

# INDICARE Monitor

## About Consumer and User Issues of Digital Rights Management Solutions

www.indicare.org

ISSN 1614-287X

### INDICARE Monitor Vol. 2, No 1, 25 March 2005

#### Content

|  |    |
|--|----|
| Editorial .....  | 2  |
| <i>Knud Böhle, ITAS, Karlsruhe, Germany</i>  |    |
| E-Payment and DRM – Integration needed. A brief summary of the second INDICARE workshop in Budapest, February 3, 2005.....         | 4  |
| <i>Kristóf Kerényi, SEARCH laboratory, Budapest, Hungary</i>   |    |
| Where do DRM- and e-payment systems meet? .....  | 7  |
| <i>Rüdiger Grimm, Technical University Ilmenau, Germany interviewed by Knud Böhle, ITAS, Karlsruhe, Germany</i>                    |    |
| Critical review of MPEG LA software patent claims. The usage of open source rights expression languages must be royalty free ..... | 10 |
| <i>Susanne Guth, Vienna, Austria and Renato Iannella, Brisbane, Australia</i>  |    |
| Economic analysis of DRMs roll-out over the Internet.....  | 17 |
| <i>Olivier Bomsel and Anne-Gaëlle Geffroy, Ecole des Mines de Paris, France</i>  |    |
| Violation of consumer rights with DRM-based usage control systems – The case of Half-Life 2 .....                                  | 20 |
| <i>Danny Vogeley, Berlecon Research, Berlin, Germany</i>   |    |
| How to implement copyright exceptions in DRM systems<br>A proposal substantiated for the copyright exceptions in German law .....  | 24 |
| <i>Dominik Knopf, Institute of Information Law, Karlsruhe, Germany</i>   |    |
| Comparing the EUCD implementation of various Member States. A review..   | 27 |
| <i>Margreet Groenenboom, IViR, Amsterdam, The Netherlands</i>  |    |
| Better take a long tail look...<br>Three remarks on the first INDICARE state-of-the-art-report .....                               | 32 |
| <i>Timo Ruikka, Nokia Corporation, Espoo, Finland</i>  |    |
| Masthead .....   | 34 |

---

The **IN**formed **DI**alogue about **C**onsumer **A**ceptability of **DRM** Solutions in **E**urope



## Editorial of INDICARE Monitor Vol. 2, No 1, 25 March 2005

By: Knud Böhle, ITAS, Karlsruhe, Germany

**Abstract:** With the second year of INDICARE we start the second Volume of the INDICARE Monitor this month. Beginning with the present issue, the Editorial will always fulfil two purposes. It will announce INDICARE project news and it will introduce the respective issue. Apart from payments and DRMs, the current issue continues debate about DRM patents, requirements of the European Copyright Directive (EUCD), and adds a further comment of the first INDICARE State Of the Art Report – this time from the IT-industry side. We also introduce a newly emerging DRM topic, namely the use of DRM systems for computer games, and we present a straight forward economic analysis of DRM by two French researchers involved in the European IST project MediaNet.

**Keywords:** editorial, INDICARE

### INDICARE news

The second INDICARE workshop last month on "E-Payment and DRM for Digital Content", hosted by INDICARE partner SEARCH in Budapest, has been a success in terms of quality of speakers and quality of participants lively debating. It became clear that "paid content" and "protected content" require integration, eventually because consumers want easy-to-use services.

The *workshop report* documenting the event has been released this week and is available online (at <http://www.indicare.org/tiki-page.php?pageName=Events>). At the same page you will also find the speakers' presentations. A *brief summary* of the Workshop, prepared by *Kristóf Kerényi*, is included in this INDICARE Monitor issue.

### About this issue

The present issue containing the brief summary of the second INDICARE Workshop already mentioned above, also includes an in depth interview with *Rüdiger Grimm*, one of the speakers at the workshop. He highlights the need for integration of DRM systems and payment system, and the role for payment service providers as intermediaries. He is sceptical about the role of PKI for DRM. In his view PKI and signatures are fine for B2B rights management but not for B2C e-Commerce as long as the infrastructure is not available for other purposes as well. He also warns that "there is a huge privacy bomb out there in DRM services". Both topics are relevant in other articles too, as we will see.

The debate about DRM patents has been taken up already in the last issue with a review of the Berlecon Whitepaper, and an Interview with Larry Horn Vice President of MPEG LA by Thorsten Wichmann. One of the crucial questions is the patent claim of ContentGuard with respect to rights expression languages and the claim of MPEG LA with respect to essential OMA 1.0 patents. We are delighted that *Susanne Guth* and *Renato Iannella* respond to this challenge and present their open source advocates view. Both are heavily involved in the development of ODRL, which is used among others by the OMA consortium as rights expression language.

The EUCD is addressed in two articles: *Dominik Knopf*, working at the "Institute of Information Law" in Karlsruhe proposes a concept how to implement copyright exceptions in DRM systems. To achieve this, he argues, a paradigm shift: would be required from object-oriented DRMs to user-specific DRMs linking the content to the person, who acquired the rights to use it. By this he contributes to an "emerging scholarship", as *Stefan Bechtold* termed it (cf. INDICARE Monitor, Vol. 1, No 4, 24 September 2004) interested in a value-centred design of DRMs able to preserve important policy and legal values. As Grimm made clear in the interview, as long as the required infrastructure to hook up to is not in place, DRMs proposals like the one by Dominik Knopf – as the author admits – have to be taken as feasibility studies, not as something we will see soon.

*Margreet Groenenboom*, IViR, reviews a paper by *Urs Gasser* and *Michael Girsberger* on the transposition of the EU CD with respect to the legal protection of technical protection measures. One of the striking points is the spectrum of legitimate interpretations. While, following a *narrow* interpretation, the EU CD only prohibits the circumvention of those TPMs that prevent or restrain uses that are relevant under copyright law, the *broad* interpretation regards any TPM protected which aims at preventing or restricting any act not authorized by the rightholder. This openness of interpretation consequently leads to a lower degree of harmonization among EU member states.

*Olivier Bomsel* and *Anne-Gaëlle Geffroy*, Ecole des Mines de Paris, provide a clear cut economic analysis of DRM systems. They start from two basic functions of DRM systems: content *protection* and *versioning*. Next they distinguish between two types of networks: "two-way communication networks" like the Internet, where everyone can technically broadcast contents, and "one-way networks" like broadcast networks. The economists hold that the "broadband Internet roll-out is largely subsidized by circumvented contents available through P2P applications". Circumvention would benefit the whole range of IT-industries, which could not be forced to accept DRMs on open networks. The situation seems to be rather different in one-way-networks where content owners "control the availability of contents and the indirect network effects". Here, equipment manufacturers have to accept protection standards demanded by the content industry. The analysis shows that in order to assess the future of DRMs deployment, it is most important to distinguish network types as they frame to a certain extent the chances of stakeholders to push through their respective interests.

**About the author:** Knud Böhle is researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at Research Centre Karlsruhe since 1986. Between October 2000 and April 2002 he was visiting scientist at the European Commission's Joint Research Centre in Seville (IPTS). He is specialised in Technology Assessment and Foresight of ICT and has led various projects. Currently he is the editor of the INDICARE Monitor. Contact: + 49 7247 822989, [knud.boehle@itas.fzk.de](mailto:knud.boehle@itas.fzk.de)

**Status:** first posted 24/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=91](http://www.indicare.org/tiki-read_article.php?articleId=91)

*Danny Vogeley*, Berlecon Research, addresses a rather new topic. Only recently the computer game industry has started to use DRM-based usage control systems. A case in point is the most successful Half-Life 2, which sold more than 1.7 million copies between November 2004 and January 2005. What Vogeley observes is not merely an emerging application field for DRMs. He can show that right from the beginning this technology is used to violate consumer rights. Another interesting observation is, how little consumers have reacted to this practice. In fact it has had no negative effect on sales. This shows how important it is to distinguish application areas and consumer groups considering acceptance and acceptability of DRMs. What might provoke protests and refusal in one area might be acceptable without grumbling in another.

The last article of this issue is again a comment on the SOAR. *Timo Ruikka*, Nokia Corporation, suggests rethinking consumer expectations in a long-term perspective with respect to flexibility and transparency requirements. He also says that the INDICARE paper "has far too great emphasis on privacy aspects, as if DRM was a bigger threat to privacy than (for instance) eBay or electronic banking or credit card statements". This statement sounds quite different from what security expert Rüdiger Grimm had termed a "huge privacy bomb out there in DRM services".

