."). Ironically, the district court's decision in the RIAA case has
constituted Section 512(h) as a far greater threat to personal privacy on the Internet than any of the technological
copyright protection devices that the Committee was concerned about when it included Section 1205 in Title I of the
DMCA.

never be raised above law enforcement and national security efforts--efforts Verizon has always been in the forefront of supporting and cooperating with.
Both the district court in our case and the copyright owners have eschewed a more measured remedy that has always existed in the law and is used by numerous businesses for many purposes, the so-called "John Doe" lawsuit. Under this procedure, a judge or magistrate

reviews the merits of a case before a subpoena is issued, and the defendant is given notice and an opportunity to contest disclosure. The law demands a reasonable investigation of the relevant facts, ownership of a valid copyright registration, and a complaint filed in compliance with Rule 11. Verizon has successfully used this process to sue unknown spammers who abuse our network. Despite the Recording Industry's assertions to the contrary, the filing of a John Doe lawsuit is much more protective of all parties' interests than the DMCA subpoena process. Since RIAA launched its subpoena campaign, the DC Clerk's Office publicly complained that its internal resources were being burdened and the clerk's office had to re-assign new employees to the fulltime task of processing subpoenas on an ongoing basis. If the district court's decision in our case is not overturned quickly, it threatens to turn the Federal courts into free-floating subpoena mills, unhinged from any pending case or controversy, capable of destroying anonymous Internet communication, and threatening privacy and due process rights as well as public safety.

While Verizon firmly believes that this subpoena process and the tactic of targeting college students, universities, libraries and other individual Internet users is inappropriate and will lead to serious harms with little gain in copyright protection, Verizon recognizes that a more comprehensive and long-term solution is necessary. This Committee should promptly call the interested parties together, to negotiate and establish a balanced process that addresses the

legitimate needs of copyright owners while respecting the fundamental due process and privacy rights of Internet users, and recognizing the capabilities and limits of Internet service providers in policing content not under their control. Indeed, this Committee recognized in its report on the DMCA in 1998 that technological rather than legal solutions constituted the best method of ensuring the lawful dissemination of copyrighted works in our new networked, digital environment. See S. Rep. No 105-190, at 52 (1998) ("The Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age."). If some form of subpoena power is deemed necessary in conjunction with technological solutions, it must be more limited and contain substantial protections for both ISPs and their subscribers. Any compromise should include, among other requirements, notice to subscribers and an opportunity to defend against such subpoenas, a requirement that all the elements of copyright infringement be established, that the jurisdictional requirements of the federal courts be met, and that a judge approve any subpoena prior to its issuance, as well as penalties for any misuse of the subpoena process, full reimbursement of costs for Internet service providers, immunity for ISPs who provide customer information in response to valid subpoenas, and protection of confidential subscriber data from publication or other misuse. This Committee never had an opportunity to address and balance those interests in 1998 because the technologies at issue simply did not exist. It should do so now before irreparable damage is done to public confidence in the Internet as a medium of free expression and association.

I thank the Chair and the members of this Committee for your attention. We look forward to working with you to resolve this critical issue.