



No, Mr. Solicitor General, We *Do NOT* Want to Live in Your World

Author _ Andrew Gallo (agallo@gwu.edu), The George Washington University.

Author _ Anita Nikolich (anitan@illinois.edu), School of Information Sciences,
University of Illinois–Urbana Champaign.

In 2018, Sony Music Entertainment, representing 50 other music industry plaintiffs, sued Cox Communications in the Eastern District of Virginia for copyright infringement. A jury found that Cox had contributed to the infringement of over 10,000 copyrighted works and awarded the plaintiffs over \$1 billion in statutory damages.

In December 2025, the US Supreme Court heard oral arguments that raised fundamental questions about the role of network operators in enforcing copyright law. There are numerous articles that do a fine job of detailing the legal issues in the case. This is not one of them. The authors are not lawyers, and this is not a legal analysis. Rather, this article examines the role of network operators in the protection of intellectual property by way of analyzing an argument made by Solicitor General Malcolm Stewart.

How We Got Here—DMCA and Safe Harbors

The Digital Millennium Copyright Act of 1998 is the US implementation of the 1996 World Intellectual Property Organization’s 1996 Copyright Treaty and Performances and Phonograms Treaty. The act established “safe harbors” for providers of internet services to relieve them of responsibility for the behavior of their users.

Section 512 of the act defines four categories of service providers: “mere conduit,” caching, hosting, and linking. A mere conduit provider is one that provides automatic transmission of data, at a user’s request, without modification of that data—essentially, an internet service provider (ISP). The other three categories involve storing content for

some length of time, something ISPs do not do. Acknowledging these fundamental differences between ISPs and other types of providers, the DMCA establishes different requirements for each category to qualify for safe-harbor protection.

ISPs are generally *not* liable for infringing activity of their customers based on 17 USC § 512(a). Courts are still defining exactly what this means, but, generally, as long as the ISP (as an organization) or its employees are not the source or destination of the allegedly infringing traffic and the traffic was neither modified nor stored, the ISP is not involved in the alleged infringement activity. A recent decision from the Ninth Circuit found that because an ISP cannot *remove* content (in the same way, say, a website hosting provider can), ISPs are not liable for infringement nor do they need to respond to subpoenas requesting the identity of alleged infringers.

Universities and Internet-Based Copyright Infringement

Higher education institutions have a checkered history when it comes to network-based copyright infringement. To understand why, remember what the online world was like in 1999. If US households had internet access at all, it was likely dial-up or low-speed broadband like Digital Subscriber Line (DSL), with speeds in the 10s to 100s of kilobits per second for most users. At colleges and universities, however, things were different. As early developers and adopters of network technologies, these institutions provided students, faculty, and staff with always-on network connections in the 10s to 100s of megabits per second. This difference is more than



just quantitative. University and lab environments are where internet applications transitioned from barely functional novelties to a rich, immersive, and useful part of daily life.

It was in this environment that Napster launched in 1999, followed shortly thereafter by the Apple iPod. Napster was an innovative and groundbreaking peer-to-peer file-sharing system that enabled content sharing on a scale imaginable only in the worst nightmares of the Recording Industry Association of America (RIAA) and the Motion Picture Association (MPA). Unfortunately, the ground it broke involved massive sharing of copyrighted media, primarily music files encoded in the then-new MP3 format, which made them easy to copy and distribute. Napster shut down in 2001 after a series of successful lawsuits against the company.

There is no doubt that residential users were also experimenting with their new broadband connections. But it was at US higher education institutions where the Napster bomb truly went off. This did not go unnoticed by rights holders.

Many schools invested extensive financial, operational, and human resources attempting to block Napster and other file-sharing applications, using technologies such as packet shaping, filtering, network usage reporting, and firewalling. The efficacy of trying to solve this problem in the network has always been questionable.

As alternative and legitimate means of accessing media, such as commercial streaming services, became widely available, users shifted toward authorized outlets for content.

It is therefore not surprising that universities were prominently featured several times during the Supreme Court arguments in this case. In fact, universities were mentioned within the first two minutes of Mr. Clement's opening argument for Cox and were referenced a total of 25 times throughout the oral arguments.

The Solicitor General's "Solution" to Copyright Infringement

Deputy Solicitor General Malcolm Stewart, arguing on behalf of the United States as an amicus for Cox Communications, engaged in a bit of live and ad hoc network engineering during oral arguments.

At about the 75-minute mark, in response to a hypothetical posed by Justice Alito concerning how an ISP should handle an infringement complaint involving a multiuser account, say, a university with tens of thousands of users, Mr. Stewart had this to say:

I don't think it would be the end of the world if universities provided service at a speed that was sufficient for most other

purposes but didn't allow the students to take full advantage of BitTorrent. I could live in that world.

Before dissecting this argument, we have to give anyone arguing before the Supreme Court some leeway. The justices can interrupt at any time and ask any question—a lawyer needs to be an incredibly skilled rhetorician and an expert in both the case at hand and a long list of previous cases used as precedent, along with legislative history, regulatory action, and so forth.

