Technological Copyright Enforcement and Open Access

Volker Grassmuck
for
Open Archives Forum Workshop
27.-29.3.03
HU Berlin

Luckily, I can spare you an introduction to general copyright issues because Mark Bide did an excellent job at that in his expert report for the OA-Forum in November 2002, „Open Archives and Intellectual Property: incompatible world views?“ [Bide 2002]. I also agree with his conclusion, that „there is ultimately no conflict between Open Archives and Intellectual Property – but open archives must work within the framework of Intellectual Property law as outlined here.“ I will take it from

there, and focus on the framework of intellectual property *technology*, and what conflicts arise from it for freely sharing information.

1. The Problem

What one perceives as a problem, of course, depends on one‘s vantage point and one‘s goals. Two main perspectives can be distinguished: open or proprietary knowledge, sharing or selling of information.

From the first perspective, openness of the architecture of cyberspace is a given. Issues arise as to how a distributed archive can be made searchable in a consistent manner, how it fits with the general project of a Semantic Web, how a long-term preservation and accessability of information can be achieved, how free information can be protected against closure etc. -- issues to which the OAI is working to develop solutions.

The second perspective is most of all that of the exploiters of copyrighted works. To them, the problem of cyberspace is twofold. One is the nature of information itself, i.e. that its consumption is non-exhaustible and non-rivalrous. To talk of „consumers“ of information is misleading. Information is not consumed by its use. Digital information by its very nature is abundant, but markets need scarcity. „The malleable and vaporous nature of digitized content“ is how a recent WIPO report put it [WIPO 2002]. Like alcohol, it seems, if you don‘t put a lid on, it evaporates. The other problem is the open architecture of PC and Internet. Whatever technology you devise to make a computer protect your data, a smart hacker can undo with the help of the same freely-programmable general-purpose machine.

2. The Solution: DRM

The solution of the media corporations to their problem is to change the nature of information: making it behave like material goods, exhaustible and rivalrous. The information itself will still be there after „consumption“ but the license will have been used up. It turned out that this can only be achieved by overcoming the second „problem“ as well, the open architecture of cyberspace.

The solution has two parts again. One is technology: DRM, and since that alone didn‘t turn out to be able to do the job, law: the new *sui generis* protection for this class of technology against circumvention that is currently being implemented throughout the globe. (On the global level, this *lex DRM* is the WIPO Copyright Treaty of 1996, for Europe it is the EU Copyright Dirctive of 2001 which is currently being implemented into the member states‘ copyright laws.)

What is DRM?

> *„Digital Rights Management (DRM) is the umbrella term for new business processes designed to unleash the tremendous capabilities of the Internet.“* (InterTrust)

> *„A more favorable way to look at trusted systems is to compare them to vending machines.“* (Mark Stefik, “Letting Loose the Light” 1996, S. 13)

> *„So loosely is the term used these days that no single definition of any use fits all the systems and operations to which it is generally applied. ... A sophisticated DRM system ... sets out to create a virtually all-embracing automated commerce system for digital information... The scope of functionality of a sophisticated DRM platform is thus, in theory, unlimited.“* (Nic Garnett, InterTrust 2001)

The term „Digital Rights Management“, coined by InterTrust, the company that pioneered the DRM market in 1990, is first of all a misnomer, as Mark Bide [2002] has pointed out in his report already. Abreviating „copyrights“ to „rights“ suggests that there is only one kind of rights in digital space, that only the exploiters of copyrighted works have digital rights. Suppressed -- not only rhetorically but also practically by technical means -- is the fact that also citizens have rights in cyberspace, e.g. the inviolability of the home, privacy, and participation in cultural life through access to published works in libraries and through private copies.

More precise would be therefore the version of Richard Stallman who recommends to speak of „Digital Restrictions Management“ [Stallman 2003]. That is very much to the economic point of DRM: to create scarcity in an environment that only knows „malleable and vaporous“ abundance, by imposing restrictions on usage, in order to then offer to dispel the scarcity as a service. When with a book or a CD we purchased all privately possible forms of usage, the technology now permits to prevent copying, backin-up, lending, extracting (by cut-and-paste) etc. etc. and to sell these functions separately.

At the heart of the technocratic vision of DRM is technology that permits to make the intercourse with knowledge controllable to a degree only dreamed of by dystopian writers like George Orwell. DRM is technology for 1.) access control in order to exclude non-authorized users, and 2.) usage control for authorized users. DRM controls who uses what, when, where, and in what way, and it does so throughout the „commercial lifecycle“ of the data. DRM is not a single technology, but by its own logic has to be an infrastructure of various components and layers that in order to function as intended has to be seamless, watertight, and ubiquitous -- „virtually all-embracing“ [Garnett 2001].

Just as an aside, DRM is related to DPM -- „Digital Policy Management“, concerning corporate information policies, e.g. non-disclosure policies and, also internally, rules on who may show what information to whom. This is unrelated to copyright but ruled by employment contracts and by data protection, trade secret and other laws. Florian Schneider, an activist from the „Open Borders“ campaign and „No Person is Illegal“, the other day pointed out another parallel to me. The officials dealing with these issues are now talking about „Border Management“. Just as with digital information, the goal is filtering and controlling flows of people across borders.

