WIPO Conference on E-Commerce

Geneva, September 2001

Presentation by Nic Garnett, representing InterTrust Technologies of Santa Clara, USA

Introduction

It is a great pleasure and honour to participate in this important conference and, as ever, WIPO, its Director General and his colleagues are to be commended for their initiative in organizing such a wide ranging and relevant programme as well as assembling a congregation of such distinguished delegates and speakers.

The 2 years that have elapsed since the last conference have seen tumultuous changes in the technology sector. Market and investment opportunities have contracted. New business models of the kind that delegates spoke enthusiastically about at the last conference have, so far, been slower to emerge than expected. And while reliance on technology continues to grow in many parts of the world, it is still far from clear what this actually presages in terms of new opportunity in the shorter term.

A most striking technological development in the field under consideration here is that of 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. It also emphasises the dramatic compression of development timeframes that "Internet time" imposes.

It is therefore important at this time for the community of policy makers, regulators and legal experts, in common with the markets and the technology developers, to take stock. Whatever the trials and tribulations of the last 2 years, the research and learning have continued apace, adding the experience of deployment to what was previously mostly supposition. What do we know now that will help accelerate the transition that so many enterprises and markets will have to make under the relentless pressure of technology? What indications are there as to the needs of particular sectors and how they are best met? What are the respective roles of public regulators and the private sector in defining the Information Society? The experiences of the last 2 years have brought the answering of these and other questions much closer.

Digital Rights Management technology – or DRM as it has come to be called – is a particularly useful prism through which to review the recent past as well as to look to the future. The term is used here, as it was first coined by InterTrust, to refer principally to systems facilitating the trusted management of rights in digital information throughout its lifecycle and however it is distributed and used. Because DRM as a term is applied to host of different technologies, it is important to explain the concept of what has come to be called "sophisticated DRM" in more detail and to distinguish it from other technical protection systems under the same generic DRM heading.

The purposes for making this distinction are essentially two. The first aim is to better describe the overall context. When contemplating the context for technical protection and management of rights in information, useful comparison can be made with the evolution of retail financial systems and services. Many consumers around the world - by no means the majority, but a significant proportion -now rely on credit cards, automated cash dispensers and on-line banking services. None of these services existed to any degree as recently as 20 years ago. As they came into existence they did so as a multitude of unconnected systems developed for specific purposes and customers, and each with own technology and security processes. What has made them so essential to many consumers is the global interoperability and security they now embody: the many individual systems now connect through sophisticated "back-end" mechanisms delivering common functionality and built on globally applicable standards of interoperability, security and usability.

Consumers are going to expect the same of the many different mechanisms applied to the protection of the rights in information. They will want transparent usability, invisible interoperability and impeccable security. And all of this will have to de developed on Internet time, not the 15-20 years it took the financial institutions to bring everything together.

The second reason for distinguishing different technical systems is to highlight those systems with dynamic rule definition and delivery capabilities, in other words systems that enable the supplier of data to create its own rules for use and access to the data and to update those rules during the commercial lifecycle of the data. Technologies involving the non-dynamic implementation of rules of more general application - e.g. prohibitions on reproduction - while critically important offer less scope for understanding the relationship between rules derived from existing law and those created through computer code. Understanding that relationship, as many commentators have pointed out, is one of the greatest challenges in this and many other areas of regulation impacted by technology.

What is DRM?

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. Saying that it refers to technology used for protecting and managing rights in information gives no real help to understanding what a particular system does or how it fits into the overall context of rights management.

Information can take many different forms, much of which is not normally associated with intellectual property laws, and copyright law in particular, for its management and protection. The protection of personal information, e-mail and other forms of messaging, medical records, notational currency, corporate information policies: these kinds of information all fall within the scope of sophisticated DRM systems or variants thereof such as DPM (Digital Policy Management). On the other hand, from a legal perspective the protection of this kind of information is dealt with in practice under specific laws on data protection, trade secrets and the like and through contractual provisions.

To provide a clearer focus for this review and given the context, a conference organized by WIPO, attention here will be paid to the protection and management of rights in information recognized as falling with the normal scope of and normally protected through the application of copyright law: data representing and embodying audio, video, images, text and other subject matter.

