

[Ed. Note: Due to the rapidly changing nature of this area of law, some of the content in this paper may be outdated, and should not be relied upon for legal research or citation.]

RIAA v. Verizon Internet Services - Is the Safe Harbor Being Swamped?

Advanced Copyright Law

William Mitchell College of Law

Spring 2003

Kevin S. Brady

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL BACKGROUND	2
III.	DISCUSSION	3
	A. THE APPLICATION OF THE DMCA IN <i>RIAA</i> v. <i>VERIZON</i>	3
	B. POTENTIAL IMPLICATIONS OF <i>RIAA</i> v. <i>VERIZON</i>	8
IV.	CONCLUSIONS	16

I. INTRODUCTION

On January 21, 2003, the United States District Court for the District of Columbia significantly expanded copyright holders' ability to use subpoena power to compel Internet service providers ("ISPs") to disclose the identity of subscribers alleged to be engaged in peer-to-peer ("P2P") file sharing of music files.¹ In its decision, the court ordered Verizon Internet Services, Inc.² ("Verizon") to hand over to the Recording Industry Association of America³ ("RIAA") the identity of an alleged song-swapper believed to have downloaded and shared more than 600 song files.⁴ The court based its holding on its interpretation of a provision in the Digital Millennium Copyright Act ("DMCA")⁵, that the RIAA contended allows it and other content-owners to subpoena anyone suspected of downloading or trading songs over the Internet. Verizon argued, unsuccessfully, that it was merely acting as a "conduit" for users' content, and thus not subject to the subpoena power of the DMCA. This holding puts Verizon in a precarious position between liability for non-compliance under the DMCA and a potential privacy backlash for disclosing subscribers' personal information to any party that claims the subscriber has engaged in unlawful conduct. Verizon has since requested a stay in the order, pending appeal with the U.S. Court of Appeals for the D.C. Circuit.

¹ *In re Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24(D.D.C. 2003).

² <<http://www.verizon.com>>

³ <<http://www.riaa.org>>

⁴ *Id.*

⁵ Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 512 (1998).

This paper will attempt to examine *Verizon*,⁶ and some of its potential effect on copyright and Internet law. There are also some privacy issues inextricably connected to this issue that must be addressed.

II. FACTUAL BACKGROUND

In the summer of 2002, a subscriber of Verizon Internet Services went online and started downloading songs using the popular Kazaa⁷ music-swapping service, something that millions of people do every day. But in this instance, someone at the RIAA was monitoring the subscriber's activity. The information gathered by the RIAA amounted to a list of more than 600 song files residing on the subscriber's computer hard drive, and the subscriber's Internet protocol ("IP") address.⁸ On July 24, 2002, RIAA served a DMCA subpoena on Verizon demanding the identity of the anonymous subscriber.⁹ Verizon refused to disclose the subscriber's identity, arguing that the DMCA subpoena provision does not apply to service providers when the alleged infringing content does not reside on the provider's network or servers. Verizon claimed that since it merely provided the alleged infringer with an Internet connection, it falls under § 512(a), thus

⁶ *Verizon*, *supra* note 1.

⁷ <<http://www.kazaa.com>>.

⁸ Some P2P file sharing programs, including Kazaa, allow a person to "browse" the shared files folder or folders on another user's computer, enabling that person to identify the names and types of files shared therein. In addition, the programs often display the IP addresses of users. However, the actual identity of the user is not revealed, as users typically use pseudonymous "screen names" when configuring their P2P programs. There is no user registration of the program, and Kazaa does not have the identities of its users.

⁹ *Verizon*, *supra* note 1, at 9.

placing it outside § 512(h) subpoena authority, which Verizon contends applies only to service providers storing content under § 512(c).¹⁰

RIAA believed that the DMCA subpoena power applies to all service providers covered in subsections (a) through (d), including Verizon, and filed suit to compel enforcement of the subpoena.