At the heart of the societal issue of DRM is the question whether the increasing reciprocal penetration of society and cyberspace will lead to a people‘s government, a democracy, or whether Digitalia, that country in which all of us are living, working, learning, teaching, communicating and relaxing to an increasing degree will turn into a privately operated shopping-mall. A central question is: who gets to decide? When PC and Internet caused a revolution, then DRM is the counter-revolution.

Four Stages of DRM

In the history of DRM one can distinguish four generations or paradigms:

0. Pre-History
1. Static Stand-Alone Systems
2. Dynamic Systems (revocation and renewability)
3. Secure Boot and crypto infrastructure

Pre-History

Ted Nelson who in the 1960s invented the concept of hyper-text, also came up with a mechanism to incorporate portions of other network-based documents into one‘s own work. This „transclusion“ is not only supposed to allow back-tracking every quotation to its origin but also automatic tracking of ownership, a concept he calls „transcopyright [Nelson 1997]. If someone purchases my article, she will pay me for my work. Since the quotes from other peoples‘ work are contained only as active pointers to the original, the royalties for them will be paid automatically to their respective authors -- given a byte-oriented payment scheme. The recipient of my text can then re-use these quotes in the same way in works of her own. Nelson‘s is a vision of free re-usability and perfect copyright. It‘s also an unlikely vision because such a system would drown in its own transaction costs.

Actual DRM technologies have their roots in developments in the informatics industries (copy-protection for software) and in the audiovisual consumer electronics (e.g. conditional access control on set-top boxes for pay TV).

The first generation of digital recording technology on the consumer market was DAT (Digital Audio Tape). By the mid-1980s the technology was ready, but intervention from the music industry prevented Philips and Sony from marketing it. The technological compromise that was reached eventually was the *Serial Copy Management System* (SCMS). Since you can‘t really prevent a recorder from recording, SCMS is intended to at least block copying of copies. The SCMS copy-control bits can be either „00 unrestricted digital copies allowed“, „11 one generation of digital copies allowed“, and „10 no digital copies allowed“. A copy from a CD to a DAT tape sets the copy bits to 10. An original recording to DAT allows one generation of copies which again are set to 10.

The technology was backed up legally by the US *Audio Home Recording Act* (AHAR) of 1992. This reform of the US Copyright Law obliges producers and importers of digital audio devices to equip them with a SCMS, and it makes illegal devices whose primary purpose it is to circumvent the copy control system. This regulation of a single technology has become the model for the general and global disciplining of cyberspace that we observe today. At the same time it is less restrictive than most technologies we see today, since SCMS does allow to make first-generation copies.

1. Generation -- Static Stand-Alone Systems

Another way of defining DRM is by saying that it is a technological enforcement of a license. Shrink-wrap and click-through licenses have been used for years, first for software, now for any digital content that is sold on- and offline. Compliance until now could only be enforced by legal means. DRM now turns the PC into a „copyright cop" that automatically complies with the rules set out in the license. In the first generation this is achieved by linking a digital object to a player.

The page description language PostScript, introduced in 1985 by Adobe did not contain a DRM mechanism. When the Portable Document Format (PDF) followed in 1993, it came from the very start with mechanisms to block certain forms of use (printing, extracting, modifying) and to protect access with a password, and it offers an interface for third-party DRMs. Today, PDF is one of the most wide-spread DRM formats. Many people are not even aware of it.

When the audio compression format MP3 was introduced in 1995, again it did not contain any DRM. But the Fraunhofer Institute that developed MP3 added the Multimedia Protection Protocol (MMP) for encapsulating MP3 files. Other DRM formats followed. The current members of the MPEG family (MPEG-4, MPEG-7 and the framework MPEG-21) are all designed from the start with DRM support.

First generation systems are local solutions that only affect the copyrighted data itself and the software for rendering it. The data is locked to the client during delivery from a server.

2. Generation -- Dynamic Systems (revocation and renewability)

Since the end of the 1990s, DRM is incorporated in all new devices (photocopying machines, harddisks, satellite decoders, CPUs, mobile phones, game boxes), in media (CD, DVD, broadcast signals, data formats) and software (viewers, editors, operating systems) that might touch copyrighted content. From local systems they develop into a global all-embracing infrastructure. Current second generation systems are a complex structure of various layers and building blocks that function on- and offline and keep content on the long leash of the rightsowners. Since the idea of a once-and-for-all safe technology proved wrong, these systems can be updated *in situ.* [For overviews s. Bechtold 2002, European Commission 2002, Grassmuck 2002]

Objekt-Identification: What?

In order to identify a given piece of data, metadata about its content, its authors, rightsholders etc. are added. This requires globally uniform numbering systems like the ISBN for books and the ISRC for audio recordings. The international umbrella organization of collecting societies CISAC (*Confédération Internationale des Sociétés d'Auteurs et Compositeurs*) is active in this area, because collecting levies in many cases depends on identifying works. CISAC is not only developing individual numbering systems like the *International Standard Works Code* (ISWC) for compositions and the *International Standard Audiovisual Number* (ISAN) for films, but also a one-stop clearing-house for copyright matters, the *Common Information System* (CIS).

