Association for Computing Machinery

Advancing Computing as a Science & Profession

April 15, 2008

Senator Edward Kennedy
Chairman
Senator Michael Enzi
Ranking Member

U.S. Senate Committee on Health Education Labor & Pensions

Representative George Miller
Chairman
Representative Howard P. "Buck" McKeon
Ranking Member

U.S. House Committee on Education and Labor

Dear Members of Congress,

As members of the U.S. Public Policy Committee for the Association for Computing Machinery, we wish to express our organization's concern about proposals that would encourage or require technology-based filtering of Internet traffic by universities.

Many members of our committee are copyright holders, and we agree that protecting the integrity of copyright is an important public policy goal. However, we wish to inform you about facts regarding filtering technologies -- based on our scientific and technology expertise -- that Congress should consider carefully during its deliberations.

First, there are known counters to filtering technology. For example, motivated content thieves can encrypt their Internet traffic or use other obfuscation methods to bypass filters that are looking for some specific known signature of the copyrighted work. Obfuscation techniques -- such as introducing "noise" to packets -- create an inevitable, and expensive, arms race of measure and counter-measure between filters and infringers. It can be proven mathematically that this race will never be won by the side seeking to filter.

Encryption is an even more effective countermeasure as strong encryption of traffic will render filtering technology useless. When traffic is encrypted it becomes impossible for any technology to distinguish infringing traffic from non-infringing traffic, or even from routine encrypted traffic such as e-commerce transactions or corporate applications such as virtual private network traffic. Encryption is a widely available technology and one that could be readily incorporated into peer-to-peer applications.

Second, because filtering technologies depend on seeing all traffic flowing over a network they raise significant new security risks. An attacker (external or internal to the filtering organization) can potentially use this infrastructure to gain the same "look" into the network traffic that the filter uses. This access would be very valuable for attackers trying to steal identities, personal or financial information or gain illicit access to valuable research.

Finally, filters can undermine existing freedoms, rights and research. Even the best filters cannot determine what is a fair use of a copyrighted work. A policy requiring or encouraging filtering without having a process to resolve fair use claims would undermine existing, long-established rights as overly aggressive filters blocked otherwise legal activities. Having such a process is not possible if the intention is to block content in real time.

Further, false positives -- blocking content that is in the public-domain because it happens to share a signature of the copyrighted work -- could have a significant negative impact on distribution of educational material at universities. False positives may also hinder legitimate academic research endeavors that rely upon an open and flexible Internet as a platform for experimentation and innovation. Overly broad filters might interfere with legitimate research on peer-to-peer networks, as well as grid or cloud computing efforts.

Infringement of copyrighted works on university networks is a serious issue. However, a Federal policy that promotes or requires filtering will indirectly add to the costs of education and university research, introduce new security and privacy issues, degrade existing rights under copyright, and have little or no lasting impact on infringement of copyrighted works.

Universities that are not already seeking solutions should be encouraged to take reasonable steps to address the issue, and there are a number of different techniques that are being used. Student education and sanctions for offenses are basic administrative actions. Traffic shaping and throttling of bandwidth are two examples of other technical solutions. Some universities have put filters on their networks, and while we believe filtering is short-sighted and will only have limited impacts on infringement, our view is that universities are in the best position to determine how to address infringement.

Thank you for considering our perspective on this issue. Should you have any questions or comments, please contact Cameron Wilson, Director of Public Policy for ACM at (202) 659-9712.

Sincerely,

Eugene H. Spafford, Ph.D.
Professor of Computer Science, Purdue University
Chair, U.S. Public Policy Committee of ACM

Edward Felten, Ph.D.
Professor of Computer Science, Princeton University
Chair, USACM Intellectual Property Subcommittee

About ACM and USACM

With over 88,000 members, ACM is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

The Committee on U.S. Public Policy acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. (See http://www.acm.org and http://usacm.acm.org/.)