Sophisticated DRM technology provides the basis for the creation of a specific computing platform which can automate and secure an entire system for the commercialism of information of virtually any kind. The technology is most often, at present, delivered and functions as software but will increasingly be built into devices either as a specific component of the device circuitry or embedded in some generic processor chip.

Sophisticated DRM technology with rich rights management functionality makes possible a range of operations in relation to information over which a supplier exercises some control and of which information a consumer desires to make some use. The specific nature of these operations is settled by the parties using the technology to effect a particular transaction; the scope of functionality of a sophisticated DRM platform is thus, in theory, unlimited. As such, a sophisticated DRM platform can be distinguished from other technology systems used, for example, in the secure vending and delivery of data or for the copy control of specific kinds of data. It should be noted however that these different technologies are not mutually exclusive and may well co-exist in certain environments and applications.

Here are some of the features that a sophisticated DRM system has to provide in order to meet the normal requirements of the right holder/ supplier:

1. A mechanism for securely packaging the data to be supplied so that it cannot be accessed or used in an unauthorised manner while en route to the consumer or while resident on the consumer’s device
2. Systems of metadata and rights languages to enable the identification of data and to express the permitted uses for that data in a way that maximises interoperability
3. Mechanisms for expressing and agreeing terms for the access to and use of the data
4. Mechanisms for securely delivering the rules of access and usage as per the agreed terms
5. Mechanisms installed on the consumer (client) device – known as a protected processing environment - for securely connecting the rules with the data to implement the agreed terms regarding access and usage, for capturing information about the permitted use of the data and for implementing consequences of use, such as decrementing an electronic budget

6. System security involving at least 2 critical features: advanced tamper resistance to reduce the risk of hacking into the system at any point and renewable security which facilitates the upgrading of software to respond to any breach in the security. The latter point must include the ability to shut down or revoke a particular user if found to be interfering with the system security.

The consumer has some additional requirements:

1. The system has to be usable. For example, the client software must be sufficiently compact to be readily downloadable, non-intrusive in terms of compatibility with other client software and readily understandable in terms of functionality and operations. It must be easy to uninstall if the consumer chooses to terminate use of the system
2. Data and rights acquired must be recoverable in the event of a systems failure in the client system
3. Personal information collected through the system must be protected and only used with the express consent of the consumer and as consistent with relevant laws
4. Certain kinds of consumers must be able to access and use data in accordance with privileges they enjoy under certain exceptions to copyright law and consistent with public policy
5. Acquiring data and rights to use such data should not be dependent on the maintenance of a relationship with a single service provider or use of a single format; there should be maximum interoperability between different devices and the applications and operating systems they use. Portability for many kinds of data is critical.

Although extensive and complex, these requirements still represent merely the basic features of a workable system. For a sophisticated DRM system to have any prospect of market acceptance it must also address the following requirements:

1. A single system of technology must be able to accommodate an enormous variety of distribution and value chains. The creator of the data is obviously not the only entity which delivers it to the consumer (or end-user). A single end user will be dealing with a multitude of different suppliers. It follows from this that on the supply, side the system must incorporate at least 2 capabilities: facilitating cumulative rule setting at different points in a particular value chain and delegating authority for establishing terms, from the top down, so that hierarchical rule setting occurs in an orderly manner. InterTrust calls this process “the chain of handling and control”.
2. A DRM system has to function in a distributed, peer-to-peer environment. Simple data protection systems that merely deliver data securely from server A to client B, locking it to the client device are basically inadequate in such a context. Consumers want to share, exchange, trade in data: Napster made that clear. Equally, suppliers will want to be able to harness delegated "superdistribution" systems provided they can maintain protection of the rights in their data in the

distributed context. These capabilities are critical to the development of new business models.

3. A DRM system needs to be able to function across a variety of different devices and operating systems: consumers will access and use data on PCs, PDAs, wireless devices, set top boxes. A DRM system needs to accommodate many different kinds of data from many different sources. It needs to be able to accommodate many different kinds of uses and transactions.
4. A DRM system must provide for the persistent protection of content and the rules that govern its use. The rules must be updateable. The content must be available in the format and quality required by the consumer and as provided in the terms agreed for its use. For this to be possible the DRM system must be constructed to allow for the independent delivery of content and rules. InterTrust invented and patented this approach.

