Comments
Relating to

DIGITAL RIGHTS MANAGEMENT TOWN HALL

(DRM Town Hall – Comment, Project No. P094502)

Submitted By

THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

to

THE FEDERAL TRADE COMMISSION

February 13, 2009

The Software & Information Industry Association ("SIIA") is the U.S. trade association of the software and digital content industries. SIIA is the nation's oldest and largest association representing software and content companies. SIIA has grappled with important intellectual property and technology issues in the software and content industries for many years. Its members range from start-up firms to some of the largest and most recognizable corporations in the world. SIIA member companies[1] are leading providers of, among other things:

- software publishing, graphics, and photo editing tools
- corporate database and data processing software
- financial trading and investing services, news, and commodities
- exchanges
- online legal information and legal research tools
- protection against software viruses and other threats
- education software and online education services
- open source software
- and many other products and services in the digital content industries.

[1] A list of the more than 500 SIIA member companies may be found at: http://www.siia.net/membership/memberlist.asp.

SIIA's members are also leaders in the development and use of Digital Rights Management (DRM) systems to protect copyrighted works. SIIA has been fighting digital piracy longer than any other trade association in the world. During the last 20 years of combating piracy, we have gained invaluable experience as to what anti-piracy policies are effective and what type of Government involvement is appropriate and necessary. It has been SIIA's experience that effective DRM technologies should (i) effectuate a broad industry consensus on this issue; (ii) not require technical standards unilaterally established by the government on industry and (iii) allow companies a choice of technologies that are appropriate to the content to be protected, the channel of distribution to be used, and the end-user environment.

The functionality provided by DRMs basically fall into three categories:

> Access Control Functions: These functions control the user's right of entry to the protected content, e.g., encryption and/or authentication.
>
> Use Control Functions: These functions control how the user can interface with the protected content, e.g., read-only rights (the user is unable to print, save or distribute the content).
>
> Tracking Functions: These functions allow the content provider to track the subsequent use and/or distribution of its content online, e.g., watermarking and digital footprints.

Within each type of protection system, there are varying degrees of protection. For example, different types of access control systems include:

Type of Protection	**Level of Protection**
Encryption	High Level of Protection
Subscription	Medium Level of Protection
Registration/Password	Medium-Low Level of Protection
Click-through Agreement	Low Level of Protection

For systems using use control functions:

Type of Protection	**Level of Protection**
Read-only	High Level of Protection
Read & Print rights	Medium Level of Protection
Full Access	Low Level of Protection

For systems using tracking functions:

Type of Protection	**Level of Protection**
Watermarking/Digital Footprints	High Level of Protection
Online/electronic Clearinghouse	Medium Level of Protection
Voluntary User Compliance	Low Level of Protection

A DRM system may include one or more of these functions. For example, a certain DRM system may incorporate password access controls and read-only use controls to prevent wrongful access and wrongful re-distribution of the protected product. To some extent access control and use control functions may also be overlapping. For instance, access controls also serve as use controls since a user who does not have access to the content may not use it.

Following are five important guidelines regarding the development and implementation of DRM technologies.

DRM is Essential to Protect Copyrighted Works from Piracy and to Encourage Widespread Distribution of Copyrighted Works: Publishers consider the unauthorized access and use of their copyrighted works, including unauthorized copying, distribution, display and revision, as the most serious risk associated with making their valuable proprietary materials available online (or otherwise in digital form). The technological ease with which piracy can occur is only exacerbated by widespread misconceptions existing within user communities regarding rights to access and use of copyrighted content that is distributed in digital form. DRM systems enable copyright protection, distribution, usage and payment for digital content such as text, music, images or software via any electronic medium. Effective DRM systems provide the requisite security to encourage copyright owners to look beyond the risks posed by piracy and make their digital works available to the public. Without such systems, copyright owners would be likely be unwilling to make their digital works as widely available as they are today.

There Is No One-Size-Fits-All DRM Solution: In light of our experience in the variety of markets in which our members operate, we find that on the whole DRM systems have been developed and implemented reflecting market demands. Those demands have not and cannot be met by a one-size-fits-all business and technical solution. On the contrary, DRM systems have been successful when they are appropriate to the circumstances of the market situation, taking into account user needs, the value of the information or content to be protected and the soundness of the business model. It is also clear that this is a dynamic market where changes in both technology and business models are evolving rapidly.

Government Regulation of DRM Technology Would Be Intrusive and Inappropriate: Any legislation in this area should not give the Government the ultimate say in determining what DRM standards will be adopted and how they will be implemented today and into the future. The marketplace – not the Government – should determine the winners and the losers in the DRM space. Only through competition in the DRM industry and the stakeholders working together to develop mutually-acceptable standards for DRM solutions to the piracy problems will we get the best DRM technological solutions. *To the extent there is a role for the Government here, the role should be only to promote confidence that technological solutions agreed to by the stakeholders can be enforced to combat piracy problems.*

Government Regulation of DRM is Slow and Ineffective: The Government decision making process is inherently ill-equipped to effectively address the types of issues raised in the DRM debate. The process is slow and unwieldy. With business models evolving so rapidly, it would be unwise to attempt to craft a new and complicated framework of government-imposed measures merely to address concerns that are likely to be rapidly addressed as the marketplace

for copyrighted works and anti-piracy technologies evolve. The Government will not be able to keep pace with the rapid changes in technology – virtually assuring that any standard the Government codifies is outdated the moment it becomes law.

Marketplace Solutions Are The Best Solutions: The high-tech industry has worked with the content community to reach consensus on ways to address similar piracy problems in the past. There is no reason to think that the stakeholders cannot again reach consensus on ways to combat the specific technological problems identified by the content and/or user communities. Only through DRM companies competing and working together with content companies and others can effective solutions be found.