A numbering scheme that emerged originally from the net is the *Digital Object Identifier* (DOI). It consists of an identifier, other metadata and a name space (URIs that can be mapped to URLs, local addresses, locations in a library etc.), and is intended for automatized copyright control from the production of works through marketing and distribution to the „aftercare" on the buyer's side.

Subject-Identification: Who?

Also the user has to be identified. Today, many systems are tying content to a player ID or some machine-specific hardware ID. This poses obvious problems for portability of content. Therefore, the trend is towards tying to a person who identifies herself through a smart-card, biometric authentication or some online „identity management system" like Passport or the competing system by the Liberty Alliance.

Online registration also of physical copies like a CD could allow to make the legally permissable number of copies. A so-called „rights locker" in which the licenses to purchased content reside would allow to access that content from anywhere, e.g. a hotel-room.

It hasn't been long since we got used to identifying ourself vis a vis a host computer. Thanks to DRM we will now have to identify ourselves towards every piece of encapsulated information as well. The times, when we could read a book or listen to a CD without having to show a passport first seem to be over soon.

Would anonymous DRM be possible? Probably yes, as David Chaum's eCash system has proven for an even more sensitive application area. But nobody in the industry is working on it. Controlling who uses what is at the core of the whole architecture. Therefore, anonymity is a feature that will not be implemented unless demanded by law.

Usage Vocabulary: When, Where, How?

Usage vocabularies or in the industry jargon *Rights Expression Languages* (REL) are the central element of DRM through which business models are being articulated. The most prominent example is the *eXtensible rights Markup Language* (XrML). It goes back to developments by Mark Stefik at Xerox PARC and is marketed by ContentGuard, a joint venture by Xerox and Microsoft. The further development has been transferred to the Organisation for the Advancement of Structured Information Standards (OASIS), the consortium in charge of XML in general, and to the MPEG-Gruppe in ISO. XrML permits to express who may use a digital resource (content, service or software) under which conditions and in what way. Practices in the digital publishing industry lead to design demand that the sytem should allow cumulative rule setting at different points of the chain of handling and control (studio, post-production, publisher, reseller, DRM service provider etc.).

Crypto-Wrapping

The actual control of the digital object is, of course, achieved by cryptoraphic encapsulation that is only opened when the conditions set by the rightsholder are met. Once packaged, the crypto-wrapper has to remain firmly attached to the payload, during the chain of delivery, on the user's device, and anywhere else, e.g. in a peer-to-peer environment.

„Superdistribution" is a business-model that industry is talking about a lot. A person sends a copy of a purchased e-book to a friend who can look a a teaser, e.g. a selected chapter. If he decides that he wants to read the whole book he can click on a button that connects him to the e-shop where he can purchase a key to unlock the rest of the file.

Crypto-experts are very clear about the fact that software-based crypto systems are inherently weak [s. e.g. Pfitzmann et al. 2002]. Therefore, the trend in third generation DRM is towards implementing them in hardware.

Cryptosystems depend on further mechanisms für key and transaction management and authentication through digital signatures, issues that overlap with other areas of application, like systems security, privacy and data integrity.

It also depends, of course, on a computing environment that automatically complies with the conditions and the usage rules, collects information about uses and bills them (e.g. by decrementing an electronic budget).

Revocation and System Renewability

The idea of a system that is installed and stays in control forever was proven wrong time after time. Therefore „renewability" became a standard feature of DRM. Systems are updatable in the field. The license for the Microsoft Windows Media Player is infamous for allowing Microsoft to remotely update the player and install operating system components at any time without permission or even knowledge of the user [s. Foster 2/02, Sieling 7/02]. When a new hack is circulating on the net, Microsoft simply plays a patch onto all installed players next time they go online.

Compromised devices, programs or data that cannot be updated in this way, must be revokable. The *Digital Transmission Licensing Administration*, for instance, uses a black-list of devices for which a circumvention is known to exist. During the authentication dialog between content and runtime environment, this list is interpreted. When a „legitimate" device talks to one whose ID is in the revocation list it breaks off contact. The „illegitimate" device will still be physically present, but it will be effectively isolated in the home environment.

Another way of achieving renewability and revocation is to keep content and license separate, a method patented by InterTrust. Even after delivery of the data, its license can be changed and rightsholders can remotely revoke the license altogether.

Search Engines and Filtering

In case that all other mechanims failed, special search engines can serve to located content on the net that has been extracted from its DRM wrapper with the help of watermarks, fingerprints or other characteristics. The rightsholder can then issue a notic-and-takedown warrant to the ISP.

If the content is hosted outside the reach of notice-and-takedown mechanisms, netfilters can be used. The unauthorized file will still be there but the users in that area will not be able to access it. Juergen Buessow, head of the local government in Dusseldorf, ordered ISPs in the federal state of Nordrhein-Westfalia to install such URL filters in order to fight nazi propaganda and child-pornography. Once in place, it can be expected that also the rightsholders will claim their right to feed the filters with URLs of infrining web-pages.

Central Source of „Trust"

A pervasive DRM infrastructure depends on centralized institutions. „The system must have an independent and dynamic root trust authority which either delivers the root key facilitating subsequent encryption or acts as the root trust authority for delegated trust functions, such as the generation of digital certificates, conducted at some other level within the system." [Garnett 2001] This requirement is similar to that of digital signature and public key infrastructures, and likewise has yet to be resolved.

