Lee Shaker
Annenberg School for Communication

An Overview of DRM System Types and Their Privacy Implications

In the analog age, the copyright protected the ability to profit from ideas and art well enough that private companies were eager to participate in the commercial marketplace. Additionally, it simultaneously allowed consumers a certain amount of license in sharing and manipulating works as they cherished, created, and collaborated. As a theoretical concept, it even enhanced individual privacy rights by preventing the unauthorized reproduction of one's physical likeness. Today, digital technology makes replication and transmission of intellectual property (IP) so convenient that copyright law is ineffective in deterring illicit distribution around the world. Because of piracy's opening maw, many artists and businessmen suggest that a new measure of protection for IP is necessary.

Ostensibly, digital rights management (DRM) systems are designed to protect IP and equitably mete out profits to those who deserve it. As such, DRM technologies are often positioned as a solution for the problem of piracy. The creators of content and the owners of copyrights require payment to propagate their efforts; DRM systems are simply a tactic to ensure this remuneration. These business interests posit that DRM systems are a necessary protection for copyrighted materials. They argue that without this security, the motive for creativity will evaporate concurrently with profits. DRM initiatives are also portrayed as beneficial for consumers who gain increased privacy and protection.

Many consumer interest groups (among others) contend that both the societal need for and benefit of DRM systems are overstated by corporate actors. In their view,

from the outset of humanity until the present, innumerable individuals have been moved to innovate and create—even when making a profit was unlikely or simply not a motivating force. They fear that DRM systems will discourage invention and progress rather than protect it, and that DRM technologies ultimately have a deleterious effect upon society. Rationalized as a tool to protect IP, DRM systems are applied in ways that extend beyond the original impetus. Because of their liberal deployment, the effects of DRM systems upon individual privacy are manifold, beginning with obvious restrictions and incursions but extending to large revisions of the general conception of privacy in the post-modern capitalist environment.

DRM systems are designed in many forms. Legal scholar Julie Cohen suggests that DRM methods be imagined as "a series of concentric levels of control, each penetrating more deeply into the user's home electronic and computing environment."[1] This conception provides a useful framework for tracing the nature of invasion, privacy, and DRM but it is vague. Tactics that appear innocuous lead to increasingly invasive layers of stricture, often with implications that are not immediately apparent. DRM systems restrict when, how, where, and how much a given piece of information is accessed. In addition, these technologies are also often deployed to collect a wide array of data regarding user behavior. Ultimately, the rise of DRM technologies signals a growing disregard for individual privacy and liberty in America while also reflecting a shift in power from government to corporate actors. This paper offers a schema for understanding DRM efforts and their impact upon individual privacy. In addition, it contains a discussion of the effect DRM systems have upon the quantifying of intellectual property and the implications of these changes, privacy and otherwise.

.

II. Legal Grounding and Foundation of DRM

Legal justification of DRM systems begins with a single claim: DRM technologies are merely an extension of traditional copyright law that protect innovators and creators in the digital era. Originally, copyright law was conceived of as a way to engender creation and ingenuity by guaranteeing innovators the exclusive right to benefit over a limited period of time from a work. Specifically, according to Article I, Section 8, Clause 8 of the U.S. Constitution, "the Congress shall have power . . . to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." Since 1787, there have been numerous modifications of copyright protections, recently and notably in 1976 and 1998. These revisions extended the period of protection to the term of an author's life plus seventy years, and in the Digital Millennium Copyright Act (DMCA), made accessing a work by circumventing a technological form of copyright protection a crime.[2] The effect of these revisions is to grant not only a greater term of benefit to copyright holders, but also to permit them broad license and leeway to explore the application of various technological controls upon IP use.

