

Contaminated P2P Networks: They Threaten Both Educational Institutions and Their Students

Popular file-sharing programs like LimeWire or Morpheus have caused over 26,000 Internet users—many of them college students—to be sued for copyright infringement. These programs have also led to multiple breaches of national, military, corporate, and personal security and widespread identity theft.

Colleges, universities and their students are all too familiar with some of the risks and costs imposed by these programs. But others—like the threat of inadvertent sharing of sensitive student or university records—have only recently been identified and explained. As a result, this paper will note threats that are probably familiar and then focus on a new threat—*inadvertent* sharing—that has profound implications for colleges that have *never before* been identified or explained.

The Devils You Probably Know: Lawsuits and Malware.

Students Almost Invariably Use File-Sharing Programs Unlawfully: Colleges and universities receiving cease-and-desist letters, pre-litigation letters, or subpoenas from copyright holders probably know that many of their students use file-sharing programs for unlawful copyright infringement. But the true prevalence of unlawful uses of these programs is staggering: In 2006, the federal court adjudicating the famous *Grokster* case found that 97% of the files *actually downloaded* by users of file-sharing programs were, or were highly likely to be, infringing—97%.

In short, 97% of the actual uses of these programs were unlawful and subjected their users to risks of crushing damages or criminal prosecution. And those risks are very real:

- *Thomas*: Civil damages of \$222,000 against a woman who illegally shared 24 songs.
- *Gonzalez*: Civil damages of \$750 per song downloaded.

- *Operation Digital Gridlock*: Criminal prosecution and conviction of DirectConnect hub administrators.
- *Chan*: Criminal conviction of a BitTorrent user sharing infringing files.

All of these cases also have one thing in common: In *none* could the defendant have avoided liability by showing that he or she had also used a file-sharing program for some *lawful* purpose 3% of the time. Consequently, the *Grokster* finding of 97% unlawful use is critical to institutions trying to assess and manage the risks—and the virtually non-existent benefits—of these programs.

Users Will Inevitably Download Malware-Ridden Files: The same factors that make file-sharing networks well-suited for infringing use also make them well suited to the needs of those who distribute malicious programs: SafeMedia's survey of the most recent studies on the prevalence of malware-infected files indicate that 15-45% of all popular downloads are malware-infected and 60-68% of executable or archived files are infected. Consequently, unrestricted use of contaminated file-sharing programs will ensure that network administrators and IT specialists will face a constant inflow of worms, viruses, Trojan-horses, and backdoors.

The Devils You May Not Know: Inadvertent Sharing of Student's Personal Files and Institutions' Educational Records.

As early as 2002, computer-science researchers showed that defects in file-sharing programs were causing their users to inadvertently "share" so many sensitive personal files that identity thieves had begun to data-mine these networks for inadvertently shared credit-card numbers. In 2003, program distributors claimed that they had remediated this problem. In 2007, the world learned that their claims were woefully wrong.

In March of 2007, the U.S. Patent and Trademark Office (USPTO) released a report on file-sharing programs that reached two disturbing conclusions.

- First, USPTO concluded that program distributors had deployed at least five “features” that were known to cause inadvertent sharing and that implementations of these “features” actually became more widespread and more aggressive *after* their propensity to cause inadvertent sharing was known.
- Second, USPTO concluded that inadvertent sharing might not be an accident: Program distributors may have *intended* to thwart the deterrent effects of copyright enforcement by tricking consumers using their programs into sharing files *inadvertently*.¹

In July of 2007, the House Committee on Government Reform held a hearing on inadvertent sharing and the USPTO Report.² It revealed that the problem of inadvertent sharing was far worse—and far more pervasive—than anyone had imagined. The resulting testimony about widespread inadvertent sharing of bank account data, tax returns, credit-card numbers, medical records, educational records and hundreds of classified documents stunned even the CEO of LimeWire:

“I had no idea that there was the amount of classified information out there or that there were people who are actively looking for that and looking for credit card information.... I think I’ve always felt that it was inexperienced users who didn’t know what they were doing. However, when you see documents coming from people who specialize in computer security about, you know, military documents, it really makes you think twice.”

Inadvertent sharing is not a stupid-user problem: It was caused by program distributors who *chose* to deploy “features” that were *known* to cause program users to share files inadvertently. As a result, their programs impose serious risks upon both colleges and universities and their students. *In effect, distributors of file-sharing programs chose to jeopardize the federal funding of every college and university and university in the United States.*

The Causes of Inadvertent Sharing: The root cause of inadvertent sharing is simple: Distributors of popular file-sharing programs chose to deploy “features” that were known to cause users to share files inadvertently. As USPTO noted, the *Grokster* case can explain why they might have done this.