Standardization

It has become clear by now that such an all-embracing infrastructure can only be build by a concerted effort of all players involved. Standardization takes place inside public forums like ISO, especially in MPEG and JPEG, or IEEE, in industry consortia like W3C, SDMI, the DVD Copy Control Association or the TCPA, or through a monopoly, i.e. Microsoft which can simply set de-facto standards.

Short of legislating compliance with these standards as in the case of DAT, a way of achieving it are bundling-contracts. The maker of DVD players will want to license the Content Scrambling System (CSS) because Hollywood allows distribution of their films only on CSS encrypted disks. Therefore players that don‘t support it would be unsellable. But the DVD CCA will license it to him only if he also licenses analog copy control by Macrovision, region management, CGMS, DTCP, HTCP and a host of other DRM mechanisms (up to ten on today‘s DVDs). According to Stefan Bechthold, this is a characteristic for technology licensing contracts in general [Bechthold 2002]. The argument given is that only in this way a uniform and all-embracing level of protection can be guaranteed. That this raises questions of anti-trust seems obvious, but, says Bechthold, surprisingly they are not being asked by politicians or the juridical literature [Bechtold 2002: 178 ff.].

3. Generation -- Secure Boot and Crypto Infrastructure

The idea to not only control data but the whole computing environment has been around in the military area since at least the early 1970s. The first models envisioned a cryptographic co-processor that takes control from the boot on and puts the computer into a secure state. This would mean changing the architecture of the PC, and it was rejected because it would require industry-wide cooperation -- or a monopoly, as we shall see.

One of the first secure bootstrap architectures was introduced by David Farber and two colleagues from the University of Pennsylvania in 1996 under the name AEGIS. Starting from a trustworthy BIOS segment on an additional PROM, one after the other the second BIOS segment, the hardware drivers, the boot block, the operating system and finally the applications are validated and started. For validation a hash is calculated and checked against a stored signature. They did place their work in the context of emerging e-commerce, of protection against viruses and trojans and general access control, but without any reference to DRM [Arbaugh, Farber, Smith 1996].

TCPA

In 1999, Intel, Compaq (now part of HP), HP, IBM and Microsoft founded the *Trusted Computing Platform Alliance* (TCPA), which by now has been joined by more than 180 other companies. Their aim is to improve security on the level of platform hardware, BIOS, system software and operating system. „The objective of the TCPA is to make trust just as much a part of the PC platform as memory and graphics.“ [TCPA, Januar 2000]

Core-element of the TCPA technology is a cryptographic co-processor named „*Trusted Platform Module*“ (TPM). It has a random generator, non-volatile memory for keys, and a mechanism for generating and managing keys, signatures and hashes. On top of this chip sits the *TCPA Software Stack* (TSS). It uses „integrity metrics“ for authenticating the system. The generaion of hashes of the components is called a „self-inspection“.

The TPM is in charge of booting the system. After starting the BIOS boot block, the BIOS then authenticates the user via smart-card or biometrics followed by the operating system loader and the operating system kernel. After everything went well and it is certain that no unwanted program sneaked in, the operating system kernel takes over.

The results of the integrity metrics are stored in the TPM. If a content provider wants to decide whether to entrust this system with his valuable wares, it asks the TPM for a signed cryptographic summary of the current state of the system. TCPA only attests to a given state of the runtime environment, a kind of x-ray of the system, and leaves it to the provider to evaluate its trustworthiness. If a virus enters the system or the users starts a debugger, the state of the system changes, and access to protected data is blocked. This attestation can also take place towards a local media player that would release content only when no untrusted program is running.

The consortium address privacy concerns in several ways. The keys built into the TPM never leave the system. The TPM generates new key-pairs, sends them to a certification authority for signing, and uses those for communication with the outside. By default, the TPM is turned off, and has to be activated by the user (opt-in). Any operation of the TPM has to be authorized by the user, e.g. through a PIN.

TCPA is targeting the complete computing landscape. In order to make the PC platform secure, an all-embracing solution is necessary. „The concept of ubiquity ... implies that at some point, all PCs will have the ability to be trusted to some minimum level. ... Every PC will have hardware-based trust, and every piece of software on the system will be able to use it.“ [TCPA, Januar 2000].

Palladium

The news about Microsoft‘s Palladium was broken by Steven Levy in June 2001. Levy is heavy on superlatives: „Microsoft’s plan to literally change the architecture of PCs ... one of the riskiest ventures the company has ever attempted,“ and “It’s one of the most technically complex things ever attempted on the PC,” he quotes a Gartner analyst [Levy 2001].

At first glance, the Palladium architecture is quite similar to that of the TCPA. The crypto-processor here is called *Security Support Component* (SSC). Other hardware changes concern CPU, chip-set, memory graphics processor, and USB-hub for connecting mouse and keyboard. The software-stack on top of the SSC is called Nexus. It creates a controlled operating environment, the „Trusted Space“, in which „Trusted Agents“, the Palladium applications are running, each in their own phyically and cryptographically isolated „vault“ or „realm“ with its own keys and policies.