Be this as it may, in any case there is still a need for discussion of DRM issues, and INDICARE is the dialogue platform for this purpose. Come and comment the articles on our website and write for the INDICARE Monitor.

Happy Easter!  
Knud

## E-Payment and DRM – Integration needed

### A brief summary of the second INDICARE workshop in Budapest, February 3, 2005

By: Kristóf Kerényi, SEARCH laboratory, Budapest, Hungary

**Abstract:** The second INDICARE workshop on “E-Payment and DRM for Digital Content” took place in Budapest on February 3, 2005. There was good interest in the event, which indicates that e-payment and DRM are topics of equally high interest to both the industry and academia. The workshop provided some revealing insights into the role of e-payment in complex DRM-enabled systems, and also called for better integration in order to create more acceptable systems to consumers.

**Keywords:** conference report, INDICARE, business models, collective rights management, e-payments, m-payments, systems integration

#### Introduction

When we started organising the second INDICARE workshop with e-payment being the intended focus, we thought we would be in a difficult situation, since from the technical point of view e-payment has hardly anything to do with DRM. However, we quickly found out that from the consumers’ point of view the situation is very different. Consumers do not really bother about technical details, at least they do not wish to. Instead, they are looking for easy-to-discover and easy-to-use services, which provide them with a new experience of consuming digital content in fascinating ways.

Thus recruiting the intended number of a dozen speakers and the optimal number of a half century of attendees for the workshop held in the excitingly modern informatics building of the Budapest University of Technology and Economics was not a difficult task at all.

The workshop was organised around four thematic blocks: “e-payment technology”, “service providers on DRM”, “content providers in motion” and “business models for consumer satisfaction”. Below I attempt to give a very brief coverage on what in my view were the interesting conclusions. Interestingly enough, consumer issues came up in more cases than expected.

#### E-Payment technology

The first block of presentations was organised around technical questions of e-payment. Traditional e-payment solutions have been in use on the Internet for years, so there is not much current development in that area. However, with the expansion of the mobile market, and with handheld devices making it into our pockets, a transition to m-payment is taking place. This will be even truer as mobile devices open up new opportunities like near-field communication and the use of smart-card-based security.

*Risto Sipilä* talked about new *touch-based* services based on near-field communication, the so-called *Radio Frequency Identification (RFID)* technology. As opposed to remote payments, near-field communication is based on locality, where new types of point of sale (POS) terminals will accept e-cash or tickets (e.g. cinema tickets) directly from the consumer’s mobile phone without having to connect to the mobile network. The speaker underlined two very important aspects when developing new mobile services: on the one hand ease of use was very important, from easy-to-use terminal (phone) user interfaces through easy service discovery to convenient payment methods. On the other hand, besides *user friendliness* he urged for *open technologies* and *open standards*.

*Péter Papolczy* talked about SEMOPS (Secure Mobile Payment Service), a research project funded under the 6th Framework Programme for Information Society Tech-

nologies of the European Union. SEMOPS is a new concept for a *real-time payment service*, which can be implemented across a variety of mobile devices or other handsets, over different data carriers and for a large spectrum of payment amounts. SEMOPS is differentiated from other e-payment services by its consumer-centric design. It provides consumers as Papolczy claimed with unprecedented *flexibility*, while also ensuring *privacy*. SEMOPS combines consumer anonymity with refundability. This is a quite new approach to e-payment, since so far in every widespread solution the consumer has been traceable.

### Service providers on DRM

In the second block of presentations two speakers brought forward their views on the provider side of e-payment and DRM. The first of them, *Pál Miletics*, who came from a major mobile service provider, presented facts and figures about the mobile telephony market and the mobile market in general. In his view, customers demand services for information access, content download, ticket purchase, parking payment, or ordering. He underlined that there was a big difference between traditional e-commerce and m-commerce, the latter providing anytime-anywhere type services limited only by the handsets' capabilities. He also said that consumers usually do not understand the benefit of new technologies, so accurate surveying of market needs would be very important in order to succeed with DRM services.

In the second presentation by *Tamás Foltányi*, the attendees heard about a selection of case studies from the technology provider's point of view. The speaker pointed out that the mobile business environment is *significantly different* in the United States, in the EU and in Eastern Europe, so care must be taken when one wants to talk about *business opportunities* in general. He said that consumer interest in e-payment services is present, as is the technical background, so using e-payment is not a problem. However, when analysing opportunities, one must look at the whole "value chain".

### Content providers in motion

The first presentation in the third block was about general DRM issues, more specifically the aim of DRM. *Tibor Sas* first looked at DRM from the *infrastructure* point of view and regarded DRM as infrastructure for the management of rights. He concluded that also for the DRM infrastructure a critical mass of consumers would be necessary to pay off. Second, he emphasised the *importance of object identification*, and proposed the widely used Digital Object Identifier (DOI) as a means of solving several DRM-related problems, especially the collection and distribution of fees as a main purpose of the DRM infrastructure. He also brought up several use cases with inherent problems, e.g. component reuse, print-on-demand of small-volume publishing and mixed-financed learning materials. He came to the conclusion that object identification and DRM could solve these, especially by identifying, tracking and billing uses of the many small-scale components by many parties. Finally, the speaker pointed out that in his view the chief problem was the lack of e-content materials in the appropriate quantity and quality. He concluded that a working DRM infrastructure and intensive content protection would encourage providers to supply more valuable content.

*Péter Benjamin Tóth*, a lawyer at a collecting society of authors and publishers gave a presentation on the role of collecting societies in a world of DRMs. The main issue of the presentation was whether with the spread of DRM systems collecting societies will die out, or whether collective rights management still has some future. He asked if DRM and levies can coexist, and if it makes sense to use DRMs to make royalty distribution more accurate. The answer, he said, might be given by the International Confederation of Societies of Composers and Authors. CISAC's aim is to develop documentation and distribution standards for the sake of better accounting between collecting societies. CISAC works together with ISO, and they have developed accepted standards for the identification of works and rights holders, which actually forms also the basis of every DRM system.

## Business models for consumer satisfaction

The last block of the day started with an analysis of DRM business models. The speaker *Vural Ünlü* categorised content protection strategies into three groups: *technical* protection, *contractual and statutory* protection and the alignment of business models forming *structural protection* for content. The speaker then analysed the optimal level of technical content protection. His conclusion was that *valuation* and *content degradation* are major determinants of this optimal level, which also rises with the *network effect*. Two further findings were that the profit of content providers is reduced when protective measures cause *utility decline* for consumers, and that the alignment of business models may lead to additional revenues.

*Rüdiger Grimm* talked about a conflicting situation between content providers and their potential customers when it comes to digital products available on the network. He examined several alternative business models, among them systems based on Light Weight DRM, the PotatoSystem, and Music2Share. The particular feature of the PotatoSystem is to allow reselling by customers and thus providing incentives not only to legally buy digital products but also to contribute to the distribution. The speaker talked about digital payment methods having to be integrated into the purchase procedure. He pointed out that payment is not integrated in most of the existing DRM systems, and that this is a mistake. LWDRM and the PotatoSystem, in contrast, have payment integrated in the purchase procedure, he said. His conclusion was that a great number of consumers are ready to pay for fair use, and providers are ready to deliver content for payment, so a *mutually acceptable level* of payment is the key. Therefore, he said, *payment has to be integrated with DRM* and free usage has to be enabled after payment. Finally, he called for

## Sources

- ▶ Jeges, Ernő and Kerényi, Kristóf (ed.) (2005): E-Payment and DRM for Digital Content – Report on the 2<sup>nd</sup> INDICARE Workshop, Budapest, 3 February 2005; [http://www.indicare.org/tiki-download\\_file.php?fileId=98](http://www.indicare.org/tiki-download_file.php?fileId=98)
- ▶ Workshop-site: <http://www.indicare.org/events/>

**About the author:** Kristóf Kerényi is a researcher at Budapest University of Technology and Economics in the SEARCH Laboratory. His interests include mobile and wireless IT security, as

a harmonised solution, technically standardised and widely accepted on the market.

## Main conclusions

Perhaps the main conclusion of the workshop was that e-payment solutions must be integrated into the content purchase process. And of course if DRM is also used, e-payment has to be integrated with DRM, too. Consumers do not want to bother about technical and contractual details, they just want to see the offer as one product and then they can decide which one to choose. Of course with today's technical advancements in mobile computing and wireless connectivity traditional e-payment is shifting over to m-payment. Integration is even more important here, since consumers have already got used to the "one finger, two buttons, three clicks" rule. Any other, more complicated purchase method will be less successful.