III. DISCUSSION

A. THE APPLICATION OF THE DMCA IN *RIAA v. VERIZON*.

The DMCA provides “safe harbors”¹¹ for service providers, providing a shield from liability if the providers follow certain conditions for eligibility¹² stated in the Act. Section 512 limits liability of service providers for four types of activity stated in subsections (a) through (d). To qualify for safe harbor protection, the service provider must fulfill the conditions stated in one the applicable subsections, and the conditions set forth in subsection (i).¹³ For example, an ISP that provides web hosting services will not be held liable for infringing content posted by a subscriber on a hosted server if the service provider removes the allegedly infringing content after receiving notice

¹⁰ *Id.* at 12.

¹¹ 17 U.S.C. § 512.

¹² *Id.*

¹³ *Id.* See also *Verizon*, *supra* note 1, at 5.

of its existence.¹⁴ This type of action is referred to as “notice and takedown.”¹⁵

Under the DMCA, a “service provider” is defined as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by the user”¹⁶

The DMCA subpoena provision states that “[a] copyright owner or a person authorized to act on the owner’s behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.”¹⁷

The party requesting the subpoena need only provide a copy of notification described in subsection (c)(3)(A), a provision used under § 512 to notify service providers that infringing material resides on the provider’s system or network; a proposed subpoena; and a sworn declaration stating that the purpose of the subpoena is to identify the alleged infringer and that the information sought will only be used to protect rights under Title 17.¹⁸ The subpoena authorizes and orders the service provider to “expeditiously disclose” information sufficient to identify the alleged infringer.¹⁹

¹⁴ 17 U.S.C. § 512(e)(1).

¹⁵ See, e.g., *IDSA Takedown to Gnutella User*, Chilling Effects Clearinghouse, <http://www.chillingeffects.org>.

¹⁶ 17 U.S.C. § 512(k)(1).

¹⁷ 17 U.S.C. § 512(h).

¹⁸ *Id.*, at (2).

¹⁹ *Id.*, at (3).

The subpoena provision clearly authorizes the subpoena process for subscribers storing allegedly infringing content on a service provider’s system or network. However, Verizon argued that the provision does not apply in their case, as the subscriber sought did not actually store the content on Verizon’s system or network. Verizon argued that it was merely providing “Internet connectivity” or acting as a “passive conduit.”²⁰ Verizon argued that the subpoena provision under § 512(h) only applied in circumstances set forth in subsection (c), where infringing material is stored or controlled on the service provider’s system or network.²¹ Verizon thus maintained that since it had merely provided an Internet connection, it was not subject to subsection (h) subpoena power.²²

The court quickly dispatched Verizon’s “conduit” claims, holding that the broad definition in subsection (k)(1)(B) expressly applies to the term “service provider” as used in subsection (h), and that the narrow definition of subsection (k)(1)(A) only applies to the term as it is applied in subsection (a). But the court read the provisions as a whole, reasoning that the plain text of the statute provides that subpoena power under subsection (h) not only encompassed the broad coverage of (k)(1)(B) service providers, it also encompassed subsection (a) service providers.²³

²⁰ *Verizon, supra* note 1, at 22.

²¹ *Id.*, at 11.

²² *Id.*, at 17. Subsection (a) of § 512 protects service providers that are only supplying “transitory network communications.” This shield from liability only applies in certain instances where the service provider has neither initiated the transmission, selected the process or recipients involved, nor stored or maintained any copy of the material on the service provider’s system or network.

²³ *Id.*, at 17.