Only SafeMedia’s Clouseau technology offers universities and their students with effective protection against *all* of the risks associated with these programs—and it does so without resort to deep-packet or deep-flow inspection technologies that compromise academic freedom by “eavesdropping” on the substance of electronic communications.

But this piracy-based business plan had a weakness: It required *many* users of file-sharing programs to share *many* infringing files. “Decentralized” file-sharing networks are not unitary networks like the Internet: Every user has a “search horizon” and can only locate files stored on a fraction of a percent of the computers connected to the “network.”³ The distributors of LimeWire have explained the implications of this architecture: “Here’s modern P2P’s dirty little secret: It’s actually horrible at rare stuff.” In other words, LimeWire users will *not* have “the ability to get all the music” for free unless a lot of them share infringing files.

Ironically—and before they actually did so—the distributors of LimeWire has *criticized* RIAA for *not* suing users of file-sharing programs who shared infringing files. But as USPTO reported,

once these users *were* sued for sharing infringing files, their propensity to share files *intentionally* plummeted.⁴ And then features known to cause users to share infringing or personal files *inadvertently* became more aggressive and more widely deployed. USPTO has explained why the history of these “features” strongly suggests that they were *intended* to cause users to share files inadvertently:

- **1H 2002:** *Usability and Privacy: A Study of Peer-to-Peer File-Sharing* concluded that search-wizard and share-folder features in the KaZaA program were causing its users to share sensitive personal files inadvertently.
- **1st H 2003:** The Senate Committee on the Judiciary and the House Committee on Government Reform confirmed that thousands of users of programs that had deployed search-wizard and share-folder features were inadvertently sharing personal, corporate or governmental files. Legislators warn that “in government agencies, employee use of P2P networks could ... disclose sensitive government data to the enemies of this country.”
- **2nd H 2003:** Distributors admitted that *Usability and Privacy* was “intelligent” research and created a self-regulatory *Code of Conduct* that precluded further use of search-wizard or share-folder features.
- **2nd H 2003:** Distributors of popular file-sharing programs told Congress and the FTC that their *Code of Conduct* had rendered further concerns about inadvertent sharing “an urban myth, no more accurate—though easily as persistent—as reports of alligators in New York’s storm drains.”
- **1st H 2004:** Programs like LimeWire had now deployed search-wizard and share-folder features more aggressive than those condemned in *Usability and Privacy*.
- **1st H 2005:** The Department of Homeland Security issued an Information Bulletin warning local, state, and federal agencies that “[m]ultiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P,” and that “there is a military investigation ... in which classified material has been wrongfully disclosed using P2P.”
- **1st H 2007:** USPTO reported that five features that caused inadvertent sharing—including the search-wizard and share-folder features condemned in *Usability and Privacy*—became more widely deployed *after* their propensity to cause inadvertent sharing became well known.
- **2nd H 1007:** A hearing before the House Committee on Oversight and Government Reform confirmed that inadvertent sharing had caused widespread identity theft and disclosed over 200 classified government documents, including city-specific risk assessments and a schematic showing the IP addresses and passwords for the routers on the Pentagon’s secret backbone computer network.



In short, distributors of the file-sharing programs used by about 8 million U.S. households in March of 2007 probably *intended* to trick their users into sharing infringing files inadvertently—even if that would inevitably compromise personal, corporate, national, and military security.

As a result, their programs pose profound risks for both students and institutions. Indeed, they pose a particular threat to all institutions that own and operate complex computer networks. On networked computers, it is possible for one mistake by one user of one computer to “share” all data on the network.

Inadvertent Sharing of Students’ Data Can Expose Students to Lawsuits or Their Families to Identity Theft: The “features” that cause users to share files inadvertently are infamous for causing users to share their own personal files inadvertently. But users affected by such features will *also* tend to share their *entire* collections of media files—even those lawfully acquired from purchased CDs or DVDs. As a result, students who share files inadvertently will tend to share two types of problematic files:

- **Infringing Music or Movies:** As an author of the USPTO Report testified to Congress, were someone to share files inadvertently on his home computer, not only would they share his personal financial data, they would also share over 3,000 copyrighted audio files ripped from purchased CDs. In other words, any student who shares *personal* files inadvertently is also likely to share *thousands* of copyrighted audio files—and become an instant target for a lawsuit.
- **Personal Files:** Searching a file-sharing network like Gnutella will confirm that because students are heavy users of file-sharing programs, they are also the most common victims of inadvertent sharing: One can easily find students sharing bank account numbers, institutional passwords, medical records, and correspondence with psychiatrists or addiction counselors. One can also easily find student-financial-aid applications that can deliver entire *families* into the hands of identity thieves.

