privacy (pro)

Because the online systems that universities have are essentially the property of the university, they should be allowed to monitor granted use, as long as they do so in a non-intrusive way that appreciates the basic human right to be left alone under normal circumstances.

The university owns and operates the network and can regulate it however it pleases. Students and employees of the university who use its online resources are therefore consenting to act under whatever standards the university wishes. The university’s network is not public, so the university can reserve whatever rights it chooses to and users essentially have few claims against this.

The university has the basic right of protecting itself, and should not have to accept any kind of threat due to the misuse of its online systems. If the university could potentially be held legally accountable for illegal activity by users on the system, it will naturally want to be able to step in and eliminate these problems. This includes events when the university could be sued or subpoenaed as well as the occurrence of possible crimes against the university.

Check out:
Duke University Office of Information Technology.
Privacy - Pro

Sarah Hong (sh57) & Serena Lam (ssl17)

The university should be allowed to monitor university networks and connected computers for improper activity because it is in the best interest of the university to protect itself and its students from getting into trouble with the law. The university can protect itself by monitoring certain internet activities of the students while not infringing upon the very basic privacy rights of the students.

When students get involved with lawsuits that involve the internet service that is provided by the university, the university is either directly or indirectly involved as well. This is bad for the university for two reasons: lawsuits are costly; and being involved in lawsuits can be bad for the university’s reputation. “Steven Zink, UNR (University of Nevada, Reno)’s vice president of information technology, said the purpose of the policy is to help keep the students and the university out of court for using music-sharing networks like the former Napster.”

While the importance of protecting the university and its students from lawsuits is great, it is not worth infringing upon the very basic privacy rights of the students. With the use of sophisticated technology, such as tracking down IP addresses based on bandwidth usage, rather than monitoring the actual activities of the internet user, basic privacy rights can be protected while the university’s interest is served.

References:

privacy (pro)

Login: jas35 and naf4

Topic: privacy (pro)

Because of the negative consequences which often result from improper usage of private networks, Universities have the right to monitor their networks for activities that are illegal or contrary to their acceptable use policy, and they can do this without compromising students' right to privacy.

The consequences of improper network activity, especially illegal P2P file-sharing, include possible legal action against a University or its students, as well as the depletion of large amounts of bandwidth that should be reserved for academic purposes.

Faced with this problem, Universities have several options: do nothing and let organizations like the RIAA do their own policing, enter into a legal partnership with a file-sharing server such as Napster, or engage in some sort of network monitoring. Of these options, the third is the only one that succeeds in both preventing lawsuits and freeing up bandwidth for academic purposes, and it would be unfair to deny a University the right to act in the best interests of itself and its students. Furthermore, while there are more and less aggressive ways to monitor networks, few of these methods constitute an invasion of privacy in the traditional sense, because while they may look for certain types of transactions on an individual user's computer, they do not actually consider the content of these transactions.
privacy (pro)- references

Oops, forgot to put the references in the last posting:


All times are GMT - 5 Hours

Page 1 of 1
Watch this topic for replies
Mary Fulweiler and Eric Blatt
Privacy
Argument: It is unethical and unacceptable for a university to monitor a computer on its network for improper activities without probable cause to believe improper activities are taking place on that computer.

The University of Chicago is a good example of a typical university policy on monitoring network activity, stating "Users have right to privacy in their computer files, comparable to privacy in University assigned spaces such as an office or residence hall room." While this is a common policy, due to the living conditions in a university setting where students are restricted to internet access only through a university network, it is unethical for a university to maintain such a policy. As students, we have no alternative option in which we can obtain high speed internet access with reasonable privacy. As such, our university provider should be obligated to grant the privacy rights that are legally required of independent service providers. The federal government ensures through the Federal Electronic Communication Private Act of 1986 that a message can not be intercepted without a court order similar to a wiretap warrant. Also, one must have probable cause before applying for such a court order. While universities can argue that they own their networks and therefore have the right to protect it from improper activity, it is unacceptable to remove a basic right from students without providing them with another viable option to ensure their privacy.

Privacy (con)

Evan Oxman (emo6) and Damon Villaronga (djv4)

Privacy -- Against

A university should not be allowed to monitor university networks because it infringes upon the freedom of students and faculty to use computer resources as they see fit.

Certainly, while a university has the right to mandate that users sign some sort of agreement to follow the law, it does not have the right to preemptively monitor its user's activities. To do so would create a dangerous precedent whereby some sort of 'Big Brother' mechanism would be able to enter our personal spaces and determine how we use a computer's resources. Also, if it is up to the university to define "improper activity," there is certainly the possibility that free speech might be abridged. Thus, the potential costs of infringing upon user's rights to privacy and free speech far outweigh the benefits of preemptively monitoring against so-called 'improper activity.' Of course, if a university were to have its records subpoenaed it would have to comply, but it should not be in the position of doing the job that belongs to law enforcement agents.

Even if a university were only to ostensibly monitor the sharing of copyrighted material (for example) in future times, this may lead to the monitoring and censorship of ideas. Unpopular sentiments may be forcibly suppressed and people may fear that their communications might be used against them in judicial hearings. This will only lead to a growing mistrust and will prevent the beneficial effects that the Internet has in fostering a sense of community and an open and honest dialogue.

While some would argue that since the university owns its network, it can do whatever it wants with it, such an argument makes little sense in practice. While it is true that students are given the privilege to use the university network, it is not as if we are not paying for this access in tuition costs. Similarly, because electronic
communication has become increasingly the official form of communication on campuses, it is not as if members of the university community have a real choice in using the Internet. Subjecting all communication to surveillance violates the concept of prior restraint and simply assumes that all users have malevolent intentions, which is certainly not the case.

References