Another key result of the workshop was that more attention should be given to consumer needs and consumer wishes. However, it is difficult to establish what they want, since they, themselves, do not know exactly what the possibilities are. Also, fair use should be considered in depth when creating new models for consumers: alternative compensation systems, like the described PotatoSystem, could have a bright future. Finding the perfect offer for consumers is, and will stay a key challenge for markets depending on DRM-protected contents.

## Bottom line

If you have more interest in the Budapest workshop, please look at the *workshop-site* where you can download the slides of the speakers' presentations. You might also want to read the more extensive *workshop report* (Jeges and Kerényi 2005) – it will bring you all of the interesting points of the presentations and of the panel discussions in detail.

well as technological aspects of DRM. He received a MSc in computer science from BUTE. Contact: kerenyi@mit.bme.hu

**Status:** first posted 22/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=89](http://www.indicare.org/tiki-read_article.php?articleId=89)

## Where do DRM- and e-payment systems meet?

By: Rüdiger Grimm, Technical University Ilmenau, Germany

**INDICARE-Interview** by Knud Böhle, ITAS, Karlsruhe, Germany with Rüdiger Grimm, Technical University Ilmenau, Germany.

The interview approaches the relation of DRM systems (DRMs) and payment systems from different angles, addressing aspects of technical integration, the need for micropayment-systems, strategic partnerships, the role of payment intermediaries in content markets, and takes a look at the near future.

**Keywords:** interview, business models, e-payments, micropayments, privacy

**About Rüdiger Grimm:** *Since September 2000 he has been professor for multimedia applications at the Technical University of Ilmenau, Germany. He also heads a research group at Fraunhofer (IDMT – Fraunhofer Institute for Media Technology). Research interests include trustworthy and secure e-commerce applications, payment systems, business protocols, privacy and digital rights. Among the solutions he has contributed to are numbered the First Virtual payment system, and more recently the PotatoSystem and Light Weight DRM. Contact: ruediger.grimm@tu-ilmenau.de*

**INDICARE:** A payment function is often regarded an important component of a DRM system. Nevertheless it seems as if there is not much communication and overlap between those dealing with e-payments and those dealing with DRMs. You are expert in both fields – would you agree that both communities are strikingly separated?

**R. Grimm:** There are two communities, partly but not completely separated. Indeed, there are a lot of "kernel" DRM systems which are not closely linked to a business model, such as Windows Media Rights Management, Helix, Atrac3 or Fairplay. Also, payment systems like PayPal or Moneybookers are not directly involved in digital goods download through a DRM system. In addition there are also business models for protected content, like iTunes and Sony Con-

nect, not associated with a strategic e-payment system. In this respect: yes, there are two different communities which are only partly interlinked.

But there are other examples of strong interrelation between these communities: The business model of the e-payment system Firstgate's Click&Buy aims at digital goods. During the payment process the purchased digital goods are tunnelled through the server farm of the payment system. This is a DRM business system. The same is true for Paybest. Paybest is closely linked with the PotatoSystem. There is no Potato download without stepping through the Paybest process. The provider of Paybest and the PotatoSystem is the same firm. And iTunes in the US (not in Europe) offer payment by PayPal, as a first step to electronic payment integration.

**INDICARE:** This means that on one side we see companies who follow an integrated approach with a business model for virtual goods in mind, and on the other side we observe an approach where different components are integrated *ex post* at the level of the eCommerce system. Why ask for co-operation and a common view if in practice there is no need for joint action and joint systems development?

**R. Grimm:** I see two reasons why the two strands are not always integrated. Number

one is the reason you mention: DRM is in the first place a technical mechanism. Only within a digital goods business system, is payment required. Nonetheless, iTunes is indeed a business system, and – in Europe – it is not interlinked with an electronic payment system. Number two is that both parties, payment systems and DRM business systems, have their own customers. It is not easy for one of the two parties to serve the customers of the other. Both want to serve their own customers. However, this situation is uncomfortable for all users. It limits market growth for both sides. Therefore, it is a matter of time until successful download or file sharing systems conclude strategic partnerships with specific payment partners. Just like eBay goes with PayPal, payment systems will concur to become strategic partners of successful download or (legal) filesharing systems.

**INDICARE:** Neither PayPal (with eBay) nor credit card payments (with iTunes) are micropayment systems. Do eContent markets need micropayment systems at all?

**R. Grimm:** Yes, they do. Payment must be (a) strongly interwoven with the purchase process, (b) immediate and able to conclude the purchase, (c) cheap enough for low-price eContent. But there are interesting other models beyond micropayment, such as packeting several purchases to one payment, or subscription, which make credit card payment cheaper.

**INDICARE:** How big is the demand for integrated DRM & E-payment systems and what are the most successful systems today?

**R. Grimm:** Successful digital goods purchase systems will provoke Internet micropayment systems. As mentioned above, FirstGate Click&Buy is a functioning integration of micropayment and download of digital goods. Paybest and PotatoSystem is another example. PayPal and Moneybookers are prominent candidates for strategic partnerships with download shops, because they do have a broad customer base. iTunes in the US have already started with PayPal.

**INDICARE:** Listening to all the names the question of interoperability as a condition for

a unified consumer experience automatically pops up. Won't we see again lots of incompatible islands? How will the interoperability problem be solved if not by a winner takes it all logics?

**R. Grimm:** Exactly so. There are so many different DRM solutions on the market, and they are all incompatible. Electronic payment is not much better. Accounts from one system cannot be used to pay with another system. So, customers get used to having as many logins, accounts, contracts and rules as they use download services and payment systems. To top this problem: They all play with the personal data of their customers. There is a huge privacy bomb out there in DRM services...

**INDICARE:** What exactly do you mean by "privacy bomb"?

**R. Grimm:** Web surfers purchase more and more virtual goods. Traces of personal data are created by communication with servers, and also in encoded form within the products. Mostly people are not aware of this networked information about their behaviour. Nor is it utilized so far. However, the information is out there, and it is increasing every day. Users should insist on being informed on the usage of their data. And providers of services should know that trust is the most important basis of business, therefore it is worthwhile to provide transparency on their actions.

**INDICARE:** Back to payments, do you think it is possible to draw lessons from the early internet payment systems like First Virtual, eCash and CyberCash for the design of DRM systems?

**R. Grimm:** All three systems worked as both, payment, and digital goods purchase. In modern language: they managed digital rights. But they were not DRM systems in the narrow sense: there was no copy protection or usage control involved. But nevertheless there are (at least) three lessons to learn: (1) payment and digital goods purchase must be simple and cheap: no public key registration or so! (2) There must be many goods of accepted value available on the Internet; (3) there must be no privacy threats.

**INDICARE:** You mentioned public keys. PKI is debated today in the context of DRM too, when it comes to the granting of exemptions from the owner's exclusive rights. At the last DRM conference in Berlin (see Orwat 2005) Thomas Dreier for example envisaged a solution to this problem through DRM systems based on PKI. What is your opinion on a PKI based DRM approach to achieve fair use?

**R. Grimm:** PKI are heavy weight for handling. PKI and signatures are fine for B2B rights management. Customers will avoid the extra load of care they have to take for their keys. PKI will be a solid basis for B2C e-Commerce if it is available and used for other purposes as well. But this is not yet in sight.

**INDICARE:** Well, in other words this means PKI and TTPs are not appropriate means to enable users to enjoy their traditional rights, like making private copies, granted by copyright? Do you have a better solution in mind how to reconcile DRMs and the legal provisions?

**R. Grimm:** Trusted Third Parties as service providers to enforce additional rights or other services (like fair exchange of high-value) might indeed be an appropriate business model. But PKI for key management just in order to sign contracts is an overload on digital goods, especially in the low value range.

**INDICARE:** From PKI to payment systems infrastructure is just a tiny step. Payment systems and also micropayment systems at the end of the day need a channel to communicate with the banking world and the monetary system. This missing link has been a problem for micropayment systems, is it an issue for DRM systems? Asked differently, what is the role for payment intermediaries in the field of paid protected content?

**R. Grimm:** The intermediaries must be the payment systems themselves. It is the purpose of an e-payment system to map the heavy-weight banking system into light-weight Internet communication. They organise intermediate accounting to bundle payment processes for clearance in the "real money world" of banks. When they do this,

they offer additional services such as reporting, control of download, re-load of lost goods, concluding a purchase.

**INDICARE:** Talking about technical infrastructures, there are (apart from convergence) still different types of networks: the open Internet, mobile phone networks and digital TV. Can we expect to see in the future most paid content via digital TV und UMTS mobile networks?

