Abstract
While Digital Rights Management (DRM) technologies have evolved as tools for the control of access and usage of digitized information resources over the internet, concerns continue to increase over their roles as systems that can be used as possible means of intruding into the private activities of consumers of digital contents. DRM technologies possess the ability to gather information about users’ intellectual, social and psychological preferences. The consumption of various forms of digital contents, in the age of the open access paradigm depends on a number of subtle, surprisingly complex, and at times conflicting elements of law, public policy, economics, and technology; elements that must be kept in relative balance in the light of today’s accelerating transformation of all types information into digital form. Unfortunately, open access also enables unauthorized usage of resource by those who deprive copyright owners the right benefits for their efforts. This paper reviews the impact of changing technology on information storage on the internet. An attempt is made to elucidate the privacy interests enjoyed by individuals when engaged in intellectual activities and the possible negative impact DRM features such as monitoring and constraints could portend for privacy rights. While advocating for a balance between DRM, protection of author’s rights and the right to privacy of individual domain, we conclude that deliberate effort must be made to beef up intellectual property law in the context of current storage innovations in order to cater for the subtleties introduced by the impact of modern storage and protection technologies.

Keywords: Access, Books, Digital, Library, Internet, Intellectual Property, Law, Storage, Web and Technology

Introduction
Technological advancements have produced radical shifts in the ability to reproduce, distribute, control, and publish information. Information in digital form has radically changed the economics and ease of reproduction. Reproduction costs are much lower for both rights holders (content owners) and infringers alike. Digital copies are also perfect replicas, each a seed for further perfect copies. One consequence is an erosion of what were once the natural barriers to infringement, such as the expense of reproduction and the decreasing quality of successive generations of copies in analog media. Today, a world of information is available with little effort and almost at no cost to the user. Such access to information has played a central role in education and social life from time immemorial. Yet the very possibility of borrowing a book, whether from a library or a friend, depends on a number of subtle, surprisingly complex, and at times conflicting elements of law, public policy, economics, and technology; elements that must be kept in relative balance in the light of today’s accelerating transformation of information into digital form. Access to resource materials in an age where libraries are getting computerized, digitized and virtual is obviously without limits. Unfortunately, this ease of access also enables unauthorized usage of resource materials as well as subtle monitoring that enables those with the right technology to track information usage pattern on networks and computing infrastructures.

Changing Technology and Content Protection
Representing information in contemporary times in digital form, as opposed to the more traditional analog form, means using numbers to capture and convey the information. Music offers a clear example of the difference between the two. Capturing musical sounds requires describing the shape of the vibrations in air that are the sound. Records capture that information in the shape of the groove in the vinyl. CDs, by contrast, capture the same information as a large collection of numbers. Digital information has a remarkable breadth of descriptive ability, including text, audio (music, speech), video (still and moving pictures), software, and shape (e.g., in computer-aided design). When information is represented digitally, access inevitably means making a copy, even if only an ephemeral (temporary) copy.
(a) Digitization: In all of these cases, the size of the digitized file containing information can be made considerably smaller by compressing it. The simplest compression techniques rely on finding more compact ways to capture the same information. One technique, called "run length encoding," takes advantage of the fact that numbers can repeat. A variety of more sophisticated compression algorithms are available, many of which rely on specific properties of the information being compressed. Video compression, for example, often relies on the fact that typically very few things in a scene change from one frame to the next. This makes it possible to encode one frame by indicating only what changed compared to the previous frame.

(b) The Connection between Access and Copying in the Digital Mode: Reading a book does not involve making a copy of it, nor does watching a movie or listening to a song. This intimate connection between access and copying has considerable significance in the context of intellectual property protection. One of the essential elements of copyright (the right to control reproduction). In the world of traditional media, there is an obvious distinction between access and reproduction. The copyright owner's control of reproduction provides just that. But in the digital world, where no access is possible except by copying, complete control of copying would mean control of access as well. This has consequences for all parties involved. Rights holders may seek to control access to digital information, because access involves reproduction. Readers may find their traditional access to information susceptible to control in unprecedented ways. Policymakers, meanwhile, must consider how to maintain the appropriate balance between control and dissemination (Stallman, 2002).