Criminalizing the circumvention of any DRM obstacle allows private interests to create data environments for their IP that are inviolable. The parameters of legal use shift based upon the DRM strategy employed, making the business entity the party that determines de facto legality rather than the government: the licenser of any work can determine what uses are legal, and summarily make all other uses illegal by placing an "effective" technological impediment in the way.[3] Circumvention of this barrier, with

only a few exemptions, is illegal, rendering most uses illegal by default except for those situations and applications specifically permitted. In legal challenges, the courts thus far "have characterized the design of DRM systems as grounded, unproblematically, in principles of copyright and contract law and justified by reference to a copyright owner's need to enforce its 'property' rights," without recognizing the important differences between the effects of traditional copyright law and DRM initiatives.[4] If "the constitutional purpose of copyright is to stimulate content creation for the public's benefit, *not* to create a private property right," then it appears that the DMCA proffers a distinctly different philosophy.[5] Consequently, the DMCA opens a window for copyright holders to design DRM that best protect their interests, omitting the Constitution's concern for balance between economic and creative imperatives. In the process of exploiting this opportunity to maximize control over copyrighted works and profit streams, individual privacy and liberty are of only ancillary concern to those designing DRM systems.

III. DRM Tactics

Optimistically, "DRM solutions promise to protect profits, create new approaches to information management, and produce new marketing opportunities."[6] Deployed in a wide variety of shapes and forms, the most basic DRM initiatives adhere to the binary nature of digitalization: software encryption or hardware construction render a bit of information either operable or inoperable depending on the manufacturer's predilection. An example of this technique manifested in hardware creation would be the decision to alter CD or DVD players to prevent them from playing burned (rather than pressed)

discs. A conglomerate like Sony, which is heavily invested in content creation through its music and film properties and is at the same time a hardware manufacturer, may choose to render CD-R or DVD-R discs inoperable in the CD and DVD players it produces in order to discourage piracy. Many large companies are forced to balance these competing interests and continually assess the most profitable route. In another case, Philips' decision to market CD burners that copy protected CDs while at the same time blocking sale of DRM-free DVD players into Europe clearly depicts the conflict between the competing interests of hardware and software factions.[7]

Inoperability can also be achieved easily by employing software to disable functionality. A well known exemplar of this DRM type is the Content Scrambling System (CSS) with which DVDs are encrypted.[8] Access to the data on each DVD is encrypted to prevent its playback by any device that does not have the proper regional key. Movies released on VHS often had a copy-prevention mechanism called Macrovision which scrambled the output to prevent duplication but still allowed any VCR to play the movie. CSS goes beyond Macrovision by stymieing not only duplication but also playback in many situations. DVDs are coded for one of five regions, and can only be played by hardware that has matching regional designation. In the case of Jon Johansen (DVD Jon), a teenager that distributed the CSS encryption crack, CSS caused inoperability between legally purchased DVDs and a DVD player because they were used in a Linux environment.[9] The encryption and manufacturer's hesitance to adapt to new technology slowed the rate of innovation, stifling a legitimate use of the purchased materials, prompting Johansen to commit what may be a crime in some jurisdictions.

DRM systems like this constitute the first circle in Cohen's model of "levels of control."[10] Clearly, these methods constrict individual liberty, but they also have privacy implications. Total dysfunction prevents use in all but pre-approved settings; whether in the privacy of the home or upon a stage in front of thousands, the content is only accessible under the permitted conditions. It can be argued that even this simple method of DRM is a privacy incursion because it strips individuals of the ability to experiment, create, or utilize legally purchased materials in their own homes. While conceptions of the home as a sanctuary in Western civilization extend back at least to classical Greece, in modern society the home is not an impermeable haven and the important privacy considerations are elusive and subtle.

Instead, this kind of DRM initiative should be acknowledged as a privacy threat because all use of protected materials must be sanctioned by a central authority. Many consumers utilize products in ways other than the purposes they are marketed for; for some of these users and uses, privacy is desired. Other uses, like DVD Jon's desire to watch films on his Linux computer, are not sensitive topics. In either case, even the most basic DRM systems give manufacturers the ability to reap unprecedented knowledge of the ways that consumers utilize their products. By default, manufacturers define the allowable uses of their products; with DRM all other uses require either a software patch, upgrade, or authorization from the copyright holder—or an illegal circumvention of the technological obstacle. Thus, even DRM with a simple inoperability trigger affect privacy by demarcating the actions of users so thoroughly as to generate an opportunity to monitor users and unapproved uses. DRM mechanisms of this kind should be

understood as incrementally beginning the loss of privacy because they identify individual users.