The court noted that the statute provides for an expeditious process: the purpose of the subpoena is intended only to quickly identify the subscriber, and not to terminate the subscriber's service.²⁴

As a practical matter, the court further maintained that the copyright holder cannot readily determine whether its infringed material was stored on or merely transmitted through the service provider's system, making it burdensome for the copyright holder to determine if it faces a subsection (c) or (a) situation in the first place.²⁵ The court also argued that, as a matter of policy, there was little sense in Congress limiting a copyright owner to obtaining information

regarding infringing material stored on a service provider's system, while simultaneously denying access to such information from a service provider transmitting the material over its system.²⁶

Finally, the court held that limiting the subpoena provision as asserted by Verizon "would create a huge loophole in Congress's effort to prevent copyright infringement on the Internet[,]” adding that “the largest opportunity for copyright theft is through peer-to-peer ... software.”²⁷

The court concluded its discussion of this issue by stating that Congress did not intend the DMCA to protect only a limited portion of copyrighted material on the Internet.²⁸ Therefore, the court reasoned, the subpoena authority extends to service providers under subsections (a) through (d), including Verizon.

²⁴ *Id.*, at 25.

²⁵ *Id.*, at 28.

²⁶ *Id.*, at 30.

²⁷ *Id.*

²⁸ *Id.*, at 32.

Two recent technological developments were addressed as underlying issues in *Verizon*. The RIAA raised concerns of the effects of peer-to-peer piracy; Verizon countered with its fears of inundation of service providers with thousands of computer-generated subpoenas resulting from online data collection by “bots.”²⁹ These two technologies were unknown to most of the public in 1998, when DMCA was enacted. However the court gave these concerns short shrift by deferring to Congress’s authority, stating that it should be left to Congress to “decide how best to pursue the objectives of the Copyright Clause.”³⁰ Thus, according to the court, the DMCA can anticipate new technologies, and later be applied to them.

Verizon asserted constitutional issues surrounding DMCA subpoena power, arguing that such power “raises substantial questions.”³¹ Specifically, Verizon contended that subsection (h) authority, if broadly construed, raises substantial questions of judicial power and First Amendment freedom of anonymous speech. Unfortunately, Verizon provided scant argumentation of these issues before the court, relying instead on amici curiae.³²

The court responded by stating that since Verizon failed to raise any explicit constitutional

²⁹ The Free On-Line Dictionary of Computing (“FOLDOC,” <<http://www.foldoc.org>>) defines “bot,” as “[a]ny type of autonomous software that operates as an agent for a user or a program or simulates a human activity.” Specifically, a bot as used on the Internet (also known as a “spider” or “crawler”) is a program used for searching. Bots access web sites, retrieve documents and follow all the hyperlinks within them, and generate catalogs.

³⁰ *Verizon*, *supra* note 1, at 42.

³¹ *Id.*, at 51.

³² *Id.*

challenges, such issues were not properly before the court.³³ The court further stated that even if it were to consider the issue, the constitutional problems facing service providers or their subscribers would remain the same under Verizon's narrow interpretation of the DMCA as well.³⁴ The court reminded that the First Amendment does not protect copyright infringement, and that previous challenges to injunctions from copyright infringement have been rejected.³⁵ The court reasoned that since the Ninth Circuit was twice able to shut down Napster³⁶ without any First Amendment violations, there could be no protected expression in Verizon's subscriber downloading and transferring 600 copyrighted recordings.³⁷

B. POTENTIAL IMPLICATIONS OF *RIAA v. VERIZON*.

Verizon has now requested a stay of the District Court's motion, and that court is reviewing briefs regarding that stay. Verizon will appeal the decision to the Court of Appeals for the District of Columbia Circuit (CADDC). At the time of this writing, the CADDC has scheduled dates for submission of briefs.

³³ *Id.*, at 52.

³⁴ *Id.*, at 53.

³⁵ *Id.*, at 54.

³⁶ *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2001); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001).

³⁷ *Verizon*, *supra* note 1, at 57.