However, Mr. Stewart's attempt to create a world free of copyright infringement through service degradation is too extreme to ignore.

Let's first get the BitTorrent issue out of the way. BitTorrent is an application and protocol that allows for efficient content sharing by using peer-to-peer distribution rather than server-to-client distribution. The application is not illegal. The protocol is not illegal. Using it to download legal content is not illegal. Suggesting otherwise is simply wrong. There are lots of legal and legitimate uses of BitTorrent.

Additionally, the DMCA process is simply the *allegation* of infringement, often made by a third party hired by copyright owners. The economic incentives in this process are questionable at best.

Even if we set that aside, there's a more insidious implication in Mr. Clement's solution for universities—that *all* users' network experiences should be deliberately degraded to discourage or prevent possible infringement by a few.

For practical reasons, this approach is unworkable. First, all types of works, not just large media files like video, are copyrighted. To truly prevent unauthorized copying, one would need to reduce network speeds to levels incompatible with modern internet usage. As an example, a short news article can easily be less than several hundred words, a few thousand bytes. Even with ARPANET's first implementation at 50k bit/s, this file could be shared quickly and easily without the owner's approval. We might need to revert to France's optical telegraph or the first transatlantic submarine cable, with capacities measured in bits per second, in order to satisfy Mr. Clement. This is absurd beyond comparison. Even if we ignore "small" copyrighted works, dealing only with lucrative movie piracy (as if that would be a defense if being accused of infringing on such works), a three-layer, Ultra-HD Blu-ray, at about 100 GB, can be sent over a 1- to 2-Mbps link in a matter of days. These speeds are absolute minimums for videoconferencing applications. There are no speeds that are sufficient for most other purposes but not for copyright infringement.



The speed silliness aside, the argument rests on the assumption that all users should have their service degraded because of the potential misuse of the network by a few. It puts the protection of copyright above all else. Such a scheme would push service far below the Federal Communications Commission's definition of *broadband*. At that point, students would lose reliable access to digital news, legitimately licensed streaming media, cloud-based tools, and real-time collaboration platforms—along with videoconferencing, remote instruction, and research workflows that assume modern bandwidth and latency characteristics. This would cut users of the university's network off from modern society.

There are some second-order consequences of throttling university networks. The solicitor general's suggestion ignores the fact that many universities operate safety-critical infrastructure, including hospitals, research facilities, and emergency services. Most campus networks have a converged infrastructure, combining phones, building management systems, elevator emergency phones, and so forth. In attempting to mitigate copyright liability, a university would knowingly introduce foreseeable risks that carry far greater legal consequences.

Universities remain culturally distinct from commercial ISPs. Network infrastructure is instrumental to their mission, and, as such, universities have always been extremely cautious about terminating network access. A policy that deliberately throttles the network directly interferes with research workflows. It also raises operational complexity and costs, which are not offset by reducing copyright liability. Practical questions also arise, such as whether research labs should be treated the same as dorms.

The DMCA Was Created Broken

The DMCA's safe-harbor provisions were always imperfect. Given the scale of modern networks, the requirement to respond to individual infringement notices and terminate "repeat infringers" (a term the statute never clearly defines) is next to impossible. The multiuser-account problem makes this even worse. Universities can have tens of thousands of users on a shared network infrastructure with a single account. In these cases, whom do you punish?

Terminating an entire university's internet access over one user's infringement is hardly realistic and would punish thousands of innocent users for one person's actions. Treating network throttling as an enforcement tool does not fix

the DMCA but rather replaces it with something Congress never authorized.

Also, most network data is encrypted, making content visibility and attribution next to impossible. Even if suppressing the use of applications like BitTorrent were feasible, virtual private network (VPN) usage easily obfuscates the app usage.

Where Does This Leave Us?

DMCA Clarity Advocacy

Universities need to press for a clearer legal/ judicial definition of the term *repeat offender*, which would lead to more easily targeted responses to problem offenders.

DMCA as a Compliance-Based Role

What is a reasonable role for a network operator in an encrypted, multiuser environment? DMCA safe harbors were designed to limit liability, not police traffic. Universities are not content hosts, and they cannot be content inspectors. Rather, they should maintain a registered DMCA agent to accept notice-and-response processes, respond to valid notices, take the position of escalating user interventions internally, and avoid proactive monitoring.

Enforcement of copyright liability must be decoupled from network/ traffic engineering. Networks should remain mission oriented and available for researchers, staff, and students. Proactive monitoring, traffic inspection, or protocol-based throttling is neither technically reliable in an encrypted environment nor authorized by the DMCA.

In practice, the solicitor general's suggestion would substitute collective punishment for individualized accountability, imposing broad harm on lawful users to deter alleged or hypothetical misconduct by a few. That approach is incompatible with the educational mission of universities, inconsistent with national broadband policy, and wholly disconnected from how modern internet applications—and modern society—actually function.

Protection of intellectual property is such an important part of society that it is established in Article I of the US Constitution. Congress has recognized the importance of promoting and protecting useful and creative works. The current situation, however, is skewed too far to the protection of rights holders, and with suggestions like Solicitor General Stewart's, it is possibly getting worse. We can do better.