The next ring of DRM systems encompass technologies that are programmed to communicate with the manufacturer or copyright owner after an item is purchased and put into use. This technique is deployed in a myriad of permutations, all essentially involving a piece of embedded software transmitting information back to the provider via an electronic information channel. There is variance in these methods, existing in the amount and kind of information gleaned from users' devices, the link between the user and those that monitor, and the transparency of the interaction. The ability to identify, track, monitor, and aggregate data coalesce to form a significant loss of privacy for the end user.

Application of this kind of DRM system was at the core of the creation and marketing of the DIVX DVD. DIVX DVDs were designed to be disposable single-use discs that would circumvent the rental industry, enticing consumers with convenience and yielding greater profits for movie studios and consumer electronic manufacturers. Though the technology failed for several disparate reasons, it was predicated upon the copyright owner's control over a limited viewing window following the sale of each disc.[11] This window was established through a phone link between each DIVX player and a central server which triggered the initial viewing period once the disc was first initialized by the consumer. Every time a DIVX disc was inserted, this authorization process occurred, and later viewings could be purchased with a credit card. The convenience of disposability was countered by the inconvenience of connecting to a

central server, but this facet of the technology (and the attendant loss of liberty) was a clear quid pro quo for consumers.

There are several examples of the deployment of this kind of DRM system in home computing. In 1999, RealNetworks, a Seattle based multimedia software vendor, was discovered collecting data about users that downloaded free copies of its RealAudio software.[12] The software was programmed to record what CDs were inserted into a computer and what songs were copied, identify each user or machine with a unique serial number, and transmit the data back to the company's headquarters.[13] Additionally, it was capable of searching "users' systems for information about their musical preferences, as well as about other software products that they had installed."[14] In addition to RealNetworks, several other companies including Mattel, Netscape/AOL/Time Warner, and Qualcomm have used similar DRM systems.[15]

Critics of these programs have called them Trojan Horses because they are designed ostensibly for one function (IP protection) while secretly performing another: harvesting whatever information is accessible to create a profile of unique users.[16] The threat to privacy in this case, and in similar DRM methods that depend upon central authorization, begins with the required unique identification of users. Identified unique users can be tracked and monitored, and their actions collected in profiles for later examination. The social concerns of data mining are well documented; customer management systems like DIVX inherently strip users of their anonymity and open an avenue for a slew of subsequent repercussions. The link between systematic data harvesting, aggregation, and protecting the integrity of the IP that the DRM system was packaged with is tenuous—though the utility of gathering such data is easily imagined.

For privacy advocates, this process is a clear trespass on individuals' rights. Secret and couched in legitimate garb, these profiling measures create data shadows that can reveal taste, consumption patterns, or possession and use of pirated materials all while unbeknownst to the user.

Following the creation of these initial profiles, the DRM systems employed by RealNetworks, Netscape, and others are capable of ongoing monitoring. Since a continual link between the end-user and the vendor is established, an individual's actions and habits can be traced in great detail. In a way, these programs turn every click, keystroke, or number dialed into an occasion for transaction generated information (TGI). For example, "at least one version of Netscape's SmartDownload software recorded every web site visited by users…and transmitted that information to Netscape."[17] In a situation like this, no action can be taken without being seen—by a secret and invisible eye.[a]

The final level of DRM initiatives seek to organize a host of disparate interests into a unified and impermeable ring of defense against piracy or undesired usage. Whether promulgated unilaterally or by a consortium, these DRM systems are designed to envelope users, delimiting their experiences to those sanctioned by the vendors in the interests of 'trusted computing.' Liberty and privacy are affected in tandem; the systems combine proscribed boundaries and constant monitoring to ensure lasting and formidable

[a] Unlike the unspoken agreement between users and vendors in the DIVX case, these examples of this kind of DRM technique are invisible and operate without even implied consent. In some cases, the DRM measure may be referenced in a privacy agreement, but in others it is not. In the RealNetworks case, the company changed their privacy policy after the fact, before issuing a public apology for its data collection.[a] The actions of RealNetworks, Netscape, and other companies show a disregard for individual privacy rights when contrasted with their interest in reaping consumer data. The aggregation of information linked to an identifiable target is a serious affront to privacy rights—but there are limited legal restrictions on gathering this information. Consequently, vast databases of information can be created, analyzed, bought, sold, and traded regardless of the potential privacy repercussions.

security. An examination of two efforts at enacting trusted computing follows, assessing the reach and impact of this broad form of DRM.