Upon analyzing *Verizon*, it appears easy to conclude that the District Court, for the most part, properly interpreted the DMCA as it applied to the facts. Nevertheless, critics of the decision argue that the statute can be read in a much different light.³⁸ In addition, many who oppose the decision also believe that the statute itself is flawed, believing it to be a threat to privacy and free expression.³⁹ Representatives of Verizon and various industry and advocacy groups have issued a flurry of declarations and *amicus* briefs to the District Court in support of Verizon's motion for a stay, with the RIAA filing its oppositions.⁴⁰ The argument of these filings gives much weight to the constitutional and privacy challenges to the DMCA, in addition to criticism of the court's reasoning. Even if one were to concede for the moment that *Verizon* was a fair interpretation of the DMCA provisions, the focus still must turn to some of the troubling aspects of the statute itself.

If the District Court's decision in *Verizon* is upheld, many content owners will no doubt greatly utilize subsection (h) subpoena power to enforce compliance. There are two functional problems that can arise from this that must be addressed. First, "legitimate" subpoena requests could be unleashed upon ISPs *en masse*, potentially overwhelming the limited resources of service providers. Second, the subpoena power can easily be abused, due to the DMCA's inherent lack of judicial oversight in the filing process.

³⁸ *In re Verizon Internet Services, Inc.*, Subpoena Enforcement Matter, Motion and Memorandum of Points and Authorities in Support of Verizon Internet Services, Inc.'s Motion for a Stay Pending Appeal, Miscellaneous Action Case No. 1:02MS00323 (JDB)(D.D.C Jan. 31, 2003), at 5.

³⁹ *Id.*, at 7.

⁴⁰ An updated archive of the *Verizon* litigation documents filed can be accessed in downloadable .pdf format at <http://www.eff.org/Cases/RIAA_v_Verizon>.

With the advent of the Internet and high speed personal computers, the ability to scour on-line sources for data is well within the reach of many. Internet “bots” can quickly retrieve and sort vast amounts of information. The large-scale collection of data regarding peer-to-peer users can easily be accomplished. Anyone wishing to identify large numbers of alleged P2P infringers could therefore file a single request for multiple DMCA subpoenas against a service provider. It would certainly be much more efficient for content owners to bundle such requests all at once, rather than targeting suspected infringers one at a time. This becomes a legitimate concern for service providers, since the provision requires the provider to “expeditiously disclose to the copyright owner ... the information required by the subpoena”⁴¹ The contemporaneous service of thousands of subpoenas would place an enormous burden on service providers, entities whose resources and margins are already spread paper-thin by the current slump in the telecommunications business. One critic of the *Verizon* holding even described DMCA subpoenas as possibly becoming “the New Spam, flooding the in-boxes of ISPs.”⁴² The DMCA subpoena provision becomes an important tool for content owners. With such a large “hammer” available to content industries, every perceived problem could start looking like a nail.

The second problem presents potentially more sinister consequences. Abuses of the subpoena process by content owners, or perhaps others masquerading as content owners, would create

⁴¹ 17 U.S.C. § 512(h)(5).

⁴² *In re Verizon Internet Services, Inc.*, Subpoena Enforcement Matter, Declaration of Peter P. Swire, in Support of Verizon Internet Services, Inc.’s Motion for a Stay Pending Appeal, Miscellaneous Action Case No. 1:02MS00323 (JDB)(D.D.C Jan. 30, 2003), at ¶ 7. (Mr. Swire is a Professor of Law at the Moritz College of Law of the Ohio State University).

serious privacy breaches. Recall that obtaining a DMCA subpoena requires only a modicum of evidence from the requesting party, and that there is no judicial oversight to the process.⁴³ The subpoena provision, as interpreted by *Verizon*, allows ample room for one to seek information for non-copyright related purposes.⁴⁴ It is not difficult to imagine someone requesting a subpoena under the guise of copyright enforcement, only to use the information to pursue another cause of action, such as a libel claim. Another possibility of abuse could involve a party requesting a DMCA subpoena to obtain personal information about an Internet user.