**R. Grimm:** The mobile world is special. Mobile phones are easier to protect against tampering. Individuals accept to pay for access to mobile networks. Mobile devices carry individual IDs for tracking and accounting. Bringing these points together, mobile networks are predestined for DRM-protected download and payment. Paid download of ring tones works extremely well. Therefore, the mobile industry has great hope, that it will be accepted as a digital goods purchase world. However, this will only succeed if the systems are compatible. OMA - the Open Mobile Alliance - is the relevant standardization initiative. Without success of OMA there will be no mobile DRM business.

The TV world is completely different. I don't see a strong overlap between the passive-consumption world of TV with the active consumption world of the B2C e-commerce – at least in the near future. This might change, but not very fast.

**INDICARE:** By and by p2p-Networks are being recognized by eContent industries as an opportunity (see Rosenblatt 2005). How will adequate payment systems look like for P2P networks? Can we envisage p2p networks as exponential "recommender-systems" with a payment function?

**R. Grimm:** A view into the near future, as I see it: Payment systems for digital goods within p2p-networks play the role of intermediaries between p2p value exchange and the real banking clearance. The payment system collects different payment activities and does the intermediate accounting before clearance. All services, such as provisions and special offers are managed by the pay-

ment service. Payment customers have access to a huge set of digital goods offerings.

**INDICARE:** By the way, can you imagine upgrading your PotatoSystem to p2p networks?

**R. Grimm:** Yes, PotatoSystem is prepared for an upgrade to p2p communication. This requires a close inter-play with an e-payment service, just as Paybest today. Already today Paybest is a broker for many other e-payment services such as Paysafecard, Micromoney, Moneybookers, and Click&Buy.

**INDICARE:** Isn't it amazing that we have talked all the time about DRMs without even mentioning copy protection? Looks like entering the DRM arena through the payment

door you automatically think of DRMs in terms of business models...

**R. Grimm:** Virtual goods are made for purchase and usage, not for being protected against usage. It is indeed amazing, that content providers emphasize copy protection and forget so much about new opportunities to make money. Payment brings it all together: content providers want money and consumers want products. Instead of raising border walls of usage protection between them, content providers should open payment doors to their customers and make their goods accessible – and consumable.

**INDICARE:** Thank you very much for this interview.

### Sources

- ▶ Information about the PotatoSystem mentioned several times is available at <http://www.potatosystem.com/info/eng/index.html>
- ▶ Rosenblatt, Bill (2004): Learning from P2P: Evolution of business models for online content. INDICARE Monitor, Vol.1, No 6/7, 17 December 2004; [http://www.indicare.org/tiki-read\\_article.php?articleId=61](http://www.indicare.org/tiki-read_article.php?articleId=61)
- ▶ Orwat, Carsten (2005): Report on the 3rd DRM Conference, Berlin, 13th and 14th January 2005 INDICARE Monitor, Vol.1, No 9, 25 February 2005; [http://www.indicare.org/tiki-read\\_article.php?articleId=75](http://www.indicare.org/tiki-read_article.php?articleId=75)

**Status:** first posted 15/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=86](http://www.indicare.org/tiki-read_article.php?articleId=86)

## Critical review of MPEG LA software patent claims The usage of open source rights expression languages must be royalty free

By: Dr. Susanne Guth, Vienna, Austria and Dr. Renato Iannella, Brisbane, Australia

**Abstract:** This article shows a current software patent case where the MPEG Licensing Administration (MPEG-LA) is claiming license fees for the implementation of the (open) rights expression language ODRL. ODRL has been developed by the international ODRL Initiative, a non-profit initiative mainly run by researchers. The article critically discusses the patents for rights expression languages and introduces early publications, showing that the concept of “rights expression languages or a rights grammar” is not new. Furthermore, it examines the patent claims with regard to the Open Mobile Alliance (OMA) DRM. The article is concluded with a discussion on the potential future impact of software patents in the field of DRM for open source software, research and consumers.

**Keywords:** competition, open source, patents, rights expression language, software patents

### Introduction

In January 2005 the MPEG Licensing Administration (MPEG-LA) announced the

terms of a joint patent portfolio license to be offered to implementers of the Open Mobile Alliance (OMA) DRM 1.0 specification. A

royalty payment of USD 1 is due for every device that is issued using the OMA DRM specification and a further 1% of any transaction in which an end user pays for delivery of a digital asset (cf. MPEG-LA, 2005). From this patent portfolio, we are reviewing the patents that are related to rights expression languages (RELs), e.g. the European Patent EP 0 715 244 B8 respectively the US Patent 5,715,403 “*System for controlling the distribution and use of digital works ... utilizing a usage rights grammar*” granted to the Xerox Corporation. Today the patent is controlled by the US Company ContentGuard which is owned by Microsoft, TimeWarner, and Thomson. These patents are obviously important in the MPEG-LA patent claim case, as the CEO of ContentGuard recently stated:

“The OMA didn’t choose to use our technology for implementing its Digital Rights Language for OMA 1.0, and instead chose to use a system developed by IPR systems in Australia. We told them that this wouldn’t mean that they could escape our patent portfolio and we’ve been telling them that all along” (cf. Faultine, 2005b).

The “system developed by IPR systems in Australia” identifies the Open Digital Rights Language (ODRL). For many years, the authors of this article developed with many collaborators the Open Digital Rights Language (ODRL). Version 1.1 of ODRL (part of the OMA 1.0 and OMA 2.0 specifications) has been implemented; license tools for ODRL have been created, and devices embedded with ODRL. With the experiences of this and other work, the ODRL Initiative members have improved and extended the ODRL data model and are creating profiles to integrate ODRL and adjacent metadata standards. The ODRL Initiative is about to publish these new research findings in ODRL Version 2.0. The new version meets all gathered requirements from the last years of experiences, and it will make the usage, implementation and processing of rights expression languages more efficient and less ambiguous and takes a step towards more interoperability between the different existing RELs. This ODRL research has mostly been supported by European and Australian

research funding and was intended to be made freely available (under open licenses) for other researchers worldwide.

The MPEG LA patent claims state that every service provider or device seller that implements the open source rights expression language ODRL as per the OMA DRM specifications shall be obliged to pay a levy to the MPEG-LA consortium members. As ContentGuard claims to hold patents on *any* REL, not just only their own solution XrML (see also Böhle 2005 and Berlecon Research 2005), it is unclear on the extent of the patent claims to any version of ODRL (now or in the future) and other machine-based languages, such as the open and free Creative Commons licenses. At present, the MPEG LA patent claims seem targeted at OMA DRM implementations only and do not seem to apply to other (non-standard) DRM implementations on mobile devices and services.

The business model of open source is to freely distribute software and technical specifications and earn money with consulting and other services. If the implementation of ODRL or the simple usage of ODRL tools leads to potential royalty payments, the attractiveness of ODRL will shrink and the further work of the ODRL Initiative is seriously jeopardised. RELs like ODRL are gaining importance in University and European research projects for the creation of platforms to distribute learning material (script, slides, and examples) (cf. EducaNext 2005).

Rights expression languages are only a small building block of the Digital Rights Management Technology but all other components of DRM systems are most likely affected by software patents in the same way. This article will focus on the specific case of above named patents on rights grammars to illustrate problems and confusions arising from software patents.

### **What is a rights grammar?**

As ContentGuard claims to hold a patent on *any* rights grammar, at this point one has to pose the question: What exactly is a rights grammar? ContentGuard always uses the

term “rights grammar” synonymously with “rights expression language”. Linguists would probably not agree here in the first place, however, a rights expression language is a *language to express usage or access rights for parties over assets*. A simple rights expression in ODRL granting the user `sguth` the right `display` for the asset `proceedings2005` looks as follows:

```
<rights>
  <agreement>
    <party>
      <context>
        <uid>sguth</uid>
      </context>
    </party>
  <permission>
    <display/>
  </permission>
  <asset>
    <context>
      <uid>proceedings2005</uid>
    </context>
  </asset>
</agreement>
</rights>
```

But also consider these two examples:

- ▶ If the system administrator of a Linux Server sets the “group” rights of file Z to “read, write, execute”, he is using some kind of rights grammar.
- ▶ If, in a running computer system, four software objects of an access control mechanism, e.g. the party object `drmUser`, the asset object `musicFile`, the permission object `play`, and the constraint object `untilTomorrow` are related to each other and therewith constitute a rights expression, the system uses some kind of object-oriented rights expression language, too.