There is one overriding requirement that must be singled out because of its fundamental importance: trust. A sophisticated DRM system which sets out to create a virtually all-embracing automated commerce system for digital information must guarantee the optimal level of system security. But it has to have another dimension. It has to include mechanisms that enable the parties to an electronic transaction - who will likely be located in very separate parts of the world - to replicate in their interaction the kind of trust mechanisms that would be available to them if they were dealing directly with each other in person. The supplier needs to be sure that the terms of the deal are understood and complied with by the consumer and that the data supplied is protected and only accessible pursuant to those terms. The consumer needs to be equally sure that the terms will be implemented, that there are no hidden costs or consequences, that the data contracted for will be supplied and that payment is made to and information used by the supplier strictly in accordance with the agreed terms.

In order for a sophisticated DRM system to guarantee this technological replication and implementation of trust - InterTrust calls the phenomenon "MetaTrust" - there are certain requirements, including the following:

1. The mechanisms for defining, delivering and implementing the rules must be as secure and tamper resistant as are the mechanisms that protect the data.

2. From a structural and functional perspective the operation of the system must be entirely predictable.

3. The configuration and operating standards of a given system must not favour any particular user of the system.

4. 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.

In short, a sophisticated DRM system is as useful as it is structurally and functionally predictable in performance. And it is as trustworthy as the root authority within the system. It therefore follows that this authority should only be exercised by an entity which maintains standards of unassailable neutrality both in its constitution and operations.

Having reviewed some of the features of a sophisticated DRM system, it is time to turn to some of the challenges which have to be faced in building and deploying an effective system. Some of these challenges have been addressed from the inception of systems design; others have only emerged clearly during early deployment programs.

The Challenges

Complexity

An obvious point: building a secure and scalable system embodying all the features outlined above is an extremely complex undertaking. Creating a system that delivers a consumer experience as intuitive as walking into a record store to purchase a CD; which delivers data that can be used on agreed terms across a variety of different devices; which provides protection against unlawful access throughout the lifecycle of the data: all this requires far more than mere expertise in architecting and coding a system, however enormous that requirement may be.

Some of the most highly sought after specialists in the technology business are the product managers. Their task is to capture relevant market requirements and turn them into working features of system products: failure to do this accurately can result in products being doomed to failure from the earliest design stages – although this may not become apparent until the market rejects a product after years of investment in its development. In short, in emerging markets, and given the timeframe for software development, matching requirements with product design is a complex and high-risk business.

Business Model Innovation

This challenge is linked with the previous challenge: it concerns the absence of generally established business models for the exploitation of data in the electronic market place. This means that too often, the development of a particular technology is necessarily confused and intermingled with the development of a particular business model. Subsequent failure of the business model frequently results, at least to some extent, in an assumption that the underlying technical components are flawed.

This is an inevitable complexity. Many media companies have been unjustly criticized for tardiness in devising and adopting business offerings appropriate to the new electronic market environment. This environment is uncharted and will take time to explore. Available material regarding possible consumer practices is of limited value: consumers rushed in their millions to Napster but so have they done to other pirate offerings for many years. There are doubtless generational factors involved in managing companies to deliver products that the more tech savvy consumers want and are willing to pay for. The overall infrastructure is still relatively immature and lacking in some critical components: micro-payment systems, for example, appropriate to the needs of usage based business models.

Interoperability

Interoperability remains the Holy Grail in so many areas of technology and commerce and the need for it grows ever stronger with the increasing use and sophistication of different kinds of technology. Many – perhaps most - of the DRM features listed above lack standardization or some mechanism for providing reliable translation between different systems and this results in ever greater divergence between the emerging systems.

Of course, vast areas of communication and commerce function globally and invisibly on established standards of interoperability: the standardization of critical Internet protocols is an obvious and important recent example. On the other hand the history of media formats is marked with the scars of competition and littered with the remains of unsuccessful proprietary systems: Betamax; DAT; DCC. The new audio formats – SACD and DVD Audio – seem set to perpetuate the process.