Privacy advocates call Microsoft's Palladium initiative, part of an attempt to create a 'trusted' operating environment, "a system that establishes trust through control."[18] Now officially known as the *Next-Generation Secure Computing Base for Windows,* Palladium uses encryption, identification, and authorization to manage what programs are run and files opened while tracking each user via embedded unique machine identifiers.[19] Technically speaking, these aims are achieved by utilizing four strategies: memory curtaining, secure input and output, sealed storage, and remote attestation.[20] In addition, Microsoft is a member of the Trusted Computing Group (TCG), "an industry standards body" that it leads with Compaq, Hewlett-Packard, IBM, and Intel.[21] The TCG aims to increase data security, bolster defenses against hackers, and limit identity theft by creating seamless integration of hardware and software offered by its members.[22] In both of these cases, consumer benefit is highlighted while business interests are also served. To achieve this, privacy interests are co-opted into product marketing: by inserting their technical standards between individuals and the world at large, Microsoft et.al. suggest that they enhance privacy, but say little in corporate proposals of the developing privacy relationship between vendor and user.

Beginning in 2004, components of Palladium will debut in personal computers. Microsoft won two patents from the U.S. government relating to its Palladium initiative which reflect the widening scope of its operating system. By making architectural changes to the operating system, Palladium aims to create a more stable and secure enclosure for computing. One way it accomplishes this is by limiting what code is

processed by the computer. As related in the first patent application, "the digital rights management operating system refuses to load an untrusted program into memory."[23] A key determinative in this example is who determines what is a 'trusted' program: Microsoft or the consumer? While measures like this may protect the integrity of the operating system, they may also shift a modicum of control from the user to the controlling corporation (Microsoft).

This liberty concern is exacerbated by the new communication facets embedded and included with the system. Versions of Windows with Palladium will be equipped with a personal information agent called "My Man" that is the next step in Microsoft's Passport initiative to develop a universal form of identification for internet transactions. My Man would automate information exchange between vendors and your computer; it is likely that in some circumstances vendors will be granted the authority and ability by a source other than the individual to access each user's private details—without his knowledge.[24] Coupled with the kind of automatic data-feedback Windows XP users are familiar with (most obviously the automated error-reporting agent), privacy is eroded significantly. Palladium beckons the onset of computing systems in which only certain programs are allowed to run on *personal* computers, Microsoft or other vendors are alerted to attempted transgressions, and personal information is made ripe for the plundering.[b]

The Trusted Computing Group unites a group of vendors in an initiative similar to Palladium, but with greater reach and ubiquity. Though it is spearheaded by core computer companies like Microsoft, Intel, Compaq, Hewlett-Packard, and

[b] See Appendix A for Microsoft's corporate perspective and reaction to privacy concerns regarding Palladium.

IBM, it encourages companies of all colors to join. Other companies like Sony, Sun, and Fujitsu have joined at the "Promoter" level. For a $50,000 annual fee they are entitled to voting privileges and the ability to influence the standards as they are adopted and imposed.[25] There are also two other membership levels; with declining cost comes less influence, and applicants must be approved by the existing board before they are accepted to membership.

An important distinction between Palladium and the TCG standards is that the latter endeavors to fully integrate software and hardware. A 'trusted' environment will be created "through hardware-based cryptographic functions, protected storage of user data and secrets, mechanisms for secure storage and reporting of platform integrity information, and platform authentication with multiple attestation identities."[26] By banding a number of influential and disparate companies together, the entire consumer experience could potentially be enveloped. Utilizing all the aforementioned DRM methods, user management can be realized in unprecedented ways, with unprecedented implications. In addition, the consortium resembles a trade cartel in a very real way, and a body of criticism is centered upon the group's potential to choke out competition. Thus, TCG standardization could result in an environment in which each individual has a profile that documents what equipment he owns, files he possesses, information he views, data he processes, and when, where, and how these actions take place. If, as so far is the case, certain dominant companies shape and guide the standards to their collective advantage at the expense of competitors, their technological pervasiveness may near technological omniscience.