Do the REL patents now apply to access control software in general? Numerous copyrighted works that describe access control mechanisms and their implementation, such as discretionary access control (access control lists, capabilities), role based access control, etc. were published long before the filing of the ContentGuard patents. Countless research papers also include formal models with respect to computer system security (cf. Landwehr 1981 and Burrows et al. 1991).

Most rights expression languages existing today are technically defined in XML schemas. Not using an XML-based rights expression language simply means that you grant or deny access rights with former programming means, i.e. access control information that is captured in software objects or variables, as shown in the two examples above. The following section will try to clarify the coverage of so-called software patents, particularly with respect to the above mentioned patents on rights grammars.

### Investigation of ContentGuard patents with regard to (European) patentable inventions

“European patents are granted for any inventions which are *susceptible of industrial application*, which are *new* and which involve an *inventive step*” (cf. European Patent Convention, 1973).

Please note that the proposed software patent directive (cf. European Commission, 2002) in the EU has not yet passed the EU parliament. The European patent of ContentGuard has been filed under the Convention on the Grant of European Patents of 1973.

In the current European jurisdiction “programs for computers” are not patentable unless they are new and provide a *technical contribution* or *further technical effect* to the prior art. Additionally, to be patentable, an invention must have *technical character* and must be *non-obvious*.

- ▶ The invention must have overall **technical character**. This means that the invention must use technical features and solve a technical problem. For example, software running on a computer has technical character.
- ▶ The invention must be a new **technical contribution** or **further technical effect**, i.e. a solution of a technical problem, e.g. an improvement of computing efficiency.
- ▶ The invention must be **non-obvious**, i.e. the invention must be beyond state-of-the-art and non-trivial for an expert in the field.
- ▶ The invention must be **new**, i.e. the applicant of the patent must be the originator of the invention (i.e. not prior art).

In the following paragraphs, we would like to address the named requirements with respect to the above mentioned patents on rights expression languages.

#### *Technical character*

What would a software patent in the EU have to look like that applies to *any* rights language if the invention must have overall *technical character*? Such an invention would have to include the underlying data model, the technical specification and implementation of all today's and tomorrow's rights expression languages. The current rights expression languages already serve different domains (music industry, publishing industry, education), have different focuses (licenses, tickets, contracts), thus have varying data models resulting in diverse technical specifications, XML schemas, and implementations. The above named patents need to be investigated with regard to this requirement.

#### *Technical contribution and non-obvious invention*

Some facts: In 1969 the first mark-up language (GML) was developed by Goldfarb, Mosher, and Lorie followed by the Standard Generalized Markup Language (SGML), becoming ISO standard in 1986 (cf. ISO 1986). The successor of SGML is XML (eXtensible Markup Language) respectively XML schema. Today, mark-up languages are widely used and state of the art. The important inventions and copyrighted work in the field of access control were published in the 1960s and 1970s.

Rights expressions have existed since humankind can talk. The example: "I lend this book to you until tomorrow" is a human readable example of a rights expression language. Is a machine readable example of this rights expression language a technical contribution to the state-of-the-art if neither the means of writing (XML) nor the content (access control expression) is new? Since mark-up languages are state-of-the-art, experts use them to describe all kinds of things: books, individuals, and also rights. As mentioned above, common rights expression languages, including MPEG REL, XrML and ODRL, use XML Schema for their serializa-

tion. XML Schema can be regarded as state-of-the-art technology. General, freely available XML parsers can be used to interpret and process MPEG REL, XrML and ODRL rights expressions.

#### *New (prior art)*

For a patent to be accepted, it must pass a number of key requirements as outlined above. These include that no "prior art" in this invention currently exists. The process to determine these requirements are "self determined". That is, the patent applicant argues in the proposal that the invention meets these requirements. The patent administrator must make a judgement call based only on this information as they are not experts in the area of the invention.

In the case of the ContentGuard patent ('403) – filed on November 1994 - a number of prior art inventions were overlooked. In particular, the well-known work of Ted Nelson's Xanadu project from the 1980s (cf. Samuelson & Glushko, 1991) clearly a decade before the '403 patent submission. Nelson's work is "novel in proposing to use a contract-based scheme for commercial distribution of written texts" and was also novel in "charging for each and every *use* of their documents" rather than each *copy*. The Xanadu project used an "intuitive *rights-to-do* framework", that is, a system that enabled the user rights to be described for content that limited its use. Strangely, the '403 patent references only a 1994 work of Ted Nelson but does not discuss it.

The European ESPRIT Project "Copyright in Transmitted Electronic Documents" (cf. The CITED Project) from 1990-1993 developed a model that provided control, policing and remuneration, in respect of the use of copyrighted material stored and transmitted in digital form. The project demonstrated and implemented software with mechanisms such as "The Use Right Collector (URC) that collects and manages the use right data base and links the data with their associated rights".

Henry H. Perritt (1993) wrote about the concept of "permissions headers" in which rights information would be attached to every digital work distributed across networks. He indicated that "this representation problem

may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions."

#### *Summary*

From this understanding, we conclude that a patent on *any* rights expression language is not possible under current European jurisdiction and would be highly doubtful worldwide. Such a patent would only be relevant to the specific implementation that it describes. The technical implementations of DRM systems today differ widely from the ideas over a decade ago. The original '403 patent authors at Xerox had a "print industry" view of the world and probably would not have even contemplated that a REL would one day be in a small mobile device managing music delivery. Therefore, open source rights expression languages must be untroubled by the software patent levy.

#### **Examining the ContentGuard patent claims with regard to OMA DRM**

MPEG-LA claims that their patent portfolio applies to the OMA DRM standards and a license must be obtained. MPEG-LA has not released the full list of the patents in question and how/where they apply to an OMA DRM implementation. One needs to take it "on faith" that all the patents do apply.

If we look at the details of the '403 REL patent as an example, some interesting facts are revealed:

Patent '403 claims that "Digital works and their attached usage rights are stored in repositories" and "The enforcement elements of the present invention are embodied in repositories" and defines repository functions to include "... store digital works, control access to digital works, bill for access to digital works, loan digital works or automatically handle the commercial reuse of digital works, and maintain the security and integrity of the system". The model is clearly one of advanced repositories undertaking the major functions of the DRM transactions. In the mobile world, it is unlikely that a DRM client on a mobile phone would fall into the category of a "repository" as defined by patent '403. Additionally, the "enforcement

elements" of OMA DRM are provided by encrypting the content and storing the keys in separate protected licenses. The OMA DRM model does not use a "repository" to request and allow access to content as this is handled by a client application on the handset.

Patent '403 claims that "A key feature of the present invention is that usage rights are permanently *attached* to the digital work" and that "It is fundamental to the present invention that the usage rights are treated as part of the digital work." This is quite the opposite in OMA DRM implementations. The content and license (usage rights) are separate data files and are never "permanently attached" to the content. Additionally, with superdistribution in OMA DRM, the content is sometimes not associated with any "usage rights" until after purchase.

Patent '403 claims that "The usage rights language is based on the grammar described below. A grammar is a convenient means for defining valid sequence of symbols for a language." The grammar of the OMA DRM licenses is based on XML, and more formally on XML Schema, which has its basis on the DTD (Document Type Definition) from SGML developed in the 1980s, and does not resemble the grammar in the '403 patent.

These are just a few examples of aspects of the '403 patent that need careful analysis for their applicability to current implementations of DRM systems.

#### **Discussion**

##### *Is the MPEG LA patent portfolio removing uncertainty?*

The MPEG LA is pooling (DRM) patent owners and offers implementers of patent affected (DRM-)technology a patent portfolio for a certain price (such as USD 1 per device and 1% of the digital asset's cost). The Vice President of MPEG LA states that "a patent portfolio assists in removing the uncertainty surrounding the 'patent overhang' " (cf. Horn, 2005), i.e. it is a convenient and efficient way to access the (DRM) technology. On the other hand the patent pooling makes the patent claim non-transparent. In the OMA DRM case it is not clear which patents apply to which parts of

the OMA DRM specifications. What consequences would it have if the '403 patent claims with respect to rights grammars turn out to be unjustified? To what extent would that reduce the patent levy? What about all the other patents in the portfolio? Who provides an independent analysis of them? From this point of view the pooling of patents probably causes rather than removes uncertainty.

In the latest news, the Mobile Entertainment Forum (MEF) announced that it has issued a statement regarding the licensing program proposed by MPEG LA for Mobile Digital Rights Management (Mobile DRM) saying that: "The terms being considered by MPEG LA ... could have a devastating effect on any business involved in mobile and wireless entertainment" and "that MPEG LA's proposed royalty rates are onerous, impractical and unclear" (cf. w/o, 2005).