Inadvertent Sharing of Educational Records Can Cause Institutions to Violate the Family Educational Rights and Privacy Act (FERPA): Inadvertent sharing threatens all institutions that employs persons who use file-sharing programs, (at home or at work) but it poses unique risks to entities legally obligated to protect confidential data by privacy laws like HIPPA or Sarbanes-Oxley. While many state or federal privacy laws potentially apply to colleges and universities, the law most directly implicated is FERPA.

FERPA Requires The Department Of Education (Doe) To Deny All Federal Funds To Institutions That Negligently Fail To Prevent Unauthorized Disclosure Of “Educational Records.” Section 1232g(b) imposes two critical prohibitions:

- “No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of educational records ... or personally identifiable information contained therein....”
- “No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in educational records....”

Both prohibitions are triggered if an institution discloses “educational records” containing “personally identifiable information.” Both terms are defined broadly. “Educational records” are those “directly related to a student” that are maintained “by an educational agency or institution *or by a party acting for* the agency or institution.” “Personally identifiable information includes, but is not limited to” a student’s name, names of the student’s parents or family, the address of the student or his or her family, any personal identifiers like a “social security number or personal number,” a list of characteristics that make the student’s

identity easily traceable, or "other information that would make the student's identity easily traceable." See 34 C.F.R. § 99.3 (2006).

Inadvertent Sharing Will Tend to Cause FERPA Violations Because "Educational Records" Will Be Widely Stored on Both Institutional and Personal Computers:

In his testimony to Congress, one professor noted that even if a corporation deployed technology that precluded use of file-sharing programs on its corporate network, inadvertent sharing could still disclose its most sensitive data because employees working at home might store corporate data on home computers running file-sharing programs.

And he was right: At the same hearing, the Department of Transportation testified that its Chief Privacy Officer had inadvertently shared citizens' personally identifying data. She did not do so because *she* had installed a file-sharing program on her computer at work. Indeed, she shared it because she had done work on her home computer—never knowing that her preteen daughter had installed LimeWire.

Unfortunately, colleges and universities have are at even greater risk of such problems. Fortunately, they also have a greater capacity to mitigate them.

Educational institutions tend to employ not only faculty and staff—but also students—in many capacities that could involve the creation or maintenance of "educational records." For example, colleges and universities may employ students as research assistants, teaching assistants, graduate assistants, or work-study students. In any of these roles, a student "acting on behalf of the institution" might create or maintain "educational records" on either a computer provided by the institution or on the student's own personal computer. On either computer, that student—or someone else—might


have installed and misconfigured a file-sharing program. As a result, any educational institution that lets its students, faculty or staff install and operate file-sharing programs will inevitably end up broadcasting over the Internet "educational records" containing "personally identifiable information" within the meaning of FERPA.

Fortunately, colleges and universities also have a potential advantage over corporate victims of inadvertent sharing that SafeMedia can help them exploit. Most corporations will not be able to protect employees' home computers because they do not provide internet-access services to those employees. By contrast, colleges and universities do provide internet-access services to student employees who live on campus. As a result, the right technology would let colleges and universities prevent the inadvertent sharing of their "educational records"—regardless of whether it originated from a student employee's work or home computer.

SafeMedia's Clouseau Technology Can Protect Both Educational Institutions and Their Students from the Risks of Contaminated File-Sharing Networks.

For both institutions and students, contaminated file-sharing networks impose unacceptable risks—INFRINGEMENT lawsuits, malware infections, and inadvertent sharing of student's personal files and institutions' educational records—without providing any corresponding benefit. And be assured—the three-way war between program distributors, program users, and copyright holders will continue. There will be more lawsuits, more deception, and more costs for anyone involved.

Fortunately, SafeMedia's Clouseau technology now lets colleges and universities chose to avoid this "war."