The main difference is that TCPA controls the complete system from boot, whereas Palladium is a separate operating environment next to a regular, and regularily insecure Windows. „Since Palladium does not interfere with the operation of any program running in the regular Windows environment, everything, including the native OS and viruses, runs there as it does today. ... realms allow a user to have a locked-down work environment and fully open surfing environment at the same time, on the same computer.“ [Microsoft Palladium White Paper]

We can conclude that Palladium is a kind of sandbox architecture, similar to the Java Virtual Machine, only that the intention is the reverse. While potentially malicous code is kept in the Java

VM so it can‘t harm the operating environment, the Palladium application is secured inside the sandbox against attacks from the regular operating environment.

Another innovation is mentioned in Levy‘s article: ‚It’s a funny thing,‘ says Bill Gates. ‚We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains.‘ For instance, Palladium might allow you to send out e-mail so that no one (or only certain people) can copy it or forward it to others. Or you could create Word documents that could be read only in the next week. In all cases, it would be the user, not Microsoft, who sets these policies. [Levy 2002] The Microsoft Palladium-FAQ confirms this change of strategy: „Anyone can impose access control over remote networks and/or enforcement of user policy over sensitive information.“ [Microsoft Palladium FAQ]

Imagine a world of ubiquitous DRM: each software would make use of it. Every editor for text, photos, sound, video, each mailer would ask you before saving or sending what restrictions you want to impose on your data. We wouldn‘t have a choice but to technically claim our „content“ as our property, even if we decided to set all the restriction options to „off“.

For the media industry it would be paradise. Not only would they have full control throughout the whole „life-cycle“ of their property, they would also get a constant stream of high-precision, personalized usage data.

Others would be happy as well. The Church of Scientology, known to systematically use copyright law against their critics, would be able to effectively seal internal documents. Critical reporting or whistle-blowing by former members or relatives could be prevented. Also Microsoft would certainly have been grateful for a means to eliminate internal e-mails that were used as evidence in the anti-trust case against it via remote-control or time-switch.

But Gates‘ real coup was to turn DRM from a control instrument of the entertainment industry into a tool for everyone. He might even gain some acceptance from individual computer users. It looks better when not only a few multinational information corporations are sitting at the control switches, but everyone gets there hands on little switches of their own. Not that your regular Joe and Jane would have anything to gain. Them the monopolist has in its pockets already, anyway.

For the digital knowledge environment, this would mean that we will be seeing restrictions on private home-pages and in postings to newsgroups and mailinglists. Ever larger parts of the net become invisible to search-engines. And once there is a functioning micro-payment system in place there will be no holding back.

Most of all, this new architecture of cyberspace will teach us to think like info-capitalists. Gates is modelling the world after his likeness. What until now was restricted to commercial entertainment data will extend to any kind of digital utterance. We will be taught to think of our vacation photos and videos, our seminar papers, our mailinglist postings as „intellectual property“, as „content“, as potential commodities. The „Volks-DRM“ will lead to a copyrighting of the entire knowledge environment.

Microsoft continually insists that Palladium has no relation to DRM. Its main purpose is improving „security“. But the different securities can already be achieved by existing technology: PGP, virus scanners, crypto tunneling, TANs for online banking. And even the possibility to impose restrictions on use of office documents has been announced as part of Microsoft Works 2003. If Palladium is needed for none of these, that leaves DRM as main application and driving force.

DRM Issues

The DRM industry is concerned about a number of issues.

- Interoperability and portability of data. It must be possible to use information on a wide variety of devices, applications and operating systems (PCs, AV equipment, PDAs, mobile phones, set-top boxes). DRM features today lack standardization and a mechanism for translation between different systems. Standardization mustn‘t lead to a lock-in into a closed proprietary system preventing competition. Garnett puts it rather bluntly: „Can a monopolist be trusted?“ Microsoft is a problem not only to users but to the industry as well.
- Roll-out & migration: How do we get there from here? Corporations and public administrations will likely be the first to jump for DRM solutions as soon as they are usable. They can set up there own internal certification infrastructure. Their employees are in no position to resist the new automated „information policy management“. And indeed, Intel‘s Security Architect in a recent interview stated very clearly that LaGrande will target first of all corporate users [Plura 2003].

  In the mass-market it is most easily introduced for new services, e.g. PDF or streamingformats, cool technology and content that people want, so they download the gratis player which comes with DRM built in. It is much more difficult with old media, e.g. billions of legacy CDs without any protection that still have to be supported by new devices.
- User acceptance. Establishing user trust in these „trusted systems“ will certainly be the most difficult part for the industry. They also have to address user expectations about usability, platform independence, and privacy.