Surveying the efforts at "Trusted" computing reveals the pervasive nature of these technologies. Users are apt to be enveloped by these DRM systems to the extent that each keystroke and mouse-click is registered and recorded. The privacy implications of monitoring are manifold and they are amplified by the loss of choice and liberty imposed by software and hardware restrictions. If the ability to choose what is consumed is limited, and what is consumed is monitored, what happens to our other basic freedoms?

IV: Review of DRM Implications & Efficacy

Not only is protection for private information consumption currently absent in cyberspace, but the aggregation of usage data is tacitly allowed and even encouraged by the government. The three rings of DRM initiative detailed earlier reach progressively further into individuals' lives, first identifying, then profiling, and finally enveloping them. The most primitive circle of DRM systems, the inoperability techniques, limit liberty and sometimes may lead to identification, but they are generally directly tied to efforts to protect IP. Samuelson notes that copyright traditionally was applicable only to public performance or display, while DRM restricts private usage.[27] In addition, as depicted by the actions of DVD Jon Johansen, these systems have had little success. So, while defensible in part, DRM systems have extended beyond the limits of the copyright while typically failing to limit piracy.

Beginning with the most primitive DRM efforts, identification is consistently present in the design of DRM measures—basic and complex. It is an early step in subjugation; the loss of privacy that results in identification may also lead to a significant

loss of freedom. Identification is rationalized as a component of authentication and authorization but is also useful in quantifying and classifying individuals into groups.[28] Identification and the fear of scrutiny or repercussion can be a powerful deterrent: individuals may cease to dissent and opposition groups could lose leadership. If this happens, American democracy would lose part of its fundamental balance, threatening the existing social order. In this way, the individual loss of privacy can swell into a systematic and serious societal concern.

Identifying users is often a precursor to profiling them; more advanced DRM systems typically take steps to monitor individuals. Whether a necessary component of a technology, as in DIVX or even TIVO, or as a silent feature hidden in a device with an entirely separate function, identifying, monitoring, and profiling create a new realm of user information which is contrary to personal privacy through its existence. DRM technologies that monitor and profile can be used to record intellectual behavior and consumption. In a way, the thoughts that occur in people's minds are the most private, invisible aspects of life—any technology that reveals part of the thought process changes the balance of society. The traditional "right to be left alone" in the American legal construction of privacy includes a tenet that restricts intrusion upon seclusion. Though seclusion may be conceived of in physical terms, the loss of mental privacy should also be protected by the right to seclusion.[29]

Once databases containing uniquely identifiable records of consumption exist, they may be used for any imaginable purpose, by any number of actors. First, there is the risk that, even if information is collected for a legitimate purpose and approved by the user, the data may be accessible to others. This information may also be sold or

otherwise disclosed—for profit or other benefit but also by compelled production even if a privacy agreement that promises data security exists. Profiles create a permanent record of activity allowing transgressions to be punishable after the fact, or even after legal changes retroactively make actions illegal or punishable. As with other digital data, these records are easily copied, allowing them to spread easily and becoming increasingly resilient to obliteration with each replication.

In addition to legal repercussions and the chilling effect discussed above, individuals as consumers also face consequences of data aggregation and examination. The creation of consumer types and groups based on profile analysis may result in new forms of discrimination—precisely targeted at those who already occupy disadvantaged positions in society.[30] To begin with, consumers cannot rationally provide consent for the myriad of analyses that may flow from TGI records. Additionally, consumers with the most limited resources (educational and financial) are likely to be the consumers that would suffer from commercial profiling; they are also the least able to engage corporate behemoths in a dispute. From a business perspective, appealing to the wealthiest demographics is imperative. Since these customers drive profits, it is important to attract their business and loyalty; this may mean offering some customers better deals than others based on past data profiling. When applied, this practice is insidious because it stratifies society further, eroding the level playing field that is part of the American myth and negatively affecting the already disadvantaged: "The use of predictive models based on historical data is inherently conservative. Their use tends to reproduce and reinforce assessments and decisions made in the past."[31]

The most ambitious DRM projects attempt to engender an atmosphere of 'trusted' computing via standards, encryption, and monitoring. These platforms and alliances approach IP and its usage holistically and try to create a safe environment. In doing so, they envelope users, placing the consumer at the center of a web of associated technologies. When all these techniques work in concert, all facets of a user's activities are regulated and recorded by the DRM systems. As the developing consortia grow to include companies producing televisions, telephones, computers, and content, ever greater amounts of an individual's life can be captured. When using these technologies, choice is limited and privacy nonexistent.

