BEFORE THE FEDERAL TRADE COMMISSION

In re Digital Rights Management Town Hall	)
FTC File No. P094502	)

Comments and Request to Serve as a Panelist of Thomas D. Sydnor II, Senior Fellow and Director of the Center for the Study of Digital Property at the Progress & Freedom Foundation.

These comments are filed on behalf of Thomas D. Sydnor II, Senior Fellow and Director of the Center for the Study of Digital Property at the The Progress & Freedom Foundation. I thank the Commission for holding its upcoming Digital Rights Management Town Hall, and I respectfully request to serve as a panelist during the Town Hall, if the Commission determines that this would help balance or assist its inquiry into digital-rights-management ("DRM") technologies.[1] My pertinent qualifications would include the following:

- I am familiar with both private and public perspectives on copyright law and policy. From 1991 to 2003, I was a litigation attorney in private practice who focused on representing clients in intellectual-property or administrative-law cases. From mid-2003 to mid-2005, I served the Senate Committee on the Judiciary as its Counsel for Intellectual Property and Technology. From mid-2005 to mid-2007, I focused on international and digital copyright issues as an attorney-advisor to the Copyright Group at the U.S. Patent & Trademark Office. From late 2007 to the present, I have studied copyright law and policy at the Progress & Freedom Foundation, a § 501(c)(3) organization dedicated to studying the public-policy implications of digital technologies.

- I have often assisted government officials seeking to better understand digital copyright policy generally, and DRM technologies in particular. At the USPTO, I trained hundreds of government officials from around the world in digital-age copyright law and policy. I also created the instructional program still used during the week-long Advanced Copyright Seminar hosted by USPTO's Global Intellectual Property Academy.

- I have conducted original research that can help show why the most severe, difficult-to-detect, and enduring risks to consumers are likely to arise—not from law-abiding

[1] DRM technologies can be loosely defined as systems for protecting or enforcing copyrights that incorporate up to three different technologies protected by existing U.S. law. A DRM system may incorporate one or more "technological protection measures" (like encryption) that effectively controls *access* to the protected work. *See* 17 U.S.C. § 1201(a). A DRM system may also incorporate one or more "technological protection measures" that effectively control the exercise of some or all of the copyrights in the work. *See id.* at § 1201(b). In either or both cases, a DRM system will also tend to incorporate rights-management-information ("RMI") that identifies, for example, the owner of the copyrights in the work and the uses authorized. *See id.* at § 1202.

businesses deploying DRM—but from the distribution of devices or programs widely used for unlawful purposes like copyright infringement.

I believe that I could assist the Commission's efforts to understand the consumer-protection and public-policy implications of DRM technologies by providing the broader perspective often lacking in debates about DRM technologies. The following two examples of illustrate these perspectives.

1. Benefits and Costs of DRM Must Be Compared to Those of Other Means of Enforcing Copyrights Online.

From the perspective of copyright and public policy generally, the significance of DRM only becomes clear when you compare its implications against those of other existing, or potentially viable, means of enforcing copyrights on the Internet. Copyrights are private property rights in expressive works that enable market mechanisms to encourage the production and broad dissemination of expressive works without the risks of control over content inherent in any system that rewards creators through private or public patronage. But like any property right, copyrights must be *privately* enforceable, *as a practical matter*, or they are illusory and ineffective. This question—how do we keep copyrights enforceable, as a practical matter?—is central to any discussion of copyright law and policy in the 21st Century.

Resolving this question, sensibly, is particularly critical to the United States. The United States is, as to every other nation, a net exporter of copyright-protected expressive works. As a result, U.S. copyright industries are remarkable drivers of employment and economic growth. For example, during 2004, they employed 5,344,000 workers whose average compensation was 26% above the U.S. average compensation level, while generating about 24% of the real annual growth in the U.S. economy.[2] During a recession, these facts have obvious implications for public policy. Never again will the United States be the world's leading net exporter of television *sets*. But the United States is, and can continue to be, the world's leading net exporter of television *programming*—if we ensure that copyrights remain privately, and practically, enforceable.

Under existing law, DRM is one of two generally-applicable means of enforcing copyrights—the other is suing alleged infringers in federal court, or threatening to do so. Historically, this latter, litigation-centered enforcement mechanism has predominated, and worked quite well. To understand the potential significance of DRM, one must thus understand how traditional copyright enforcement worked, and why it will work differently in the future.

In the past, copyright owners relied upon a system of intermediary-focused enforcement. In other words, distributors, (entities that wanted to add value by making available to the public works created and funded by others), usually had to do one or more of the acts that copyrights reserve to the copyright owner—acts like copying the work, distributing copies of the work or publicly performing the work. As a result, the threat of strict liability for copyright infringement ensured that works reached consumers in ways and in forms that reasonably accommodated the

[2] *See* Stephen E. Siwek, *Copyright Industries in the U.S. Economy* at 4-5, 10 (2006).

interests of creators, funders, distributors, and recipients of content. In addition, courts applying the Copyright Act also developed doctrines of contributory and vicarious liability for copyright infringement that would let copyright owners retarget enforcement "up the chain of distribution" when doing so would be fair and would preserve the enforceability of their rights. This system had many important consequences, and three are particularly relevant here:

- Intermediary-focused enforcement ensured that ordinary people—from toddlers to seniors—could enjoy expressive works safely without any detailed knowledge of copyright law.

- Intermediary-focused enforcement also allowed copyright law to become both specialized and flexible, with different rules for different types of works and open-ended, equitable limitations like the fair-use defense.

- Intermediary-focused enforcement also, however, results in a "white-list" distribution system: distributors must be sure that they have acquired the relevant permissions before distributing any particular work.