  Nic Garnett from Intertrust at the 2001 WIPO conference on e-commerce, talked with a notable degree of envy about Napster: „The rapid take-up of its technology - it is reported to have attracted some 65 million subscribers in less than a year - illustrates that consumers are more than ready to move to new technology if they like what it does.“ [Garnett 2001] The Microsoft employees who authored the famous Darknet Paper concluded that in the end, the media industry will have to compete with the darknet on its own terms, i.e. usability and price [Biddle et al. 2002]. Garnett puts it into more of a straight business talk: „[DRM] must provide a basis for delivering a consumer experience and business models that go someway to neutralizing the appeal of pirate offerings.“ [Garnett 2001]
- Time-frame. InterTrust calls the widescale commercial deployment of sophisticated DRM „imminent“. Intel‘s improved TCPA chip LaGrand is slated to come out in one to two years. Microsoft‘s next version of Windows with Palladium inside is announced for 2005.
- DRM doesn‘t work. This is the foremost and most well-kept problem for the industry. Four Microsoft DRM engineers presented convincing reasoning for this in their presentation at the 2002 ACM Workshop on Digital Rights Management [Biddle et al. 2002]. They argue that there will always be a darknet, i.e distribution networks for physical copies or for file sharing, and there will always be experts able to break the DRM systems that the industry experts are constructing who will then input the unwrapped information itself and know-how for circumventing DRM into the darknet. Targetting the average user, as the DRM industry currently does, is therefore meaningless. But targetting the expert if technically possible at all, is economically not feasable. The authors therefore predict further rounds of

technological and legal escalation, until an economic limit is reached. Even before that point it might show that stronger DRM systems may actually act as a disincentive to legal commerce. Their conclusion: „In short, if you are competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security."

3. Problems of the Solution

Having said that we could go back to business and continue building open architectures for the free exchange of knowledge. That's the attidude of many hackers: simply ignoring DRM. Technically, I sympahize with this attitude, politically I think it's rather naiv. As long as DRM was still insular, connected only to certain data formats and players, one could still avoid those. If you don't like the licensing scheme and the DRM mechanisms around MP3 you can just switch to Ogg Vorbis. But when the DRM project strives to modify the very architecture of the PC, it will affect the digital knowledge and communications environment even if it proves useless in the end.

The American Library Association in its position paper on DRM states that these systems are intended to control the use of a work after sale. „It is in this ‚downstream' control over consumer use of legitimately acquired works that DRM presents serious issues for libraries and users." [ALA 2002] Strange enough, the paper goes on to say that „the principal policy issues for libraries and schools are not derived from DRM technology, itself, but from the business models the content industry chooses to enforce." ALA seems to argue that DRM is neutral, but has the potential to prevent non-infringing uses and to enforce restrictions far beyond those allowed by the copyright law. „The scope of functionality of a sophisticated DRM platform is ..., in theory, unlimited." [Garnett 2001]

DRM can eliminate the „First Sale" doctrine which has been a bedrock principle for balancing the interests of exploiters and users of works [ALA 2002]. It allows us to give a book or CD to a friend, to sell it to a second-hand shop, and it allows libraries to loan works to the public. Eliminating First Sale has been an established practice for digital works which is now being reconfirmed by law. The EUCD proscribes that existing limitations mustn'd be applied to works sold online. To a user it shouldn't make any difference whether she buys music on a CD or online as MP3s. But there is no and will not be any legal market for used MP3s. Libraries already depend entirely on licensing contracts for digital works which, of course, do not allow a transfer of rights, e.g. to another library.

ALA's second issue is that DRM can be used for enforcing a "Pay-per-use" model of information dissemination which is contrary to the public purposes of copyright law. Libraries and other public institutions whose task it is to make information accessible to all citizens regardless of their financial means, will be turned into shopping-windows for commercial offerings. If they choose to pick up the bill for their users it would have severe economic consequences for them.

The next issue concerns preservation and archiving. ALA sees a problem with DRMs enforcing time limits or other limitations of use. The whole purpose of DRMs is to impose limitations. Even if content does not essentially disappear after a specific period of time or number of uses, its DRM wrapper will certainly prevent copying and conversion to new formats, which is

exactly what libraries, historical archives, museums, research institutions, and other cultural institutions need to do in order to preserve and provide long-term access to the knowledge products of our society. The logical consequence would be to extend the existing system of compulsory library copies to digital works. Publishers who, after all, do not fulfill the task of long-term preservation on their own would be required to submit a DRM-free copy of the work in a non-proprietary format. Such a law does exist in the German federal state of Berlin, but chances of extending it are slim.

Limitations to copyright that society needs for education, journalism, criticism, scholarship, access for disabled persons etc. can be eliminated by DRM. As mentioned before, the EUCD explicitly states that limitations do not apply to works marketed online. When DRM is a technical implementation of copyright law, then it should allow to exercise limitations as a function of the system.

InterTrust, in stark contrast to the rest of the industry, does talk about limitations. But they also argue that the search for implementation of privileges „must include, from the start, a re-examination of the basis and nature of the privileges themselves. ... Existing exceptions to copyright protection based on technology induced market failure seem obvious candidates for repeal, notwithstanding the institutional inertia supporting their perpetuation, when new applications of technology correcting that failure become generally available." [Garnett 2001] This is followed by a telling quote on where this re-evaluation might lead: „Traditionally, piracy of copyright works has been regarded and treated as an activity distinct from other forms of unauthorized copying. The former is the domain of gangsters, the latter the occupation of innocent consumers exercising legitimate rights. This general distinction is no longer tenable. Private copying has always inflicted significant damage on the copyright industries, damage that has only been minimally alleviated by the unfair and inefficient levy systems instituted in certain countries." [Garnett 2001] The goal of DRM is clearly to finally do away with the „irrational insistence on privileged access to data."

