

Ms. Velica Steadman, Office of Legislative and International Affairs:

The following is in connection with the USPTO's Request, previous comments made in connection with digital rights management ("DRM") and digital watermarking technologies, and technologies that my company, Blue Spike, Inc., has deployed to the satisfaction of several entertainment and information technology vendors.

DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

[Docket No. 2003-C-006]

Request for Written Comments and Notice of Hearings on Technological Protection Systems for Digitized Copyrighted Works AGENCY: United States Patent and Trademark Office, Commerce. ACTION: Request for written comments and notice of hearings.

There is no "DRM" [digital rights management] without digital watermarking. DRM without watermarking cannot offer any way of handling content once it is rendered, heard, seen or enjoyed. Further, predetermining the price of newly released content is about as effective as Soviet pricing schemes. The "little knowledge is a bad thing" argument about DRM is a perfect example of why the only technology that can act as an objective means of serializing, and thus accounting for content, is digital watermarking.

Many arguments against such deployment, including Professor Ed Felten's arguments concerning HackSDMI and subsequent alleged "legal action" in connection with hacks on the various watermarking systems, miss the entire point: metering content and applying actuarial measures to information exchange are inherent to the workings of a commercially viable information economy. In fact, my own Company, one of the three finalists, successfully hacked the available systems more frequently than any other party in an effort to direct attention to the value of the technology. Key-based watermarks have been successful at identifying and associating piracy with particular individuals at many large entertainment companies. Blue Spike, has deployed many of these systems for over five years.

When digital content is watermarked, it should be watermarked using a cryptographic key: just like a digital signature of a text document. SDMI and other efforts at standardizing forms of watermarking, including the FCC's "Broadcast Flag", should focus on this point—authentication tools are far more important than copy restriction tools for the simple reason that all that can be seen, heard and rendered is technically easy to capture and re-use. Any good or service which achieves high levels of recognition, in the physical and intangible worlds, suffers from unauthorized copying. Authenticity is both the tool and means by which companies and governments should leverage appropriate and existing laws.

The real problem is: Once copies of media are released in a manner that is not unique, unfettered copying will happen. There is no commerce without serial

numbers and receipts; only key-based watermarks can provide this utility and bring the current holy war to a rational discussion of what and where the problem of piracy is. If a content company has high profits, is there piracy? Can the government collect 100 percent of taxes? There are no clear cut answers to these questions.

It would seem that the complication is more about consumer acceptance. To balance piracy with privacy is indeed difficult. To offer systems that do not fairly compensate consumers for the value propositions they have grown used to (fair use, first sale doctrine, copying, and so on) is not the fault of those consumers. The focus should be on content itself, not content file formats or government-sponsored "rules" for handling content. More succinctly: answer the question "Is this copy authentic?"

In the real world, too, we focus on serial numbers even when we deploy additional security measures, as speed bumps to rampant and unabated piracy. The Government should have a role in measuring and managing spectrum, including digital copies in networked environments, in a manner consistent with actuarial accounting.

The marketplace issue: only small fraction of content accounts for a lion's share of the revenues realized by content creators. Picking hits continues to be guesswork, at best. An important issue is that content needs to be made unique, even though copies can be made. Key-based watermarks are the only technology that enables such uniqueness to be integrated with the content and to indicate any subsequent tampering. Without receipts for information content, it is unreasonable to expect success in predetermining price and commercial viability of newly released content typically offered to the consumer's detriment under the rubric of traditional access restricted DRM.

Before there can be successful rights management, responsibility for individual copies, not wrappers or locks, needs to be attributed. Otherwise, how is any party to a content transaction able to properly account for or differentiate between piracy and marketing?

Sincerely,

Scott Moskowitz
Founder, CEO
Blue Spike, Inc.
<http://www.bluespike.com/>

P.S. The following attachment discusses existing technologies developed and deployed by Blue Spike with very successful results, and appeared in the following.

CEO Scott Moskowitz on

What is Acceptable Quality in the Application of Digital Watermarking:
Trade-offs of Security, Robustness and Quality

IEEE ITCC 2002 Special Session on Watermarking April 8-10, 2002

ABSTRACT: Quality is subjective. Quality can be objectified by the industry standards process represented by such consumer items as compact disc ("CD") and digital versatile disc ("DVD"). What is lacking is a means for not only associating the creation of valued intangible assets and extensions of recognition but establishing responsibility for copies that may be digitized or pass through a digital domain. Digital watermarking exists at a convergence point between piracy and privacy. Watermarks serve as a receipt for information commerce. There is not likely to be a single digital watermark encoding scheme that best handles the trade-offs between security, robustness, and quality but several architectures to handle various concerns. The most commercially useful watermarking schemes are key-based, combining cryptographic features with models of perception. Most importantly, in audio watermarking there currently exists mature technologies which have been proven to be statistically inaudible.

Published in IEEE Computer Org. 2002 International Symposium on Information Technology (ITCC 2002).

<File attached: 068_MoskowitzS.DOC>