There is no doubt much to be learnt from studying the difficulties that the media companies and the consumer electronics industry have encountered in trying to standardize formats. It is important to note in this context the work of MPEG and a number of other organisations working diligently to bring industries together around common standards for protocols, interfaces and languages, but it is still far from clear to what extent interoperability between different DRM systems, for example, can be achieved. The highest priority must be given to the work of these bodies because to rely on the functioning of the market to settle on a standard could severely delay or restrict development in the area.

Having said that, proper recognition must also be accorded to, and appropriate protection maintained, in accordance with established principles, for the proprietary rights and interests in inventions. Without this recognition and protection, the basis for the level of innovation that the new environment demands will simply disappear.

Limitations to Rights

Reference was made earlier in this paper to consumer expectations in terms of access to material in the public domain or subject to exceptions and limitations to copyright protection. Numerous commentators, particularly in the USA, have cross referenced these expectations to the constitutional or other basic rights of individuals, attempting thereby to elevate all these limitations to the level of direct challenges to the basic proposition of DRM. In fact, sophisticated DRM can provide solutions to many of the problems in this area, solutions that to date simply have not been possible.

There are indeed concerns that have to be addressed. The hierarchy of rules system referred to above – the chain of handling and control – embodied in the InterTrust DRM systems involve recognition and application of public interests as expressed through law as the supreme rule set. That of course raises enormous complexities as to the applicable rule set for a particular transaction as it unfolds in a global context but the principle of the supremacy of the sovereign interest remains intact.

How can relevant privileges be implemented?

The first point to make in this connection is that DRM technology is and must remain a neutral factor in the equation and must be able to give effect in practice to virtually any rule set. Baking a particular implementation of a privilege into the native configuration of the technology and, equally, mandating the export into the clear of data for the benefit of certain classes of consumers, compromises that neutrality. Of course, the common response to this assertion of system neutrality, is the proposition that the users of the technology, particularly in the media industries with high degrees of concentration, cannot be trusted to make data available to consumers on acceptable terms. The instinct of such suppliers is to use technology to circumvent the legal privileges: so it is argued.

Reference can be made to a number of ideas in response to this but again, general observations are needed first.

There is little evidence that many of the issues in play here have yet been analysed on an adequately informed basis: technologists and lawyers seem to largely inhabit parallel worlds. Equally, the focus of the work done to date seems somewhat lopsided, concentrating almost exclusively on the demand side of the situation. It seems only logical that in the new environment the search for ways to define and implement data access privileges must include, from the start, a re-examination of the basis and nature of the privileges themselves. Uncodified privileges present particular problems.

A second critical observation is that whatever decisions are ultimately made about the shape of the privileges they must be given effect to as functions of the technology and not as exceptions to or in parallel with it. The existence of data in the clear as a consequence of implementing privileges effectively negates the use of technology in relation to that data for any other purpose. Assume for example that a library enjoys access to literary material on a privileged basis and is entitled to make that same material available to its members on similarly preferential terms. There is no way to ensure, absent the continued application of the DRM technology, that the same material will not find its way back into the general commercial distribution channel where it will undermine the market, reliant as it is on the legitimate application of DRM technology.

Even if the market distortion due to the removal of protection can be prevented in some other way, a basic principle of trust management technology also comes into play: the original supplier of data, using particular trust technology, must be able to rely on a consistent trust proposition, delivered by that technology, underpinning the distribution of his data and the management of his rights therein from start to finish. If transfers and translations across different protection and trust mechanisms are mandated and given effect to at different points in the value chain without the authorisation of the supplier, the chain of trust is broken between the supplier and the consumer and both parties suffer as a consequence.

Turning then to ways to address these issues, three possibilities may be mentioned as worthy of study.

First, given the extent and scope of the work that is currently ongoing in the field of Rights Expression Languages, and against the background of the emerging "Semantic Web" where vast of areas of commerce will be conducted on an automated basis between servers, efforts could be made to develop semantic tools to express appropriate privileges in relation to certain data. As suggested however, that has to link to parallel work on the nature of privileges and re-evaluation of the public interest requirements. New privileges may be found necessary; equally, established privileges should be reviewed. 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.