Internet service providers do not want to alienate customers by policing them on behalf of copyright owners. On the other hand, the cost of DMCA non-compliance by service providers would be more than most would be willing to pay. Not all ISPs have the tenacity or resources to fight the subpoena process as *Verizon* has. Quite likely, many service providers would quickly hand over the identities of their subscribers, rather than risk a court battle. Realizing this, on-line users might be reluctant to partake in certain activities, lest they become the targets of content owners' wrath. Such situations would result in a chilling effect upon on-line expression, and a curtailment of a user's expectation of privacy.⁴⁵ Due to the broad scope of copyright protection,

⁴³ 17 U.S.C. § 512(h).

⁴⁴ Although paragraph (2)(C) of § 512(h) requires from the requesting party a sworn declaration stating that the purpose of the information sought is to pursue protecting Title 17 rights, it would not be difficult for a party to obtain a subpoena under fraudulent pretenses, due to the very low threshold of oversight provided for in the statute. The clerk of the court, having little reason to doubt the statements made, would be compelled to issue the subpoena.

⁴⁵ Motion and Memorandum, *supra* note 38, at 7. In *Verizon's* motion for stay, it was argued that Congress was concerned with interests of Internet users in their freedom of expression and privacy, and that a user's expectation of privacy is greater for material stored on the subscriber's own personal computer at home than for material placed on an external service provider's system.

the types of entities that could enforce their rights would be virtually limitless. Any plaintiff with protectable copyright interests could find cause to seek subpoena action against any on-line user the plaintiff has deemed a threat to its rights, with no judicial oversight to protect the on-line user.⁴⁶ Furthermore, the broad construction of the DMCA's definition of "service provider"⁴⁷ leaves ample room to encompass other entities that provide Internet connectivity.⁴⁸ The information systems within businesses, schools, and other institutions could be classified as service providers under the DMCA, and thus subject to subpoena power. When served with a DMCA subpoena, an institution would be compelled to turn over the names and other information regarding its allegedly infringing employees. It also follows that the institution would be required to comply with the notice and takedown requirements⁴⁹ of the DMCA and pull the plug on such employees' Internet access. This poses some rather delicate possibilities, with the employer being thrust into the position of copyright enforcer, and the employees having misgivings about the

⁴⁶ Consider the recent case of FatWallet.com. FatWallet, a consumer price-comparison website popular with bargain-hunters, allows individuals to post information regarding sales prices, product reviews, and other consumer information. In November, 2002, several individuals anonymously posted sales circulars from approximately a dozen major retail chains, including Wal-Mart, onto FatWallet's site. These postings revealed, two weeks before their planned release, product prices for goods to be placed on sale the day after Thanksgiving, considered to be the most profitable shopping day of the year for retailers. Wal-Mart and the other retailers were not amused, demanding that FatWallet remove the postings, under the premise that the postings constituted copyright infringement. In addition, Wal-Mart filed a declaration in federal court to obtain a § 512(h) subpoena ordering FatWallet to identify the persons who posted the Wal-Mart sales information. After a law clinic at the University of California at Berkeley agreed to represent FatWallet and fight the subpoena, Wal-Mart abandoned its subpoena request. *See, e.g.,* Declan McCullagh, *Wal-Mart Backs Away From DMCA Claim*, CNET News.com, December 5, 2002, <<http://news.com.com/2102-1023-976296.html>>.

⁴⁷ 17 U.S.C. § 512(k)(1).

⁴⁸ *In Re: Aimster Copyright Litigation*, Master File No. 01 c 8933, Multi District Litigation #1425 (N.D. Ill. 2002). "A plain reading of both definitions reveals that "service provider" is defined so broadly that we have trouble imagining the existence of an online service that *would not* fall under the definitions."

⁴⁹ 17 U.S.C. § 512(c)(1)(C).

legality of their online activities. An activity as seemingly innocuous as performing scientific research⁵⁰ or writing a review of software⁵¹ could put a user at risk.