The power vested in manufacturers and standards boards is ominous. It is important to realize that even without the rise of an evil state based in Redmond, Washington, other subtle effects of 'trusted' computing are deleterious. For example, the profiles that are generated in these user envelopes will be accurate to the most minute extent and individual opportunity and choice will be affected. Free thought and speech is also impacted by the insertion of corporate filters into the information environment; websites or software deemed threatening may be eliminated from user purview—without their knowledge. These standards bodies raise the cost of entry into industry as well, making start-ups costlier and potentially limiting innovation. Any witness to the stream of exploited weaknesses in Windows to this point is wise to carefully consider the utility of an operating system empowered with more private information.

V: Conclusions

Legal scholar Pamela Samuelson views DRM technologies as a serious threat to science, progress, and society because, while couched in the rhetoric of piracy and copyright protection, in practice DRM systems have vastly exceeded the intent of the traditional copyright.[32] Even if they were designed solely to protect IP rights, DRM initiatives have evinced little potential in limiting piracy—which is more rampant now than ever because of a number of slippery online distribution channels. Samuelson goes so far as to say that, "The main goal of DRM mandates is not, as the industry often claims, to stop "piracy" but to change consumer expectations.[33] If one effect of DRM is to reorient the consumer's expectations, another is to collect information about this disposition and its expression. For privacy scholars, the exploitation of the DMCA by DRM systems to allow large-scale, systematic data gathering is an egregious affront.

The anti-circumvention clauses in the DMCA pose an opportunity for corporate business interests to design DRM techniques that remake the marketplace to their specifications. Written with control over IP rights in mind, the legislation prompts a shift in the locus of control away from the government and towards private interests. DRM systems determine both what uses of content are legal and what the punishment for violating the strictures will be. Beyond this, the systems have been designed in ways that penetrate deeply into individual's private lives when there is no necessity beyond corporate advantage. These intrusions into seclusion are not innocuous and the legislation that permits them should be reassessed.

Maintaining a shroud of privacy over the mundane yet sacred daily details of life is important. The simple loss of dignity that occurs with the loss of privacy should not be undervalued, but more relevant is the possible impact on individual expression and

behavior. Private library use and even video rental are rights protected by the Federal government as necessary elements for the formulation of an informed public sphere and free speech—institutions that exist at the core of America.[34] There is an undeniable migration of information and intellectual research to online resources: it is important to extend protection for private intellectual activity to cyberspace as well. Whether users read *The New York Times*, refer to the Lexis/Nexis database, or search via Google, their information gathering mirrors what scholars have traditionally done offline. Allowing monitors of their electronic actions to exist could cause a powerful chilling effect: if there is any fear of recrimination, there is a chance for controversial or unpopular intellectual activity to be stifled by fear. If a loss of privacy prompts fear, which in turn halts research and discussion, one of the fundamental pillars of American life is eroded.

By nature, DRM systems are designed to remove uncertainty and invisibility from the marketplace and empower owners and producers of IP. "The most important aspect of IPRs is their formal construction of scarcity where none necessarily exists;"[35] while DRM technologies manage to make informational privacy increasingly scarce.[36] By limiting the utilization of existing IP, a trade-off between profit and progress is designed. "Knowledge and information, unlike material things, are not necessarily rivalous, co-incident usage does not detract from utility."[37] DRM systems permitted by the current interpretation of the DMCA "impede the progress of science, [are] economically unjustifiable, and lack the balance that the Constitution requires of IP legislation."[38] Despite this, greater short-term profits may be realized.

Privacy enhancing technologies exist, but are developed by fewer companies with less manpower than the parties developing DRM. In addition, they face the scrutiny of a

government which fears privacy in the hands of individuals.[39] Some observers have offered a plan for PRM: privacy rights management.[40] Similar in many ways to DRM, PRM shifts control of information sharing into the hands of individuals and the intermediaries they select. It is an interesting reversal of the current system, but cost and security are among the concerns that threaten its viability. Relying on marketplace solutions may be a misstep because corporate clout and resources are overwhelmingly on the side of DRM. Additionally, due to the esoteric nature of this debate, public comprehension will likely never be high enough to apply sufficient pressure to cow corporations. There are other voices in the debate: trade groups, watchdog organizations, and the media may all challenge the status quo, but their might is limited in the face of corporations, a pro-business government, and an apathetic public.