The problem with the Rights Expression Language approach, apart from its many complexities, is that it does not adequately answer the concerns regarding actual implementation. To a certain extent the standardisation of languages will facilitate the wider use of appropriate DRM technologies but it will not per se overcome the concerns regarding the packaging and rule setting for particular items of data. And again, the technology must not itself impose particular standards.

The answer lies, perhaps, in the hands of the representatives of particular sectors subject as necessary to the operation of law and the maintenance of competitive conditions. Legitimate suppliers of data have an interest not only in ensuring that their rights in data to which they apply DRM remain protected and managed as they intended but also that their data is not captured by competitors, packaged with DRM technology without authorisation and made available as pirate material to unsuspecting consumers.

"Trusted" packaging of data becomes critical to the process from both the supplier's and the consumer's perspective. The supplier needs protection from unlawful competition; the consumer needs assurance that legitimate privileges are incorporated in the rule set applicable to particular data. An independent authority, with the necessary official recognition and where necessary, appropriate clearance from competition authorities, can be the source of trust for such operations. They can ensure that individual suppliers of data work in accordance with appropriate codes of practice as they electronically package data and incorporate certain default rule sets implementing the appropriate privileges for certain classes of users. Trade associations representing certain sectors would seem well-placed to undertake such a role.

The support for delegated trust authority mechanisms in the InterTrust DRM system are particularly well-matched to this approach.

A third idea involves the use of what are commonly referred to as rights lockers. Key among the many inventions which InterTrust has patented in the DRM space is the idea of securely delivering data and the rules for its use independently of each other. This approach offers enormous possibilities to both suppliers and consumers.

It is foreseeable that services will be created that make it possible for a consumer to acquire the rights to access and use a particular piece of data - a favorite recording of music for example - on a variety of different devices and from any location. Imagine, for example, checking into a hotel room and instead of watching the standard array of films available on the hotel video system, the consumer simply calls up rights to a personal collection of music, film or other data from an on-line rights locker service and downloads the selected data from a content server in the format appropriate for the playback equipment in the hotel.

A similar approach might be envisaged in relation to certain data access privileges based in the public interest and available to certain classes of users. In this instance, one might refer to a "Public Rights Locker", on-line services created to make rights available to particular classes of users and to which non-standard terms of use are applied. 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. The ability to create highly accurate audit trails within the system would also ensure that both data and privileges were treated precisely in accordance with the prevailing law and industry agreements.

These are not specific proposals: there are obviously a host of issues that would have to be resolved for such arrangements and systems to become a reality. They are offered at this stage merely to illustrate how the existence and the nature of sophisticated DRM technology can be applied to better defining and implementing the balance which good copyright laws strive to achieve. As ever, the technology is probably the easier part of the equation to put in place: the definition of the appropriate terms as between the respective parties will probably prove the most problematical.

Article 9 of the WIPO Digital Agenda which emerged from the first Conference on e-commerce provides as follows:

" 9. Study any other emerging intellectual property issues related to electronic commerce and, where appropriate, develop norms in relation to such issues."

It is submitted that work should start as soon as possible under the auspices of WIPO in accordance with Article 9 of its Digital Agenda to bring together suitably qualified and interested representatives of the private sector for the study of the issues related to the protection and management of rights through the application of technology and the implementation of the exceptions and limitations to copyright. There are numerous issues that, of necessity, need resolution at the international level and which are not dealt with in the 2 treaties which emerged from the 1996 Diplomatic Conference. Unless work starts in near future to resolve them, there is the very real prospect of conflict between the approach of law on the hand and technology on the other restricting important innovation and thereby the opportunities the new technologies offer both to suppliers and consumers of data.

It is further submitted that this effort should also be closely coordinated with the important collective efforts that are already underway to establish standards promoting interoperability between technologies and the languages they employ.