There is room for argument that DMCA subpoena power, lacking the judicial oversight present in ordinary subpoena duces tecum, may violate a user's Fourth Amendment rights to an expectation of privacy.⁵² The U.S. Supreme Court has held that people have "the right ... to be secure in their ... houses, and ... that the home is entitled to special protection as the center of the private lives of our people."⁵³ However, in *U.S. v. Miller*,⁵⁴ the Supreme Court held that "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."⁵⁵ However, the *Miller* Court conceded that the Fourth Amendment might guard against abuse of subpoena power by way of "too much indefiniteness or

⁵⁰ See Electronic Frontier Foundation, *Unintended Consequences: Four Years under the DMCA*, January 9, 2003 <http://www EFF.org/IP/DMCA/20020503_dmca_consequences.pdf>. This article summarizes many of the instances of chilling effects due to various provisions of the DMCA. One particular instance involved the research performed by Princeton Professor Edward Felton, and his team of researchers. After being encouraged by a public challenge issued by the Secure Digital Music Initiative (SDMI), Professor Felton and his team succeeded in "cracking" the watermarking technology used in protecting digital music. However, when Professor Felton attempted to present the team's findings at an academic conference, representatives of SDMI threatened the researchers and Princeton University with liability under the DMCA. The researchers reluctantly backed down, but were later able to publish portions of the research findings. *Id.*, at 2.

⁵¹ *Id.*, at 5, discussing the case of the Slashdot forum, where users posted Microsoft's published specifications regarding one of its server software products. Microsoft invoked the DMCA, demanding that Slashdot removed the posted material.

⁵² *Rakas v. Illinois*, 439 U.S. 128 (1978), at 143 (citing *Katz v. United States*, 389 U.S. 347 (1967)).

⁵³ *Minnesota v. Carter*, 525 U.S. 83 (1998), at 99 (Kennedy, J., concurring).

⁵⁴ 425 U.S. 435 (1976).

⁵⁵ *Id.*, at 443.

breadth of the things required to be ‘particularly described.’”⁵⁶ This concession might be useful to Verizon on appeal: that the DMCA subpoena provision is indefinite and/or over-broad in its scope of information sought. The breadth of potential infringing content on users’ personal computers is vast. A party could request a DMCA subpoena to go looking for just about anything copyrighted.

Verizon maintains that the § 512 subpoena power presents serious constitutional questions, as it does not require the filing of an Article III lawsuit prerequisite to obtaining the subpoena.⁵⁷ In an Article III lawsuit, a plaintiff is required to meet certain burdens under the Federal Rules of Civil Procedure. These include demonstrating that the plaintiff’s “allegations ... have evidentiary support,” or “are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery,”⁵⁸ that the court has jurisdiction over the controversy,⁵⁹ and that the plaintiff can “state a claim upon which relief can be granted.”⁶⁰ If the party filing the complaint does not meet Rule 11 evidentiary standards, that party is subject to sanctions.⁶¹ Section 512 provides no such evidentiary standards, nor does it provide any sanctions for abuses, despite the

⁵⁶ *Id.*, at 445 (citing *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946)).

⁵⁷ Motion and Memorandum, *supra* note 38, at 7.

⁵⁸ Fed. R. Civ. P. 11(b)(3).

⁵⁹ *Id.*, at 12(b)(1).

⁶⁰ *Id.*, at 12(b)(6).

⁶¹ *Id.*, at 11(c).

provision's clause invoking the Federal Rules of Civil Procedure.⁶² Under the DMCA, the only statement that must be made under penalty of perjury is that the complaining party is authorized to act on behalf of the alleged copyright owner.⁶³ Such a low threshold of proof means that a complaining party is held to a low standard regarding the allegations it makes. No Article III "case or controversy" is required; only the complainant's allegations are needed to dispatch a subpoena - without any civil procedural bounds. The complaint may be completely baseless, yet there is no Rule 12(b)(6) protection that, *in any other circumstance*, would dismiss such a claim. There are no mechanisms in place to quash a bad faith DMCA subpoena. There are no Rule 11 sanctions to punish those that abuse the subpoena process or to discourage others from abusing it. By the time it is determined that a DMCA subpoena is defective, based on erroneous information or having been requested in bad faith, it is too late. The target of the subpoena has suffered a breach of privacy, and has no recourse against the complainant. Content owners are free to engage in fishing expeditions by serving DMCA subpoenas against anyone they even suspect of possessing or distributing copies of their content.