InterTrust does seem to believe that after this re-evaluation some justified limitations will remain. It's solution is an independent authority ensuring that providers of data comply with aggreed codes of practice, including provisions for privileged classes of users. It suggests that trade associations could play this role of „independent trusted authority". As a technical implementation, the DRM company proposes the rights locker modell. In this case, a Public Rights Locker would make rights available to entitled users under „non-standard" terms of use. „Establishing entitlement to these non-standard terms would be based on the applicant delivering the appropriate credentials, identifying it as a qualifying institution -- a library or educational establishment -- a process which is relatively simple and secure from a technical perspective." [Garnett 2001]

Another area of concern is the public domain. The e-book version of „Alice in Wonderland" is an infamous example of works whose copyright term has expired but which through simple digitization acquire new rights that are enforced by DRM. Privacy is another major issue that ALA doesn't even mention. DRM controls who uses what, and in doing so creates high-resolution usage profiles of each user. The legal anti-circumvention provision also prevents privacy officials from examining whether DRM systems comply with privacy laws. The right to read anonymously, taken for granted in analog media, is now threatened with extinction. A final point that will be at the center of the copyright discussions in the upcoming months concerns collective rights management organizations. Since publishers argue that DRM allows rightsholders to control secondary uses of works directly, they will use their justification and are threatened with extinction, as well.

Some observers like July Cohen in the US and Rainer Kuhlen in Germany have suggested ways of reforming DRM into something socially, democratically, culturally acceptable by technically implementing some of the issues mentioned. But maybe DRM is inherently flawed. Maybe in the end we will find out, that DRM is akin to nuclear energy: you cannot reform it, you can only do away with it altogether. But if we do find that out it‘s likely going to be too late. The fundamental transformation of the very architecture of cyberspace might prove to be irreversable.

4. Alternatives to that Solution

Science is already an alternative to commercial information. The scientific community should remember that it is bound by the scienctific ethics which according to Robert Merton rests on the four CUDOS pilars: Communism, Universalism, Disinterestedness and Organized Skepticism [Merton 1974].

Open Archives are an important answer: the movement is there, and it does receive some official backing. The German National Conference of University Deans issued a statment last year, in which they demand that the distribution of scientific knowledge must serve science again, and not primarily the commercial interest of large publishers. They recommend the development of alternative peer-review systems and university publishing servers in order to free science from monopolistic structures [HRK 2002].

In a similar but somewhat more cautious statment, the German Federal Ministry of Education and Research criticized in a recent „strategic position paper“ that the global networks favor the emergence of world monopolies which threaten the existing system of public science information. But increasingly science is opting for self-publishing, and the ministry is committing itself to supporting this movement by setting up a nation-wide information and knowledge network [BMBF 2002].

Scientists who, after all, don‘t earn their living by selling their work can obviously profit from a wide dissemination, gain reputation, get cited. The free software movement, namely through the GPL has shown how freedom can be expressed and secured with the means of copyright and contract. Mark Bide recommends several times that authors should make the terms under which they want their works to be used explicit. The GPL is specifically devised for software. But the Creative Commons licenses, that Bide mentions but which were only released after he finished his report seem to be the ideal instrument.

What CC offers is an Open Content Licenses Generator. The licensor choses one or more options. „Attribution“ permits others to copy, distribute, display, and perform the work and derivative works based upon it only if they give him credit. „Noncommercial“ permits others to use the work only for noncommercial purposes. „No Derivative Works“ permits others to copy, distribute, display and perform only verbatim copies of the work, not derivative works based upon it. „Share Alike“ does allow derivative works but only under a license identical to the license that governs the original work.

The CC license generator then produces a human-readable version of the license, the legally binding text, and a machine-readable version that helps search engines and other applications identify the work by its terms of use. The metadata used for the latter comply with the Resource

Description Framework (RDF) developed by W3C.

It is not the intention of CC that DRM systems are addressed by the machine-readable license. In fact, all flavors of their license explicitly prohibit to distribute the licensed work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this license agreement. But in a world of ubiquitous DRM, expressing freedom in the vocabulary of a Rights Expression Language might be the only way to force the Windows Media Player and other soft- and hardware to comply with the terms set by the author. In a landscape with DRM fortification everywhere, there would digital objects with full DRM armor around them, but all switches set to „free". They could float around this landscape full of „digital barbed wire" without any resistance, like angels.

Whether this worst case scenario can be prevented or not, in the end, freedom of science is a matter of awareness and active choice of scientific authors. Bide concludes: „Whether [Open Archives] are successful will ultimately depend in the first instance on the attitude of authors ...; if authors continue to believe that formal publication in the literature is what they want, and continue to be willing to give up some or all their rights over their content in order to achieve this – then the current mechanisms of scholarly publishing are likely to continue." [Bide 2002] For this to change, the most urgent task is to develop an alternative peer-review-system and alternatives to the current citation index, lending credibility to open science.