Piracy

Digital technology makes copying much easier both in terms of quality and quantity. With the Internet and the Web providing both a highly efficient distribution mechanism and channels for obfuscating the origin and illegitimacy of data, piracy will increase exponentially if the rights holders' only recourse is to the traditional copyright based legal remedies and the "search and destroy" enforcement mechanisms.

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. Napster showed how that damage will grow exponentially unless checked. Ironically, it also demonstrated it is virtually impossible to derive direct commercial gains from on-line piracy at present. That will change rapidly as legitimate revenue generating business becomes commonplace on-line and ways are found – as they certainly will be – to tap into the revenue streams illegally.

DRM does not provide the complete solution. As numerous commentators have pointed out, however secure a DRM system there is some point in the rendering of the content where it becomes copyable without permission of the rights holder. Information, it is said, wants to be free. Of course, the motion picture industry is all too familiar with pirate videos sourced from video cameras smuggled into theatres.

The challenge for DRM from piracy is in several areas:

- A DRM system has to be as secure and tamper resistant as possible; it must be able to rely on access to device driver mechanisms that help reduce problems such as audio-jacking

- it has to be configured so that legitimate exceptions to copyright protection can be exercised as a function of the system;
- it must provide a basis for delivering a consumer experience and business models that go someway to neutralizing the appeal of pirate offerings.

As another commentator said recently: it must become as easy to buy music legitimately on-line as it is to steal it.

Competition

Interoperability is not of course an issue where a single system becomes the dominant standard. But if that system is a closed proprietary system then a very different set of problems emerges particularly in a trust management system where, as explained above, the administrator of the system acts as the root authority. Can a monopolist be trusted?

There has been much examination of late as to what constitutes monopolistic conduct in the technology field and what is to be done to reverse or mitigate the consequences of monopoly maintenance or acquisition. Examination of the issues in this area is beyond the scope of this paper but it is pertinent to suggest that particular regard has to be given to the analysis of what constitutes monopolistic conduct with regard to the alignment of technologies supporting a trust management system such as DRM.

Conclusion

This, in outline, is how InterTrust sees the landscape for DRM as the end of 2001 approaches. Its vision for the form and function of DRM remains as complex and ambitious as ever because it continues to believe that DRM has a fundamental role to play in the commerce of digital information. As a company it is learning diligently how to build the kind of DRM systems that consumers want even as those consumers are themselves learning about their needs in the new environment. It is hugely complex process and one without precedent: the practical challenges are many and the impatience for solutions insistent.

The private sector alone cannot settle all the issues in the development and deployment of DRM and the management of rights in data that need to be addressed. It is almost 5 years since the world's copyright experts came together in Geneva to work out an international copyright regime for the 21st century. Notwithstanding their accomplishments, the legal environment for the application of technology to the protection and management of rights in copyright works remains in some respects unclear. For this reason the there is a real need for WIPO to take an active role in building the necessary connections between legal mechanisms for the protection and management of rights and the technology being developed and deployed to that end. The stasis which exists at the confluence of law and technology at present and which is marked somewhat by hesitation in business innovation, irrational insistence on privileged access to data and by the threat of dramatically increasing piracy cannot be tolerated indefinitely. A decisive initiative from WIPO along the lines outline above should help to remove some of the uncertainties responsible for the current state of affairs as well as to enhance the many positive developments which are already clearly underway.

However imminent the widescale commercial deployment of sophisticated DRM technology with the rich functionality of the kind developed by InterTrust, the anticipation of its use should remain firmly in focus while working out the many legal and practical issues that will help define the emerging electronic media markets. Incremental revision of existing laws, absent appropriate conceptual re-evaluations and a sufficiently broad and informed vision of the role of technology, will not provide an adequate basis for building the legitimate versions of markets and electronic distribution systems that will come to be in any event. Those who continue to develop the systems which will help deliver the many opportunities and benefits of electronic commerce must be able to do so without undue restriction from legal constructs rooted in a different era.

Since the first WIPO E-Commerce Conference two years ago an alternative system for the electronic distribution of music, built with an investment of $10 million and reaching 65 million subscribers, has come and, at least for the moment, gone. As anyone with more than a passing knowledge of technology knows full well, enjoining Napster's unlawful operations has to be seen as the start of a process, not the end of one.