The court's reasoning in *Verizon* has its flaws, not the least of which being the quick dismissal of

⁶² 17 U.S.C. § 512(h)(6). This subparagraph mandates that the DMCA subpoena provision "shall be governed *to the greatest extent practicable* by those provisions of the Federal Rules of Civil Procedure..." (emphasis added). However a cursory examination of the language of the subpoena provision allows little room for Rule 12 defenses or Rule 11 sanctions for abuses. The term "greatest extent practicable" in the FRCP governance provision does not give the impression that the FRCP will necessarily apply in any case, despite the *Verizon* court's acknowledgment of the provision, in which the court offered that service providers "can resort to the Federal Rules, including Fed.R.Civ.P. 45 ... for quashing subpoenas." *In re Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24(D.D.C. 2003), at 58. There is little consolation in that opinion, as it is difficult to envision how a recipient of a DMCA subpoena could adequately protect himself procedurally with the looming possibility of losing safe harbor protection for non-compliance.

⁶³ 17 U.S.C. § 512(c)(3)(A)(vi).

the privacy issues,⁶⁴ discussed above. One such flaw is the court’s logic of consolidating subsection (a) transitory activity with subsection (c) activity involving information residing on the systems. This becomes readily apparent when one analyzes the transitory activity in respect to “take down” notification, as required in obtaining a subpoena. Since a transitory service provider is not storing the alleged infringing content, and cannot identify the existence of such material, it has no means of removing it. Thus, a transitory ISP could only terminate a subscriber’s account. Since the notice requirement refers to the removal or disabling of material, and not termination of a subscriber’s account, this seems to indicate that subsection (a) transitory activity was not covered by the subpoena provision.⁶⁵ Of course, it could be argued that this a mere statutory anomaly; indeed the supporters of Verizon have conceded this.⁶⁶ But since the trial court gave such weight to the “plain language” of the statute,⁶⁷ it follows that this “anomaly” should be examined upon appeal.

IV. CONCLUSIONS

The holding in *Verizon* seems to interpret the DMCA fairly well, though it has some arguable flaws. This author has some difficulty reconciling how the trial court rolled subsection (a)

⁶⁴ *Verizon*, *supra* note 1, at 52.

⁶⁵ Motion and Memorandum, *supra* note 38, at 6.

⁶⁶ *Id.*, at 7.

⁶⁷ *Verizon*, *supra* note 1, at 14. “We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.”

transitory activity together with subsection (c) storage. It is difficult, if not impossible, for a service provider to identify data that is not stored on its system. Therefore, how can the provider remove or disable such material? In this case, the service provider can only terminate the user's account, which is inconsistent with the statute's take-down notice prerequisite to allowing a subpoena to issue.

The subpoena provision of the DMCA is not without its problems. A system of granting subpoena power to parties without judicial oversight, without a requirement of a "case or controversy," without a requirement of evidentiary standards, and without any threat of sanctions is a blank check for abuse. The subpoena power may be indefinite or over-broad, sparking Fourth Amendment privacy concerns. This system, coupled with content owners' ability to gather data on large numbers of alleged infringers, means this abuse can become widespread. It seems inevitable to this author that abuse of DMCA subpoena power will adversely impact many people. While the rights of copyright owners must be protected, this should only be accomplished in the same procedural manner that any other rights are protected. At the same time, Internet service providers should not be unduly burdened with mass requests for subpoenas requiring prompt disclosure of numerous customers. Service providers are not in the business of being the copyright police, nor should they be.