*What are the possible consequences for the customer?*

- ▶ It was the aim of the Open Mobile Alliance to develop an *open* standard, to minimise any impact of patents, and to eliminate royalty payments (cf. Buhse 2004). Hence, all players in the mobile industry had a high motivation to support and implement this standard. Now, device sellers and service providers have been faced with a new potential royalty payment to MPEG-LA - significant additional costs that have not been calculated in their business models. This may also lead some vendors to continue to implement their proprietary DRM systems as there is little benefit in moving to the "open" standard. In this case the customers would have to bear the consequences of non-interoperable mobile phones.
- ▶ If the claims of MPEG LA can be imposed (and software patents continue to be granted), the additional costs of the above mentioned patent levy will be transferred to the customer. The latest news about the adoption of software pat-

ents in Europe (cf. The Copenhagen Post 2005) shows that software licensing will be an important future business of large software companies.

*What are the consequences for the ODRL Initiative and Open Source Developers in general?*

If the claims of MPEG LA are validated, the work of the ODRL Initiative and other RELs such as the Creative Commons Licenses will be critically endangered. No open source developer would have a motivation to work on new concepts and implementations for RELs if the royalties for their application are paid to a different organisation. This would mean that open source developers, researchers and universities would have to now constantly monitor and review software patents in future. They will have to apply for patents themselves in order to make research freely available for the public and other researchers. This is costly (maybe not realizable with the restricted budgets at universities) and time consuming (i.e. disables progress). Additionally, the many software patents are an unpleasant surprise for researchers (and others) that started their work in a software patent free environment and are then faced with the fact, that maybe a large part of their work is not sufficiently protected by copyright. This has happened in Standards groups previously and has earned the name "submarine patents" – that could surface at any time in the future.

#### **Bottom line**

From the concrete case above we can summarize that more transparency is needed with respect to the legal basis of software patents and its application to DRM technologies. The MPEG-LA patents have the clear potential to disturb research and development in the field of RELs and other DRM technologies. Furthermore, the MPEG-LA patent claims have a negative effect on the growth of European mobile (entertainment) industry. This article is also an appeal to politicians and patent offices to rethink the proposed software patent directive in the EU.

#### **Sources**

- ▶ Berlecon Research (2005): DRM, DRM Patents and Mobile DRM, Berlecon Whitepaper, [http://www.berlecon.de/output/en/studien.php?we\\_objectID=207](http://www.berlecon.de/output/en/studien.php?we_objectID=207)

- ▶ Böhle, Knud (2005): Obscurity in Patent Matters, INDICARE Monitor, Vol. 1, No 9, [http://www.indicare.org/tiki-read\\_article.php?articleId=82](http://www.indicare.org/tiki-read_article.php?articleId=82)
- ▶ Buhse, Willms (2004): Open DRM standards for interoperable mobile services, INDICARE Monitor, Vol. 1, No 3, [http://www.indicare.org/tiki-read\\_article.php?articleId=37](http://www.indicare.org/tiki-read_article.php?articleId=37)
- ▶ Burrows, Lampson, Plotkin (1991). A Calculus for Access Control in Distributed Systems. Advances in Cryptology -- CRYPTO '91, Springer-Verlag (August 1991), pp 1-23
- ▶ Coverpages (2005), Patents and Open Standards; <http://xml.coverpages.org/patents.html>.
- ▶ Creative Commons: <http://www.creativecommons.org>
- ▶ European Patent Convention (1973), Convention on the Grant of European Patents, Art.52, Patentable inventions; <http://www.european-patent-office.org/legal/epc/e/ma1.html#CVN>
- ▶ Faultline (2005a) : ContentGuard talks DRM futures, The Register; [http://www.theregister.co.uk/2005/01/19/contentguard\\_drm/](http://www.theregister.co.uk/2005/01/19/contentguard_drm/)
- ▶ Faultline (2005b) : Mobile DRM Levy Hits Operators Where It Hurts, The Register; [http://www.theregister.co.uk/2005/01/19/mobile\\_drm\\_levy/](http://www.theregister.co.uk/2005/01/19/mobile_drm_levy/)
- ▶ Horn, Lawrence (2005): MPEG-LA's portfolio license – A jumpstart for DRM-based markets?, INDICARE Monitor, Vol. 1, No 9, [http://www.indicare.org/tiki-read\\_article.php?articleId=81](http://www.indicare.org/tiki-read_article.php?articleId=81)
- ▶ ISO (1986) Standard. No. 8879. Information Processing -- Text and Office Systems - Standard Generalized Markup Language (SGML), <http://www.iso.ch/cate/d16387.html>
- ▶ Landwehr (1981): Formal Models for Computer Security, ACM Computing Surveys, Vol. 13, No.9
- ▶ MPEG-LA (2005): News Release, MPEG LA Announces OMA DRM Patent License Terms; [http://www.mpeg-la.com/news/n\\_05-01-06\\_drm.pdf](http://www.mpeg-la.com/news/n_05-01-06_drm.pdf)
- ▶ Perritt, Henry H. (1993): Knowbots, Permissions Headers and Contract Law. Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment Conference. April 2-3, 1993; <http://www.ifla.org/documents/infopol/copyright/perh2.txt>
- ▶ Samuelson, Pamela; Glushko, Robert J (1991): Intellectual Property Rights for Digital Library and Hypertext Publishing Systems: An Analysis of Xanadu. ACM Hypertext 1991 Proceedings, December 1991, pp. 39-50
- ▶ The CITED Project website is available at: <http://www.newcastle.research.ec.org/esp-syn/text/5469.html>
- ▶ The Copenhagen Post (2005): Bill Gates threatens to close Navision in Denmark, <http://www.cphpost.dk/get/85881.html>
- ▶ The EducaNext Platform (2005) website is available at: <http://www.educanext.org>
- ▶ The European Commission (2002): Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions [http://www.europa.eu.int/comm/internal\\_market/en/indprop/comp/index.htm](http://www.europa.eu.int/comm/internal_market/en/indprop/comp/index.htm)
- ▶ The Open Digital Rights Language (ODRL) Initiative, website is available at: <http://www.odrl.net>
- ▶ The Open Mobile Alliance (OMA) website is available at: <http://www.openmobilealliance.org>
- ▶ The Project Xanadu website is available at: <http://www.xanadu.com/>
- ▶ w/o (2005): MEF Issues Industry-Wide Position on MPEG LA's Proposals for DRM Licensing, Business Wire, News of 21. March, 2005; [http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news\\_view&newsId=20050321005243&newsLang=en](http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20050321005243&newsLang=en)

**Disclaimer:** The content of this article was compiled with the greatest possible care but should not be taken as legal advice in patent matters. The authors cannot take any responsibility for its correctness or completeness. Names and terms used in this article may be trademarks.

**About the authors:** *Susanne Guth* received her master's degree in information systems from the University of Essen (Germany) in 2000. She specialized in software techniques and production/operations management. Since August 2000, she has been an assistant professor in the department of information systems at the University of Economics and Business Administration in Vienna, Austria. For the last four and a half years, her research focus has been on contract and rights management for digital goods. She wrote her doctoral thesis in this field. Susanne Guth is a private, active member of the ODRL Initiative, leading the development of ODRL Version 2.0.

*Renato Iannella* is a researcher at National ICT Australia (NICTA). He has extensive experience in the development and standardization of Internet, Web, and mobile technologies and was a former member of the World Wide Web Consortium (W3C) Advisory Board. He is also visiting

associate professor at the University of Hong Kong and was previously the chief scientist at IPR Systems and principal research scientist at the Distributed Systems Technology Centre (DSTC).

**Status:** first posted 22/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=90](http://www.indicare.org/tiki-read_article.php?articleId=90)

## Economic analysis of DRMs roll-out over the Internet

By: Olivier Bomsel and Anne-Gaëlle Geffroy, Ecole des Mines de Paris, France.

**Abstract:** After a functional definition of DRM systems (DRMs), this article studies the economic mechanisms of their roll-out over Internet networks. We underline the difficulty of their adoption by the vertical media chain (equipment and networks industries) on two-way communication networks compared to traditional one-way networks. We then analyze the overall competition between broadcast, physical, free and DRMs-based Internet distribution of digital contents.