(c) Economics, Character, and Speed of Digital Reproduction: Digital representation changes both the economics and the character of reproduction. Copying digital information, even on a home computer, is easy and inexpensive: A standard (1.44 megabyte) floppy disk, which holds the equivalent of about 500 pages of text, takes no more than a minute to duplicate and is treated as if it were a piece of paper (e.g., routinely given away). A CD, which holds 700 megabytes (the equivalent of about 220,000 pages, or 44 cartons), can be copied in 15 minutes to a blank compact disk that costs less than $2. The advent of digital information brings an extraordinary increase in the amount of information that can be easily and inexpensively reproduced. Consequently, the traditional physical and economic impediments to copyright infringement have been considerably undermined. The character of reproduction has changed as well. Although a photocopy often is not as sharp as the original, a digital copy is indistinguishable from the original as are all successive digital copies. With the traditional form of information, the successively lower quality of each generation of copy offered a natural limitation to redistribution. With digital information there are no such limitations.

(d) Separating Intellectual Materials from the Containers: Information in digital form is largely liberated from the medium that carries it. When information is sent across networks, there is no need to ship a physical substrate; the information alone flows to the recipient. The liberation of content is also evident when bits are copied across media (disk to tape to CD to flash) with the greatest of ease. The choice of media may have consequences for the amount of storage or speed of access, but the content of the information and its properties (e.g., the ability to make exact copies) are preserved perfectly across a variety of media. The liberation of content from the medium has unsettling consequences for the protection of intellectual property (IP) in digital form.

(e) The Plastic Nature of Digital Information: Digital information is easily searched, indexed and cross-indexed. It is "plastic" in the sense that it is easily changed. Although a paper book is difficult to alter and hard to search even with a good index, online text can be changed easily, for instance, by adding and rearranging paragraphs. Coupled with digital transmission, plasticity of information confers, along with great advantages, the potential for fraudulent acts such as plagiarism or forgery. The ease of searching and indexing digital information enormously facilitates the creation of derivative works of unusual forms. In a similar vein, a practice on the Web known as "framing" has raised a number of intellectual property related questions, particularly in the commercial context.

(f) Remote Access: Remote access removes the need for geographical proximity, eliminating another of the familiar limitations of information in traditional forms. As a consequence, digital information presents opportunities for access and violations that are vastly greater than those presented by traditional media. Most pirates and counterfeiters are interested in making quick and (preferably large) profit by producing many copies of a product and then moving on to exploit another. Thus, the extended consumer type market provided by the sudden emergence of the various forms of the microcomputer was a real attraction to the illegal operators some of who migrated across from producing counterfeit copies of music audiotapes and books.

The Illusion of Privacy
The threat from invasion and unauthorized usage of digital content over the Internet is very real. Content providers can provide authorization and access control to ensure that only paying users can access content. They can also use encryption to protect content during transport. The major challenge therefore is how to control what customers do with the purchased content once it reaches their premises. As a result of the limitations involved in controlling what customers do with Internet contents of all types, content owners are reluctant to release valuable content in digital
format because they fear for the unauthorized usage of their content (What is now popularly referred to as napsterization) (James, 2003). New technologies called “ubiquitous computing” now include the ability to track an employee’s location at all times.

When we use shared folders, download assignments, and browse the Internet, data are gathered directly and indirectly about us. From what feels like privacy, we participate in on-line chat rooms, leave a message on a bulletin board, shop online, and register with a commercial site. With more classes and degrees offered online, education is becoming consumer oriented. Knowledge is now considered a content commodity. Students have a sense of being in control with access to information anytime and anywhere. Ironically, on the Internet, users are more visible and open to surveillance.

Information Trailing in the Digital Age
Developments in digital trailing systems have advanced to an extent that they can now be used to track the time users spend online, noting log on and log off. It enables the observer to calculate the time taken to perform a task, to note laziness, to evaluate the aptitude of the observed, to judge performance, to assess success, to monitor the nature and type of the consumed content and to classify the observed. It all boils down to the fact that the sense of autonomy, anonymity, privacy and control over one's intellectual and social consumption especially on the Internet is an illusion!

