

September 21, 2007

## Release Concerning Digital Citizen Project Monitoring Partners

*"The monitoring technologies don't seem to be ready to do what Congress or the entertainment industry wants -- yet." (DCP July 23 Bulletin)*

That single sentence from the Digital Citizen Project's Bulletin released on July 23, 2007 is the most quoted and most misinterpreted statement from the entire body of work that has been shared to date by the Digital Citizen Project (DCP). Most who have used this sentence leave off the "yet". Some interpret the statement to mean nothing works. To clarify that sentence, therefore, the DCP leaders are providing explanation and early comment about the partners involved in our network monitoring and enforcement research. Note that this briefing does not attempt to explore or offer opinion on the policy or political issues (such as mandates) nor the cost issues associated with such monitoring technologies. Each is an important factor in the overall evaluation of technology-based implementations. More information will be provided later in a separate in-depth, technical bulletin on the products we are testing.

### *Changing the Conversation . . .*

When discussing monitoring and enforcement systems, we recognize there are multiple aims. The entertainment industry would like illegal downloading to stop. Higher education would like DMCA complaints and lawsuits to stop so limited resources are not devoted to piracy but to the core values of teaching, research, and service. Those goals are not the same, but there are many common interests and the elimination of costly DMCA notices benefits both industry and higher education. To our knowledge, there is no technology that can stop all illegal peer-to-peer downloading, nor is any vendor making that claim. Similarly, to our knowledge, there is no technology which can guarantee that DMCA complaints will stop. So the more realistic aim for both higher education and the entertainment industry is to REDUCE illegal downloading, thereby reducing the copyright complaints. Indeed the last congressional hearing on peer-to-peer issues was entitled "*The Role of Technology in Reducing Illegal Filesharing.*" If higher education, the entertainment industry, and Congress can come together to agree that one avenue of success at this time is to REDUCE illegal filesharing on college campuses - then the conversation and subsequent actions can be much more productive.

The Digital Citizen Project leaders can say unequivocally that the monitoring technologies with which we are working can and do reduce illegal downloads of songs and, to a lesser extent, movies and videos. As encrypted streams and traffic become more prevalent, tracking and interrupting illegal downloading becomes far more difficult and complex. It is important to keep in mind that no product is 100% perfect but a question is when is it ready? Again industry and

education have different aims. To industry, a technology is ready when it can reduce illicit activity. To higher education, many pragmatic concerns of deployment are involved such as initial cost outlay and cost effectiveness, ease of which to deploy, degree of support required and availability of such, how it works within privacy constraints, network performance, and that which allows all legitimate services to continue. When the DCP says solutions are not ready -- yet, it means that although a technology may be viable, it might not meet all of the requirements necessary for broad deployment. But just as no city would go without a police force because their officers cannot stop every single crime, no technology should be simply discounted because it cannot find every file transfer. We believe technology can play an important role in addressing the issue -- along with:

- education and awareness,
- alternative legal entertainment services,
- aggressive K-12 education,
- clear understandings and practical applications of educational fair use,
- and a system of rewards for compliance.

### ***With whom is the Project working?***

A goal of the Digital Citizen Project is to work with and understand the leading monitoring and enforcement technologies available. We intend to evaluate each technology fairly and report back to the higher education community about each vendor's abilities, strengths, weaknesses, limitations, and successes. Each of the following companies has equipment up and running on varying parts of Illinois State University's campus network.

### ***Audible Magic ([www.audiblemagic.com](http://www.audiblemagic.com))***

Audible Magic became a partner very early in the work of the DCP and from the perspective of the DCP leaders and technical staff specialists, Audible Magic is certainly one of the key industry leaders at this point in time. Much of the network data being reported by the DCP is taken from Audible Magic equipment. The CopySense appliance relies on electronic signatures and hashes -- markings that studios have provided which identify the song, movie, or TV program and, optionally, block individual file transfers. With such fingerprints, CopySense can detect streams with copyrighted content on University networks. While we have not seen any impact on our production network regarding stability or performance, we have learned that it is very important that the hardware appliance be matched with the capacity of the network.

Tests of the Audible Magic CopySense appliance have highlighted a significant task that the entertainment industry must tackle before any system can be fully effective. In April the CopySense appliance, in monitoring mode, discovered over 12,800 unique copyrighted titles. The non-signed metadata-coded files identified another 16,000 songs and movies. Yet this was a small part of the full P2P stream crossing the ISU network during this month. Much of the rest of the stream was unidentified and one explanation for such would be the lack of signatures on the files being transferred. Copyright owners and studios must address the significant need to signature their material -- and not just the top 20 and blockbuster releases. However, from our preliminary tests it is obvious that Audible Magic and systems like it can reduce illegal file-

sharing significantly, but at the same time the vendors and entertainment industry must improve their technologies and file signatures.