Beginning with the Constitution, America's history is characterized by innovation and profit. Copyright protection is a fundamental tenet that protects and nurtures creativity which in turn is the engine for progress. In the digital environment, the balance between progress and profit is threatened; the DMCA and the DRM systems it spawns are an attempt to restore order to creation and consumption in the modern world. To this end, the DMCA and subsequent legal decisions have allowed DRM technologies to grow too invasive. The technologies are too extensive and unregulated; left unchecked, they will stifle creativity and expression in a fashion toxic to individual and national well being.

Among privacy scholars, the consensus is that the DMCA's anti-circumvention technologies are too empowering. A first step in corralling the reach of DRM technologies would be to allow circumvention under more conditions. Legal scholars

suggest that "the act-of-circumvention rule initially sought by the Administration was simpler" and that it has grown more nuanced and responsive in progressive iterations.[41] An initial reassessment of the DMCA, followed by periodic reviews of its expression and effect could contribute to establishing the proper balance between property and privacy, profit and progress. Most importantly, the government must be the party that defines legal and illegal behavior—rather than those with vested interests. With minor steps to narrow the license granted to private interests developing DRM, privacy and its benefits may be ensured while business maintains its profitability and innovation is encouraged.

Lee Shaker
Annenberg School for Communication

Appendix A

Microsoft is aware of privacy and liberty concerns, and the company touts Palladium as a privacy boon. According to the company's white paper detailing Palladium, it "must provide the means to protect user privacy better than any operating system does today."[42] Identity theft, malicious viruses, and data security are important issues to users; as a business, Microsoft must recognize and address these needs to satisfy its customers. The company also has strategies to maximize profitability, some of which conflict with its commitment to privacy. For example, the second patent secured in reference to Palladium states:

> "The guaranteed loading of a digital rights management operating system on a general-purpose personal computer ensures that downloaded content can be protected from unauthorized access. Furthermore, the generation of an identity for an operating system based on its loaded components allows a content provider to knowledgeably determine whether to trust content to the subscriber computer."[43]

This tenet speaks to corporate interests—at the expense of individuals, their privacy, and their liberty. First, it describes a system that prevents users from opening content without authorization—as determined by vendors. Next, it profiles users based on their behavior, including what files they have and what they have tried to do with them. Based on this assessment, the offers and opportunities available to users can then be varied. The following passage is excerpted from Microsoft's Windows Media Player end-user licensing agreement:

> "Digital Rights Management (Security). You agree that in order to protect the integrity of content and software protected by digital rights management ("Secure Content"), Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. If we provide such a security update, we will use reasonable efforts to post notices on a web site explaining the update."[44]

Policies like this are already part of Microsoft's modus operandi, and Palladium is an extension of this ethos from one program to an entire platform. Though there may be legitimate and beneficial aspects of the Palladium initiative, it also imbues Microsoft with an unprecedented level of power and license in determining the user's experience.

---

[1] Cohen, J. E. "DRM and Privacy." *Communications of the ACM* 46(4): 47-49.

[2] Jackson, M. "Using Technology to Circumvent the Law: The DMCA's Push to Privatize Copyright." *Hastings Communication and Entertainment Law Journal* 23: 607-646.

[3] National Research Council. *The Digital Dilemma: Intellectual Property in the Information Age* (Washington D.C., National Academy Press, 2000).

[4] Cohen, J. E. "Overcoming Property (Does Copyright Trump Privacy?)," *University of Illinois Journal of Law & Tech. Policy* 375: 101.

[5] Jackson, M. "Using Technology to Circumvent the Law: The DMCA's Push to Privatize Copyright." *Hastings Communication and Entertainment Law Journal* 23: 607-646.