Digital Rights Management (DRM) and Privacy Implications
As a result of the limitations involved in controlling what users do with Internet contents of all types, content owners are reluctant to release valuable content in digital format because they fear for the unauthorized usage of their content. Napsterization still being very fresh in their memories. Technology is available that enable content providers provide authorization and access control to ensure that only paying users can access content. They can also use encryption to protect content during transport (Chiemeke & Longe, 2007; Longe & Chiemeke, 2006). The major challenge therefore is how to control what customers do with the purchased or available content once it reaches their computing facilities. Protecting digital content has to go beyond the prevention of illegal file sharing common in the musical world. Current efforts must embrace the development of techniques that can alter the paradigm of content owners so that they perceive the distribution of digital content over the Internet as an opportunity rather than- as a threat (Moffaert et al, 2003).

Digital Rights
Digital rights refer to copyright and related rights over digital contents (digital contents can be text (data), audio, and video streams in digitized version). The goal of digital content protection can be summarized as the identification/definition of digital rights and the implementation of digital content usage rules using proven digital content management techniques. DRM enable legitimate owners of intellectual property to regulate the right of access to their assets via electronic means. There is a strong ambivalence about digital products and the Internet. The network provides a vibrant market for digital products; however, once stolen, digital products can be broadcast quickly to all corners of the earth. According to Moffaert (2003) the term “Digital Rights” refers to copyright and related rights of digital content (data, audio and video). Digital Rights Management is sets to achieve the following goals:

(a) Identify digital rights;
(b) Describe associated usage rules and
(c) Enforce these usage rules using Digital Rights Management Software.

In designing and implementing DRM systems, there are two critical architectures to consider. The first is the functional architecture, which covers the high-level modules or components of the DRM system that together provide an end-to-end management of rights. The second critical architecture is the information architecture, which covers the modeling of the entities within a DRM system as well as their relationships (Hoeifmester, 2000). The overall DRM framework suited to building digital rights-enabled systems can be modeled to manage the creation of content so it can be easily traded. Manage and enable the trade of content. This includes accepting content from creators into an asset management system and manages the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software (Renato, 2001).

Content Protection over Cables
Conditional Access Systems (CAS) popularly implemented using decoders Set Top Box (STB) was developed mainly to protect content delivered over cable and satellite networks and displayed on TV sets. Contents are transmitted and delivered through a STB that is secured using Smart cards. The smart card, which is "owned" by the consumer is a Tamper-Resistant Device (TRD) into which the smart card is inserted (e.g. the crypto modules). The STB stops
functioning completely when the smart card is removed (Schneier, 1996).

Principles for Implementing Protection over Cables

In protecting contents over cable, the content is encrypted before being sent over the network and the encryption keys change frequently. At start-up, the network authenticates both the smart card and the STB hardware. When a client is interested in particular content, the client sends a request to the content provider who checks the request against a policy database. When the client is authorized to receive the content, the content is streamed and the correct decryption keys and key updates are sent over a secure connection initially set up between the content provider's server and the customer's smart card. The principle is illustrated in Figure 1.

![Fig. 1: CAS for Distributing Digitized Content over Cable](source)

Usage control after the content download is fairly easy. The STB usually has only an analog output interface to a TV. Although the STB is on the customer's premises, it is largely controlled by the smart card and the fact that the STB are tamper-resistant. Although the analog output could be used as a source for pirated copies, this would result in serious degradation from digital to analog quality (as opposed to digital copying where degradation in quality does not occur). The experience is the same when content is distributed via traditional TV and Video Tapes.

Developing Analogous Protection for Internet Content

The development of an analogous protection system for contents downloaded via a client PC is a much bigger challenge, as the PC is an open platform over which the content provider has little or no control. The content provider must, as a matter of necessity, take additional measures to control the usage of the digital content after it has been stored on the end user's system. Traditional CAS will not suffice in this case. An emerging trend is for clients to increasingly deploy client networks to connect to the Internet via Digital Subscriber Line (DSL) rather than connecting a single computer or STB. It is possible for a user to buy or license content that can then be accessed on different devices within one network without losing the protection and control over usage of content and without the need to pay a separate license fee for each device on the network.

![Fig. 2: Framework for Content Protection over the Internet](source)
Chiekeme & Longe, (2007) proposed the development of an analogous protection scheme for internet content (Fig. 2). The architecture is based on a separate distribution chain for encrypted content on the one hand, and for usage rules and the decryption key on the other. Encrypted content together with a small amount of metadata is digitally signed and stored on a web download or streaming server. Metadata is descriptive data associated with the content. It may vary in depth from merely identifying the content title or providing descriptive information to populate an electronic program guide, to providing business roles detailing how the content may be displayed, copied, or sold. The metadata also provides the information necessary to retrieve the correct usage rights and the keys for decrypting the content. The combination of usage rules and the correct key to decrypt the content would in this architecture depict the license.