**Keywords:** economic analysis, business models, competition, consumer behaviour, content protection, copyright law, stakeholders, standards

### Introduction

This article stems from a study on the economic analysis of DRMs (Bomsel and Geffroy 2004) carried out within the FP6 IST project MediaNet. The objective of this project is to remove the obstacles to end-to-end digital communications and content exchange, from content/service providers to customers and between persons. In the MediaNet open architecture model it is crucial to examine the conditions under which Digital Rights Management systems could emerge and be reliable enough to ensure the compatibility of circulation of both copyrighted and non copyrighted material.

Digital Rights Management systems are means of assigning access to digital contents. This paper deals with the economic characteristics of DRMs. First, it aims at defining their economic functions, that is to say content *protection* and *versioning*. We then analyze the mechanisms of DRMs adoption over the Internet. Emphasis is put on the importance of network effects on complementary goods within dynamic vertical relations. We underline the difficulty of DRMs roll-out over two-way communication networks and draw the comparison with traditional one-way distribution networks. The final question is the overall competition between broadcast, physical, free and DRMs-based Internet distribution of digital contents.

### DRMs: Protecting and versioning contents in the digital era

*DRMs: Protecting contents in the digital era*

The first goal of DRMs is to protect the exclusive rights of content owners. On the one hand – comparably to physical supports or entrance tickets – they exclude consumers from the consumption of the cultural good if they don't pay the price for it. On the other hand, they determine the range of uses granted to the consumers like other copying control mechanisms.

DRMs and all other private protection tools supplement copyright laws. Yet they follow different objectives. While private protection measures are designed to maximize rights owners' benefits, copyright law seeks for optimal social welfare. It therefore makes a trade-off between excludability, which provides incentives to creation, and the social benefits of diffusion. That is why the exclusive rights granted to the content owners are limited both in length and in scope by exemptions, like *fair use* and *first sale* doctrines.

Digitization has changed the terms of copyright laws' trade-off. By dramatically reducing the costs of copying, storing and transmitting digital files, it has increased diffusion possibilities together with threats to content owners' revenues and incentives to create.

The DMCA (1998) and the EUCD (2001) made a relatively clear choice towards strengthening the ownership rules. While the first sale doctrine or principle of exhaustion cannot apply to digital files, anti-circumvention rules enable DRMs to override the traditional *fair use* limitations of copyright laws.

#### *DRMs: Versioning contents in the digital era*

The second function of DRMs is the versioning of contents. Contents address markets through a form of price discrimination called quality pricing or versioning. The idea is to offer different qualities of the good at different prices to get consumers select themselves from among these versions, according to their different willingness to pay. Think, for instance, of hardback and paperback versions of a good.

DRMs enable content owners to make further versions of a digital file with respect to the liberalities of uses attached to it. They allow copyright owners to charge a price that varies according to the particular uses authorized. To be more concrete, digital files with embedded DRMs may offer various rights to modify or excerpt, time of possession, number of accesses, of copies on different devices or of people one can share with.

DRMs' enhanced versioning possibilities not only mean that content owners will better extract consumers' willingness to pay and increase their profits. Although it seems at first unfair to make people pay different prices, it may improve consumers' overall welfare. By enlarging the range of prices, versioning can allow more people to access the good, more consumers to be served. For instance, if audio digital file versions with restricted uses are sold at far lower prices than digital files with more liberal uses or than physical supports, new consumers may be able to enjoy songs.

#### **DRMs roll-out and distribution networks competition**

##### *DRMs, network effects and standardization*

Contents can't be taken apart from their distribution networks and encryption standards have to be accepted by the entire vertical media chain.

Networks effects are attached to products for which users' benefits increase with the number of users. Rolfs (1974) showed that there is a critical mass of subscribers below which a network cannot be sustainable. Once it is reached, every new consumer brings additional utility to all the others and the roll-out speeds up. A general rule to reach the critical mass is to subsidize the early adopters.

Distribution networks roll-out may be subsidized by piracy or circumvention of copyrighted media contents: the utility of the distribution industry is increased by the availability of free contents. This situation existed well before digitization. Yu (2003) and Varian (2004) refer both to the American delay of the International Copyright Act in the 19<sup>th</sup> century, that enabled the expansion of the domestic publishing industry thanks to pirated English novels until the rise of domestic authors at the end of the century (Hawthorne, Poe, Twain, etc.). As for content owners, they need their content to be protected against circumvention and benefit from its compatibility with the largest range of equipment. They have to make equipment and delivery networks industries accept a protection standard. But it is a different burden in two-way communication networks and in traditional one-way distribution ones.

In the case of one-way networks, like physical or broadcast distribution, content owners control the availability of contents and the indirect network effects. Equipment manufacturers have to accept their protection standard. An illustration of this idea is the recent broadcast flag agreement for the US over-the-air digital TV.

Over two-way communication networks like the Internet, everyone can technically broadcast contents. Moreover, circumvented contents are made available by individuals and not by professional pirates that could be located and prosecuted relatively easily. These contents are widely compatible thanks to free encoding formats like MP3 or DivX. As of today, the broadband Internet roll-out is largely subsidized by circumvented contents available through P2P applications. Circumvention benefits all complementary equipment as PCs, microprocessors, operating

systems, printers, Internet modems, media players... . While DRMs oppose these Internet network effects, equipment and networks industries are not enforced to accept any encryption standard.

Nevertheless, some actors consider that DRMs roll-out is likely to happen in the future and are positioning themselves to have their proprietary solution accepted as the standard. That is for instance the game of Microsoft, Apple and Sony in the digital music market. This game results in a standards war bringing incompatibility between DRMs. It delays DRMs adoption by consumers and extends over time the cross-subsidy of equipment and networks through copyright circumvention.

#### *DRMs and the overall competition between distribution networks*

The standards war on DRMs penalizes *legal* digital content distribution over the Internet and therefore benefits alternative diffusion systems: circumvention through P2P sharing, broadcast on dedicated networks and physical distribution. The overall competition between these different distribution networks depends also on price, quality, novelty and liberalities of uses.

- ▶ Physical versions could last for more than forecasted. They can increase their utility through quality and information density, decrease its prices or innovate in distribution like in the Netflix model (online DVD rental choice combined with postal delivery and return). Finally it can benefit from a valuable equipment legacy (the large base of DVD players).
- ▶ Content owners should push dedicated distribution networks like television or mobile phones. From an economic perspective, mobile phones are very comparable to broadcast networks because they distribute communication services according to a pay-for-service model. These distribution networks benefit from

a stronger content protection and are easier to standardize. They could therefore benefit durably from a larger range of contents

- ▶ As for free contents on P2P networks, their total liberty of use contrasts with DRMs-files opaque restrictions and the advantage of DRMs-files is not systematic on quality and novelty. The on-going circumvention dynamics may have irreversible effects on broadband pricing and equipment. Being used to pay for capacity only (storage, processing, bandwidth) and to get always more value for his money, the broadband consumer may be reluctant to pay for services or contents. This behaviour may orient future investment in broadband networks.

#### **Bottom line**

DRMs are necessary to bring exclusion to digital IP goods. They are the only means to enable the exclusiveness of intellectual property rights and consequently, the sufficient incentives to create. While they restrict the short term consumers' benefits of cultural goods free diffusion, they insure their long term welfare by enabling these cultural goods to be financed and produced in the future.

The success and the pace of DRMs adoption will determine the format of the future digital libraries, whether encrypted or not. Two kinds of networks are presently competing to diffuse digital contents. One, the descending distribution model, in which the content owner masters the utility of the network, is DRM friendly. The other, the Internet open communication network, carries major circumvention incentives. A crucial stake in this competition is the roll-out of the home network equipment, i.e. the investment made by the consumer to equip his home with connected digital devices. This process will be shaping the access, the uses and the willingness-to-pay of the consumer for contents.

#### **Sources**

- ▶ Bomsel, Olivier and Geffroy, Anne Gaëlle (2004): Economic Analysis of DRMs. IST-Project: FP6-507452. Deliverable DB.5.14; <http://www.cerna.ensmp.fr/Documents/OB-AGG-EtudeDRM.pdf>
- ▶ Bomsel, O; Le Blanc, G.; Charbonnel, J.; Zakaria, A. (2004): Economic issues of content distribution. Cerna, Ecole des Mines

- ▶ DMCA (1998): Digital Millennium Copyright Act; [http://www.eff.org/IP/DMCA/hr2281\\_dmca\\_law\\_19981020\\_pl105-304.html](http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html)
- ▶ EUCD (2001): European Copyright Directive; [http://europa.eu.int/information\\_society/topics/multi/digital\\_rights/doc/directive\\_copyright\\_en.pdf](http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf)
- ▶ Fisher, William W. III (2004): iTunes: How copyright, contract, and technology shape the business of digital media – A case study. Digital Media Project. Berkman Harvard Law School.
- ▶ MediaNet: Homepage of the project is at <http://www.ist-ipmedianet.org/home.html>
- ▶ Rohlfs, J. (1974): A theory of interdependent demand for a communications service. *Bell Journal of Economics* 5 (Spring):16-35.
- ▶ Varian, Hal R. (1997): Versioning information goods. (1998): Markets for information goods. (2003): The social cost of sharing. (2004): Copying and copyright. All papers are available at: <http://www.sims.berkeley.edu/~hal/people/hal/papers.html>
- ▶ Yu, Peter K. (2003): The copyright divide. Michigan State University.