More recently, however, technological change has created new types of intermediaries that raise fundamentally different concerns. Essentially, these new intermediaries provide consumers with products or services that enable consumers to perform acts like reproducing copies and distributing them to the public. Examples of these new intermediaries would include distributors of consumer copying devices and online service providers. They raise difficult questions that become all the more intractable if we insist upon

On the one hand, traditional liability rules can impose liability too broadly when applied to these new intermediaries. For example, distributors of home copying devices should not be directly or vicariously liable for infringing uses of their devices, but they probably would be contributorily liability if their devices had foreseeable infringing uses. Similarly, online service providers might well be directly, vicariously, and contributorily liable for infringing uses of their services—unless they adopted the traditional white-list model that could deprive consumers of many of the communicative benefits of the Internet.

On the other hand, simply exempting these new intermediaries from liability would be tantamount to directing copyright owners to enforce their federal rights against ordinary consumers—the end users of expressive works. Efforts to deter illegal uses of the global copyright-piracy rings deliberately created by the distributors of file-sharing programs like KaZaA, Grokster, and Morpheus have made one point clear. In a fast-moving technological environment, directing copyright owners to enforce their rights against consumers will inevitably redirect enforcement, disproportionately, toward consumers who happen to be unusually technically or legally unsophisticated. In other words, we would be directing artists to sue their fans who happen to be particularly young, poor, uneducated, or otherwise technically unsophisticated. That seems fundamentally unfair to both consumers and artists.

Obviously, the law must devise some new balance that accommodates the legitimate needs of both these new intermediaries and copyright owners *without* generally redirecting copyright

enforcement towards consumers. But as cases like *Sony* and *Grokster* would suggest, except in the easiest of cases, (overwhelming non-infringing use or intent to induce piracy), there is little agreement as to what this new balance should be.

These comments are not intended to propose some new solution to these fundamental challenges. Rather, they are intended to show that DRM is important precisely because it provides a broadly applicable mechanism for developing a system of copyright enforcement that relies mostly upon technology, not lawsuits. As a result, any reasonable debate about the advantages and disadvantages of DRM must consider the existing alternatives. Those who disfavor or reject DRM must answer the fundamental question that follows from their opposition: then whom do you want copyright owners to sue? Should they sue the intermediaries, and if so, what standard of liability would make it unlikely that consumers would have to be sued for making infringing, yet foreseeable uses of the intermediaries' products and services? Or should copyright owners sue consumers who merely used seemingly legitimate technologies in ways that were wholly foreseeable, yet largely illegal?

2. The Most Severe and Enduring Risks to Consumers Will Be Caused by Lawless, Piracy-Based Businesses—Not by Law-Abiding Businesses Using DRM.

Virtually any technology can be implemented in a way that imposes undue risks, burdens or confusion on consumers, and this is true of DRM technologies. Nevertheless, this tells the Commission little about whether DRM technologies ought to be a focus of the Commission's consumer-protection efforts. To resolve this question, the Commission must determine whether DRM technologies or some other sort of technology are most likely to pose the most significant risks upon consumers.

While no one would want to expose consumers to risks of harm in order to determine which sources of risks were more likely to be dangerous and enduring, such risks do sometimes arise. By comparing the severity, duration, and real-world consequences of risks arising from different sources, the Commission can assess which sources are more likely to create the serious, enduring, and difficult-to-detect consumer risks that require the application of its enforcement powers and expertise.

Recently, two roughly contemporaneous situations revealed the remarkable difference between our existing consumer-protection system's capacity to detect, respond to and remediate computer-security concerns arising from uses of DRM, and security concerns arising from uses of Gnutella, FastTrack, and eDonkey 2000-based file-sharing programs that are almost always used to infringe copyrights. For example, when security concerns arose from potential vulnerabilities allegedly caused by the XCP DRM technology briefly used on some CDs distributed by Sony/BMG, our existing system worked quickly, and decisively—the vulnerability was quickly identified and publicized, affected consumers filed class-action lawsuits, and consumer-protection agencies supervised the settlement of those claims to ensure that they served the public interests.

But when more severe concerns arose from defective file-sharing programs that consumers used almost exclusively to download infringing copies of copyrighted music, movies, and software, our consumer-protection system let severe defects persist—and worsen—for years. These defects compromised national security. They caused identity theft; they empowered spammers and pedophiles; and they created avoidable conflicts between copyright owners and consumers.[3]

In testimony to the House Committee on Oversight and Government Reform, I suggested the critical difference between these two situations.[4] Consumers who acquire works protected by DRM are likely to do so legally. As a result, they have both legal rights to expect those works to be reasonably safe when used in foreseeable ways and the practical ability to enforce those rights if they are violated. By contrast, when consumers are engaged in an illegal activity, like copyright piracy, they have neither the incentives nor the practical ability to complain if they are wronged.

As a result, real-world experience teaches that any risks arising from uses of DRM are likely to be resolved quickly and effectively. On the other hand, when consumers use a given product or service mostly for unlawful purposes, they will be unwilling and unable to complain about even the most fundamental and reckless invasions of their rights. Copyright piracy and the lawless business-models that it breeds are thus far more fundamental threats to consumers and the nation than DRM has ever been, or will ever be.

//s Thomas D. Sydnor II

[3] *See, e.g.*, Thomas D. Sydnor II, et al., *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform*, at 5-8 (Progress and Freedom Foundation, Oct. 2007) (discussing and citing my prior report on inadvertent sharing published by USPTO).

[4] *See also* Federal Trade Commission, Transcript at 205, *Public Workshop on Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues* (Dec. 15, 2004) (statement of James C. Miller, former Chairman of the Federal Trade Commission)