Clouseau can protect colleges and universities—and their students—from *all of the devastating risk posed by file-sharing programs*. Institutions that deploy Clouseau can prevent their students, faculty and staff from accessing contaminated file-sharing networks while permitting them to access lawfully distributed music and movies. As a result, Clouseau can prevent both inadvertent sharing of infringing files *and* inadvertent sharing of personal files. No other traffic-shaping device or filtering system can prevent unintentional sharing of both infringing and sensitive personal files.

Moreover, institutions can deploy Clouseau without risking the potential legal liability that can arise from use of traffic-shaping technologies not clearly authorized by terms-of-service agreements with ISP subscribers.

As stated in Section 512(g)(1) of the DMCA: “[A] service provider shall not be liable *to any person for any claim* based on the service provider’s good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.” Because Clouseau disables access to contaminated P2P networks used almost exclusively to access infringing or sexually explicit files, its use is legally privileged under 17 U.S.C. § 512(g)(1) and 47 U.S.C. § 230(c).

Finally—but critically—Clouseau technology preserves the privacy of an institutions, faculty, staff, and students. It does not electronically eavesdrop on communications to, from, or among members of the educational community. By contrast, filtering or shaping technologies that use techniques like deep-packet or deep-flow inspection do so *in order to determine the substance of a given communication*. Needless to say, this inspection—and the potentially permanent record it creates—compromises the privacy of every member of the university community—regardless of whether they are engaged in unlawful file-sharing.

And to what end? At best, this eavesdropping will protect copyright holders—but not the privacy of an institution’s educational records, faculty, staff, or students. For example, a filtering technology will just check the substance of a given communication against a database of copyrighted music and movies. And once that database check reveals that the file being shared contains a student’s credit card number or an institution’s “educational record”—instead of a song—it will authorize the transfer.

SafeMedia’s Clouseau technology is the solution that can protect copyright holders, educational institutions and students from all of the unacceptable risks posed by file-sharing programs that are used unlawfully 97% of the time.

The file-sharing war will continue. But thanks to Clouseau, educational institutions can now choose to say, “No thanks,” and retire from the battlefield unscathed.

Endnotes

- ¹ Thomas D. Sydnor II, et al., *Filesharing Programs and "Technological Features to Induce Users to Share,"* (U.S.P.T.O. 2007) (the "USPTO Report").
- ² A video of the hearing and copies of the witnesses written statements are available on the Committee's web site. See *Inadvertent File Sharing over Peer-to-Peer Networks, A Hearing before the House Committee on Oversight and Government Reform* (July 24, 2007) (<http://oversight.house.gov/story.asp?ID=1424>). The transcript quoted is also available. See Federal News Service, *Hearing of the House Oversight and Government Reform Committee, Inadvertent File-Sharing over Peer-to-Peer Networks* (July 24, 2007).
- ³ The Internet would not be a unitary network if its architects had tried to house DNS servers surreptitiously on users' home computers. In the *Napster* case, the distributor of the first popular file-sharing program was held liable because *it* owned the computers that housed the search-index server that let network users locate desired files. As a result, distributors of programs like KaZaA and LimeWire tried to avoid liability under *Napster* by relocating their search-index servers: Instead of creating these servers on *their* computers, distributors re-wrote their programs to create these servers *on the computers of users*. As a result, students who install programs like LimeWire and eMule thus "agree" to house *on their computers* search-index servers like those that subjected Napster to billion-dollar liability. Predictably, these students are not warned about the potential consequences. Just as predictably, home computers that run many other programs are far less efficient search-index servers than banks of dedicated computers. As a result, users of file-sharing programs can only locate and download a fraction of a percent of the files being "shared" across the entire network.
- ⁴ USPTO Report at 35-36 & n.66.

SafeMedia is a global technology company that has developed patent, best of breed Peer-to-Peer Disaggregator technology (P2PD™) coupled with Digital Internet Distribution system(DIDS™) that is revolutionizing the monetary value of the Internet as a medium for the global delivery of digital copyrighted contents.



CLOUSEAU™ 500

Mid-level system appropriate for use in small to medium size organizations and institutions. The 500 model handles 1-2 Gigabit (10/100/1000) Ethernet lines. It uses multi-core technology with hardware accelerated inspection and I/O to deliver high throughput and low latency.

CLOUSEAU
— NETWORK SECURITY —

CLOUSEAU™ 1000

High-level system engineered for use in large organizations and institutions such as universities and large corporations where 10 Gigabit network throughputs are required. It uses more on-chip cores and co-processor acceleration blocks and will easily meet this high performance mark.