Throughout planning, design, implementation, and analysis, Audible Magic staff have been flexible and easy to work with. Evidence of their willingness to partner in the Project and an example of the value that the Digital Citizen Project can return to a vendor is the collaboration that led to AM's Escalated Response product. The idea was incubated at Illinois State and developed for beta testing by the company. Whenever possible, vendor partners of the DCP may explore their products on the living laboratory of ISU's campus, make product improvements, and make their systems more effective and attractive to the higher education market.

### ***Packeteer*** ([www.packeteer.com](http://www.packeteer.com))

Illinois State University has employed Packeteer hardware since 2001 to shape its bandwidth and direct various layers of Internet traffic. Packeteer can block or shape data transfers based on university-defined criteria. It has allowed ISU to effectively allocate a very small percentage (5% for both uploads and downloads) of its established commodity Internet bandwidth to peer-to-peer transactions 24 hours a day. Illinois State chose this route specifically because it made a major difference and there are legitimate uses for P2P such as Linux, gaming software updates, library file transfers, scholarly exchanges, and others. The 5% pipe should not imply that ISU condones unacceptable uses of peer-to-peer technologies - but rather supports legitimate scholarly, educational, and operational applications of P2P. The DCP recognizes that this technology is only as good as the application list.

### ***Red Lambda's Integrity*** ([www.redlambda.com](http://www.redlambda.com))

The DCP has a multiple-year history with Red Lambda; we were introduced to their technology early in our research. After investigating such Red Lambda products as Icarus and cGrid, we installed the Integrity appliance on a discrete part of ISU's network in July 2007. This system identifies and blocks P2P transfers based on the application protocol rather than the content of the transferred file. It then has a series of graduated notifications and responses available for selection by the University. Since it detects the data streams and not the content of those streams, Red Lambda is not affected by the encryption methods used in some P2P applications. The flexibility of the included scripting engine in the Integrity application framework allows for varying responses to detected infringements. Results and further experiences will be reported on Integrity in spring 2008.

### ***Others***

eTelemetry is new to the DCP. The "Locate" appliance was installed on a segmented part of the campus network in early summer 2007. This tool facilitates the mapping of IP addresses to end-users. Data collection on performance and activity has just begun and the DCP expects to do a full report on eTelemetry late in the spring semester 2008.

Other systems that the DCP is having active conversations with and/or reviewing from the marketplace literature include Allot, Enterasys, and Safe Media. We recognize that new products come on the market almost monthly, if not weekly -- so our list of possible vendor products to evaluate grows and changes rapidly.

### ***Conclusion***

The DCP leaders are aware of other approaches to combating campus piracy, ranging from ignoring complaints and the issues surrounding downloading to simply managing DMCA complaints the most direct way possible to completely blocking P2P transfers. Many of these tactics have been described in professional and industry literatures. The DCP continues to advocate a multi-faceted approach involving education and awareness, monitoring and enforcement, better avenues to multiple legal media services, aggressive K-12 education, and significant improvements in the understanding and application of fair use in education.

We've used the analogy of seat belts often in our documents, presentations, and testimonies. The first seatbelt law was passed by Congress in 1963, and still last year people were only 80% compliant – even when the technology could save their lives! The traffic safety programs created were trying to change culture and behaviors -- very deeply rooted, personal behaviors. The DCP believes that anti-piracy campaigns are also about changing behaviors and culture. We hope that illegal piracy can be reduced in less than the 40 years it has taken seatbelts to gain acceptance. But any impact will only happen with several different approaches to the problems. We believe the DCP's work will show that partnerships, marketing, education, and enforced campus policies can change the culture of digital entertainment.

**Bottom line** - College and university campuses CAN REDUCE campus piracy with the technologies that exist today. They aren't perfect. They can't, in and of themselves, end campus piracy. And they can't promise DMCA complaints will stop upon installation. Still, the technologies available today CAN positively impact the problem of illegal file sharing on a college campus today.

### ***DCP Principal Authors:***

**Cheryl Elzy**  
*Dean of  
University Libraries*

**Mark Walbert**  
*Associate Vice President, Academic  
Information Technology*

**David Greenfield**  
*Director, Student  
Technology*

**Sue Stroyan**  
*Director  
Digital Citizen Project*

**Warren Arbogast**  
*President & Founder,  
Boulder Management Group*

Contact [digitalcitizen@IllinoisState.edu](mailto:digitalcitizen@IllinoisState.edu) or see [www.digitalcitizen.ilstu.edu](http://www.digitalcitizen.ilstu.edu) for more information.