As for authors who do depend on the returns from their creative works, Bide writes „there must be a real possibility that, on the Internet, copying compensated by levy schemes could become the primary mechanism for Intellectual Property distribution, in which case the entire creative process would be supported by what is essentially a taxation-based system." [Bide 2002]. This is indeed the solution to the DRM problem that the Electronic Frontier Foundation and others are considering to promote. Authors would voluntarily put a copyright flag on their works which could be registered by an ISP when one of its users downloads the work. An appropriate lump sum levy would then be added to the online fee and passed on to a new „Collecting Society Cyberspace" that redistributes it to the authors. Commercial offerings could be protected by simple password authentication, as database providers and journals are doing today. No DRM would be needed. Ted Nelson's dream of free re-distribution plus compensation would finally come true.

Literature

American Library Association (ALA), Digital Rights Issues, May 1, 2002, http://www.ala.org/washoff/DRM.pdf

American Library Association (ALA), Washington Office on Digital Rights Issues, http://www.ala.org/washoff/digrights.html

Arbaugh, William A., David J. Farber Jonathan M. Smith, A Secure and Reliable Bootstrap Architecture, December 2, 1996, http://www.cis.upenn.edu/~waa/aegis.ps

Bechtold, Stefan, Vom Urheber- zum Informationsrecht. Implikationen des Digital Rights Management, C.H. Beck, München 2002

Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman, „The Darknet and the Future of Content Distribution“, given at the 2002 ACM Workshop on Digital Rights Management, 18 November 2002, http://crypto.stanford.edu/DRM2002/darknet5.doc

Bide, Mark, „Open Archives and Intellectual Property: incompatible world views?“, expert report for the Open Archives Forum, 12 November 2002, http://www.oaforum.org/otherfiles/oaf_d42_cser1_bide.pdf

Bundesministerium für Bildung und Forschung (BMBF), Strategisches Positionspapier „Information vernetzen – Wissen aktivieren“, November 2002, http://www.dl-forum.de/Foren/Strategiekonzept/strategischespositionspapier.pdf

Creative Commons, http://creativecommons.org/

Digital Transmission Licensing Administration (DTLA), http://www.dtcp.com/

EU Copyright Directive 2001/29/EG, 22 May 2001, http://europa.eu.int/comm/internal_market/en/intprop/news/com29de.pdf

European Commission, Commission Staff Working Paper: Digital Rights. Background, Systems, Assessment, SEC(2002) 197, Brussels, 14.2.2002, http://europa.eu.int/information_society/topics/multi/digital_rights/index_en.htm

Foster, Ed, „Check the fine print“, in: InfoWorld, 8.2.2002, http://staging.infoworld.com/articles/op/xml/02/02/11/020211opfoster.xml

Garnett, Nic, InterTrust Technologies of Santa Clara, USA, presentation at the WIPO Conference on E-Commerce, Geneva, September 2001, http://ecommerce.wipo.int/meetings/2001/conference/presentations/pdf/garnett.pdf

Grassmuck, Volker, Freie Software zwischen Privat- und Gemeineigentum, Bundeszentrale für politische Bildung, Bonn 2002, http://freie-software.bpb.de/

Hochschulrektorenkonferenz (HRK), Beschluss zur Neuausrichtung des Informations- und Publikationssystems der deutschen Hochschule, 6 November 2002, http://www.hrk.de/presse/2821.htm

Levy, Steven, „The Big Secret. An exclusive first look at Microsoft’s ambitious-and risky-plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?“, Newsweek, 1. Juli 2002, vorabveröffentlicht auf MSNBC: http://www.msnbc.com/news/770511.asp?cp1=1

Merton, Robert K., „The Normative Structure of Science“ (1942), in: The Sociology of Science, University of Chicago Press 1974, S. 267 ff.

Microsoft, Palladium White Paper: A Business Overview, August 2002, http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

Microsoft Palladium Initiative Technical FAQ - August 21, 2002, http://www.microsoft.com/technet/security/news/PallFAQ2.asp

Nelson, Theodor Holm, „Transcopyright: Pre-Permission for Virtual Republishing“, in Educom Review, 32:1 (January/February 1997), 32-5, http://www.xanadu.com.au/ted/TPUB/transcopy.html

Open Borders campaign and No Person is Illegal, http://www.contrast.org/borders/kein/

Pfitzmann, Prof. Dr. Andreas (technical part), Prof. Dr. Ulrich Sieber (legal part), Gutachten: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen, erstellt im Auftrag von DMMV und VPRT (eds.), September 2002, http://www.vprt.de/aktuelles/veroeffentlichungen.html

Plura, Michael, TCPA Inside. Intel erweitert den TCPA-Stadard mit „LaGrande“, Interview mit David Grawrock, c‘t Heft 5, 2003

Sieling, Lars, „Auf leisen Sohlen vom Betriebs- zum DRM-System“, in: Telepolis 3.7.02, http://www.heise.de/tp/deutsch/special/copy/12838/1.html

Stallman, Richard, Some Confusing or Loaded Words and Phrases that are Worth Avoiding, (1996) 2003, http://www.gnu.org/philosophy/words-to-avoid.html

Trusted Computing Platform Alliance (TCPA), Building a Foundation of Trust in the PC, January 2000, http://www.trustedcomputing.org/docs/TCPA_first_WP.pdf

WIPO Copyright Treaty, 20 December 1996, http://www.wipo.int/treaties/ip/wct/

World Intellectual Property Organization (WIPO), Intellectual Property on the Internet: A Survey of Issues, December 2002, http://ecommerce.wipo.int/survey/index.html