The Electronic Frontier Foundation

Universities Should Resist Network Monitoring Demands

As part of their attack on filesharing, the recording and motion picture industries are hammering universities with warnings about copyright infringement. Movie and music companies are asking academic institutions to assume the role of cop, judge and jailer, calling on college administrators to snoop on their students and cut off the Internet access of anyone they claim is sharing copyrighted files. Universities should respect copyright and encourage their students to do the same, but they must do so in an environment of academic freedom.

Some schools have capitulated to Hollywood's demands and are actively monitoring all campus Internet traffic; some are hunting down anything that looks like file-sharing and disconnecting the implicated students' computers from the network. Others are blithely turning over students' names and addresses at the drop of a RIAA subpoena, even when the papers are filed in the wrong jurisdiction. This is not what students expect from an educational institution.

Worse, this betrayal of academic principles doesn't necessarily shield universities or their students from legal liability, and it doesn't stop the lawsuits – Michigan Technological University had been cooperating with the RIAA before music companies sued MTU student Joe Nievelt. Instead, monitoring creates entirely new classes of liability, by collecting and retaining pools of data about students' online activity in excess of the law's requirements. In place of the spying demanded, the Electronic Frontier Foundation proposes alternative principles to guide university administrators in setting copyright policies for their networks and responding to requests for monitoring and takedown.

Network monitoring has numerous flaws:

- **Chilling effect on academic discourse:**

  First off, network surveillance is fundamentally contrary to universities' educational mission: the sharing of knowledge. Academic communities flourish on open expression and exchange of ideas, and the Internet is a tremendous communications network, but surveillance chills the climate for inquiry and research. The learning process depends on the freedom to test new ideas and correct early errors. Students who fear that their every communication will be monitored and stored will feel less free to engage in this experimentation. We urge universities not to adopt monitoring that will stifle their network users' expression in this manner.

- **Invasion of privacy:**

  Monitoring invades network users' privacy. The University of Wyoming reportedly used a program that "fingerprints" all network traffic to look for unauthorized copying. In the course of that survey, however, the program must also copy everything sent over the network – all personal emails, confidential counseling or grade reports, web pages viewed, and documents exchanged – along with any media files. Among this information may be some the university is not authorized to collect or disclose, and whose collection may violate the Electronic Communications Privacy Act. Moreover, the data collection may become an attractive target to malicious hackers. This loss of privacy is a tremendous price to pay in order to fight someone else's battle.

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

- **Tagging of false positives:**

Because there is no precise way for a computer to identify a copyrighted song, or to distinguish an unlawful copy from a fair use parody or criticism, automated processes are inherently flawed. Many of the current technologies fail even before these edge cases, however: automated demand letters from "Mediaforce DMCA Enforcement Center" asked UUNet to take down a child's "harry potter book report.rtf", while Universal asked the Internet Archive to remove a film promoting home economics because its filename partially matched a Universal title, U-571. Should students hesitate to exchange their own compositions or samples from a music theory course for fear they will be tagged infringers?

- **Presumption of guilt:**

In the face of these inaccurate identifications, monitoring's advocates would nonetheless like to see all accused infringers removed from the network first, then given the opportunity to ask questions later. Students at some schools have found themselves disconnected in the middle of online assignments, before they have a chance to explain their network use. A student could be sharing copies of his or her own papers or public domain reading materials for a course. The mere use of peer-to-peer software does not prove any copyright infringement.

- **Monitoring's burden detracts from school's mission:**

Further, network monitoring takes resources that the school could better use in its core educational mission. The music and movie industries' demands can amount to a legal "denial of service" attack on a university administration or other Internet Service Provider, as their volume mounts. Instead of permitting themselves to be drawn down the track of greater and greater surveillance, universities should stand up early and assert their rights to set their own educational priorities.

- **Not required by law:**

Finally, any claims that this monitoring is "required" misinterpret the law. Universities, like other Internet service providers, are not required to monitor student Internet usage, not even at the request of copyright holders such as the MPAA. Instead, the Digital Millennium Copyright Act's "safe harbor" provision gives copyright holders specific notice-and-takedown provisions for material hosted on the provider's network, and gives safe harbor to connectivity providers who "ha[ve] adopted and reasonably implemented, and inform[] subscribers ... of, a policy that provides for the termination in appropriate circumstances of ... repeat infringers." Even the law's subpoena procedure, by which copyright holders can request the identity of a network user alleged to be infringing their copyrights, is currently under challenge by Verizon in a lawsuit opposing such a demand from the RIAA. The law of contributory infringement requires a service provider to act when it knows it is assisting in unlawful conduct – not when it has been given often-fallible notices of potential infringement. Service providers who want the safe harbor must adopt use policies, but they need not alter their general-purpose networks to seek out potential infringers.

Instead of implementing invasive network monitoring, universities can respect copyright law by instituting clear policies relating to the use and republication of copyrighted materials. These policies can explain to students the basics of copyright law, the contours of fair use defenses, and the consequences of repeat copyright infringement. They may trigger investigation on reports of suspicious activity, but should not presume every student suspect. Like the fair use doctrine itself, university copyright policies should be flexible, and should always permit the student to explain his or her activities. After all, the universities' goal is to educate, not to punish.