Some philosophers conceive of “privacy” as a condition of inaccessibility or limited accessibility to the rest of the world (Jeff, 1999; Cornish, 1990). Invasions of privacy involve rendering the individual more accessible to others in some way. The future of copyright and the future of copyright enforcement raises deeper questions about the nature of privacy and what counts, or ought to count. Despite all, the protection it affords owners of contents, DRM technologies are poised to affect both the spatial and informational dimensions of intellectual consumption. These technologies therefore affect both spatial and informational dimensions of the privacy that individuals customarily have enjoyed in their intellectual activities (Julie, 2003).

Apart from the questions of intellectual property policy that surround DRM technologies, the proper balance between DRM and user privacy is an important question in its own right. Interrogating the relationship between copyright enforcement and privacy raises deeper questions about the nature of privacy and what counts, or ought to count. DRM technologies are designed to report back to the information provider on the activities of individual users. This restrictions amount to an invasion of privacy. Using DRM technologies, much of this record-keeping activity is conducted automatically, without the direct involvement of a human observer or controller, but the fact of automation does not
necessarily neutralize the threat to privacy interests. The relevant question, instead, is whether information about intellectual consumption is gathered and stored in a form that is both personally identifiable and potentially accessible to others (Jeff, 1999). If the information exists in such a form, it is subject to disclosure or compelled production. Absence of stringent privacy protections and the threat of disclosure may discourage intellectual exploration, and therefore compromise intellectual privacy interests. DRM monitoring technologies can have second order privacy effects. Specifically, data gathered through monitoring can later be used to generate detailed profiles of users’ revealed intellectual preferences. The information provider can use the resulting profiles to market additional information goods to users, or can sell it to third parties who may use it for a wide variety of other purposes.

(c) The Technologies of Self-help
At times, direct restriction protocols are designed to encode penalties as well as features that disable access to a content upon detecting unauthorized usage. These self-help technologies can be directed and controlled externally upon detection of prohibited activities. They therefore present a special case of the constraint problem and potentially, a special case also of the monitoring problem. The punitive quality of self-help systems implicates privacy interests because the identification of a particular customer or user as a target for self-help measures entails loss of the relative anonymity usually enjoyed by an individual among many customers or users. By inserting self-help automated functions into private spaces and activities, these technologies elide the difference between public/rule-governed behaviour and private behaviour that is far more loosely circumscribed by applicable rules and social norms.

Conclusion
Technology changes rapidly, making previously secure systems progressively less secure. Social environments also change, with the defeat of security systems attracting more (or less) interest in the population. Just as in physical security systems, there are inherent trade-offs between the engineering design and implementation quality of a system on the one hand and the cost of building and deploying it on the other, designers of digital content must employ imperatives that will balance reward for copyrighted works and accessibility to users. In the words of Alrashid et al (1998), the best that can be hoped for is steady improvement in method, quality and affordability and keeping a step ahead of those bent on defeating the protective schemes. As with every other security measure, protecting digital contents comes at a cost. A trade off must be made between security, strength, cost and ease of use.

The Deployment of DRM technologies raises questions about the nature and function of the boundary between public and private spheres. Although DRM technologies represent the future of secured and profitable information access and use, their design and use raises open questions. A shift to an information environment characterized by pervasive constraints and universal monitoring will severely undermine intellectual privacy. To balance the odds, law and technology will have to synergize in sharing the responsibilities for protecting intellectual privacy. Law will have to define individual rights and correlative obligations while DRM technology designers must come to terms with the importance of the law, and more broadly of public policy and values in establishing design parameters. The time to do that is now – before highly restrictive technical proposals and highly pervasive and permissive legal responses harden into legacies that will prove far more difficult to dislodge.

References
Jeff, S (1999): opting-in, Opting-out, or No Options at All: The Fight for Control of personal Information. Wash Law review. Vol. 74, No. 1033
James, E. (2003); Securing Deliberate Autonomy. Stanford law review. Vol. 8, No. 1