[6] Pack, T. "Digital Rights Management." *EContent* 24(3): 22.
[7] Oksanen, V. "Transnational Advocacy Network Opposing DRM: A Technical and Legal Challenge to Media Companies." *International Journal on Media Management* 4(3): 156-163.
[8] National Research Council. *The Digital Dilemma: Intellectual Property in the Information Age* (Washington D.C., National Academy Press, 2000), 172.
[9] http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/
[10] Cohen, J. E. "DRM and Privacy." *Communications of the ACM* 46(4): 47-49.
[11] National Research Council. *The Digital Dilemma: Intellectual Property in the Information Age* (Washington D.C., National Academy Press, 2000), 168.
[12] Cohen, J. E. "DRM and Privacy." *Communications of the ACM* 46(4): 47-49.
[13] SOFTWARE MAKER SECRETLY COLLECTS PERSONAL DETAILS, AP, November 2, 1999 The Toronto Star.
[14] Cohen, J. E. "DRM and Privacy." *Communications of the ACM* 46(4): 47-49.
[15] Ethan Preston, *Finding Fences in Cyberspace: Privacy, Property and Open Access on the Internet*, 6.1 J. TECH. L. & POL'Y 3, <http://grove.ufl.edu/~techlaw/vol6/Preston.html>(2000).
[16] SOFTWARE MAKER SECRETLY COLLECTS PERSONAL DETAILS, AP, November 2, 1999 The Toronto Star.
[17] Cohen, J. E. "DRM and Privacy." *Communications of the ACM* 46(4): 47-49.
[18] http://www.epic.org/privacy/consumer/microsoft/palladium.html
[19] EPIC Alert Volume 11.01, January, 14, 2004 http://www.epic.org/alert
[20] http://www.eff.org/Infra/trusted_computing/20031001_tc.php
[21] https://www.trustedcomputinggroup.org/home
[22] https://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf
[23] http://www.epic.org/privacy/consumer/microsoft/palladium.html Digital Rights Management Operating System, No. 6,330,670
[24] http://www.theregister.co.uk/content/4/25852.html
[25] https://www.trustedcomputinggroup.org/join/levels/
[26] https://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf
[27] Samuelson, P. "Digital Rights Management {and, or, vs.} the Law." *Communications of the ACM* 46(4)
[28] Gandy, O. "Exploring Identity and Identification in Cyberspace." *Notre Dame Journal of Law, Ethics & Public Policy* 34: 1085-1111.
[29] Cohen, J. E. "DRM and Privacy." *Berkeley Technology Law Review* 18: 575.
[30] Gandy, O. "Exploring Identity and Identification in Cyberspace." *Notre Dame Journal of Law, Ethics & Public Policy* 34: 1085-1111.
[31] Gandy, O. "Exploring Identity and Identification in Cyberspace." *Notre Dame Journal of Law, Ethics & Public Policy* 34: 1085-1111.
[32]Samuelson, P. "Digital Rights Management {and, or, vs.} the Law." *Communications of the ACM* 46(4).
[33] Samuelson, P. "Digital Rights Management {and, or, vs.} the Law." *Communications of the ACM* 46(4)
[34] http://www.epic.org/privacy/vppa/ Video Privacy Protection Act of 1988 (Bork).
[35] May, C. "Digital Rights Management and the Breakdown of Social Norms." *First Monday* 8(11).
[36] Samuelson, P. *Privacy as Intellectual Property*. Proceedings of Financial Cryptography 2000 Conference.
[37] May, C. "Digital Rights Management and the Breakdown of Social Norms." *First Monday* 8(11).
[38] Samuelson, P. "Digital Rights Management {and, or, vs.} the Law." *Communications of the ACM* 46(4)
[39] Cohen, J. E. "Overcoming Property (Does Copyright Trump Privacy?)," *University of Illinois Journal of Law & Tech. Policy* 375: 101.
[40] Korba, S. and Korba, L. "Applying Digital Rights Management Systems to Privacy Rights Management." *Computers & Security.* 21(7): 648-664.
[41] Samuelson, P. *Privacy as Intellectual Property*. Proceedings of Financial Cryptography 2000 Conference.
[42] http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp#core
[43] http://www.epic.org/privacy/consumer/microsoft/palladium.html Loading and Identifying a Digital Rights Management Operating System, No. 6,327,652

[44] http://www.onlisareinsradar.com/archives/000478.php