**About the authors:** *Olivier Bomsel* is senior researcher and professor of industrial economics at CERNA, Ecole des Mines de Paris. Contact: [bomsel@ensmp.fr](mailto:bomsel@ensmp.fr).

*Anne-Gaëlle Geffroy* is Ph.D. Student on the economics of digital contents at CERNA, Ecole des Mines de Paris. She works currently on digital copyright and vertical contracting issues in the media chain. Contact: [ageffroy@ensmp.fr](mailto:ageffroy@ensmp.fr).

**Status:** first posted 09/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=84](http://www.indicare.org/tiki-read_article.php?articleId=84)

## Violation of consumer rights with DRM-based usage control systems – The case of Half-Life 2

By: Danny Vogeley, Berlecon Research, Berlin, Germany

**Abstract:** DRMs for computer games was just about copy protection for a long while and it wasn't a hot topic. This is about to change with the Internet enabling DRM-based online usage control systems. The case of Half-Life 2 illustrates the potential of this approach and how it can be abused to violate consumer rights. Even though most players are heavily complaining about the usage control system, most of them do not forgo to play Half-Life 2.

**Keywords:** technical analysis, access control, consumer rights, content protection, games, usage control, transparency

### Introduction

Discussions about DRM usually focus on digital music or movies. The game market is often neglected in these discussions, despite its rising market size and the increasing relevance of DRM for the game industry.

In the USA 2001, the market volume of the game industry (9,4 billion Dollars) exceeded for the first time the turnover of the movie industry (8,1 billion Dollars) (Wirtz 2003, p. 493). The production and marketing costs of high quality games such as “Lord Of The Rings – The Two Towers” by market leader Electronic Arts was above 25 million Dollars (Jensen 2003, p. 49). Successful games like

Myst have realized revenues of 125 million Dollars (Wirtz 2003, p. 493). It is estimated that the turnover of the PC and video game market worldwide is about 18,8 billion Euros (VUD 2005).

### Rising importance of DRM in the game market

Piracy and the emergence of new DRM-based business models are a big issue in the game industry as well. National entertainment software associations worldwide like the British ELSPA ([www.elspa.com](http://www.elspa.com)) or the German VUD ([www.vud.de](http://www.vud.de)) are complaining about massive sales losses due to illegal circulation of game copies. For example, it is

estimated that in Germany about 11 million blank CDs/DVDs have been illegally used to burn copies of games between January and June 2004 (GfK 2004).

Therefore, the most important role of DRM in the traditional gaming market has been pure copy protection for CDs and DVDs. But other roles of DRM are gaining more and more importance. Similar to the digital music and movie market, DRM systems are now more frequently deployed to enable new online distribution (streaming, full-download) or revenue models (subscription services, pay per game/time).

In addition, new roles that are rather unique to the game market are gaining significance. Examples are the management of the game play and persistent online usage control. The management of game play relates to the control of a played game itself. For example, in multiplayer online role games, the developer is in charge to supervise a virtual world. Among other things, a developer prevents cheating among role players or controls the trade of virtual assets. Virtual assets, such as valuable weapons or virtual money, have often been traded on eBay without the permission of the game developer. Therefore, DRM can be implemented in virtual assets to control or restrict such trading.

Online usage control encompasses the management of access to and further usage of retail games via the Internet. Retail games are sold in CD or DVD boxes, which are usually played in offline modus on PCs. Traditional access control mechanisms of retail games are focused on a closed system environment: When the copy protection of a game has been cracked or a license number is shared, it can be easily disseminated to other systems beyond the developer's control. However, the Internet has enabled new control mechanisms, which have the potential to manage the access and further use of a game persistently. They can be considered as DRM technology, because they give a content distributor a sophisticated means to manage game users' rights persistently. Persistent usage control mechanisms have a special potential on the game market, because for game players there exist incentives to uphold

an online relationship with the game developer. Unlike music or movies, games themselves are highly adaptable and can be enriched with additional features like new game levels, maps or weapons. There is a high demand for such features for an enhanced and continuous game play.

Online usage control systems force the purchaser of a retail game to validate it via the developer's online platform. If a developer assumes an illegal use, he may disable an account instantly. Game access activation can be required only once during game installation or repeatedly over a given period. The latter gives the game provider an ongoing control system to identify illegal licenses. Although a user might have successfully registered an unlicensed copy of a game at the initial activation process, he cannot be sure if this illegal license will not be detected the next time. As a result, to crack a game only once will not be sufficient any more. This is especially efficient against the casual user, who often receives cracked games or licenses from friends.

### **Case Study: Half-Life 2**

The first game developer to use DRM as an online usage control system for retail games is Valve. Valve uses its online platform "Steam" as a Digital Rights Management system to verify legitimate access keys and to keep control of the further usage of its games. Steam is also deployed to administer customer billing, to provide updates and to allow the users to backup games on CD-Rs or DVD-Rs. Valve introduced Steam as a DRM system with the release of Half-Life 2 in October 2004. Half-Life 2 is a so-called first-person shooter game, in which the user basically takes a first-person perspective in a three-dimensional space to battle against enemies. It also provides the option to play it in a multi-player mode. Half-Life 2 is a long-awaited sequel to Half-Life in the game community. Its production time was several years.

To install Half-Life 2, Valve requires in addition to an online activation the creation of a personalized online account via Steam. If Steam detects any identical licenses, it will cancel all accounts that have used these li-

censes. Steam even disables the account of the user that originally obtained the license legally. Valve claims to have cancelled more than 50.000 (allegedly) illegal accounts so far.

Beyond the pure authorization of legally obtained games, Valve's Steam also has the potential to intensively control the user. For example, Steam has been abused to postpone the point in time when users were able to start playing Half-Life 2. After the official release of Half-Life 2 in November 2004, purchasers were not able to install and play their games for almost one week. Valve had been in a contractual licensing dispute with its distributor Vivendi, which did not allow Valve to unlock Half-Life 2 during this legal issue. In this case, the purchasers of Half-Life 2 were locked in a licensing battle between two corporations (Grimmelmann 2003).

The relevance of usage control systems will gain significance, when they are used to enforce changes to an End User License Agreement (EULA). For example, Valve reserves the right to change fees or billing methods at any time. Therefore they force users to agree to review the EULA periodically for any amendments:

*“Valve reserves the right to change (...) fees or billing methods at any time and Valve will provide notice of any such change in at least thirty (30) days advance. All changes will be posted as amendments to this Agreement or in the Rules of Use and you are responsible for reviewing the billing section of Steam to obtain timely notice of such changes.”*

*“Your non-cancellation of your Account thirty (30) days after posting of the changes on Steam means that you accept such changes.”* (Steam 2005, section 4b)

In other words, Valve basically allows its customers to use their game only as long as Valve wants them to have it. Valve claims the right to demand additional fees at any time without notifying its customers personally. When a user connects to Steam to receive additional features or necessary patches, which are normally provided for free, he cannot be sure if he will not be billed. With Steam, any changes in the

EULA will affect the game user instantly. Regardless of whether Valve has the legal right or not to disable accounts, Valve can simply do it. And if one considers going to court, it is especially difficult for non-US citizens to sue this US-based company for any unfair practice. With Steam in combination with its EULA, Valve can be described as judge, jury and executioner.

In another section of the EULA, Valve claims the right to download via Steam additional software or updates on users' computers without noticing them:

*“Steam and your Subscription(s) require (...) the automatic download of software, other content and updates thereto onto your computer. (...) You understand that Steam may automatically update, pre-load, create new versions or otherwise enhance the Steam Software and accordingly, the system requirements to use the Steam Software may change over time.”* (Steam 2005, section 2b)

Users of Half-Life 2 have to agree that Valve is going to download software beyond the users' control, when they connect to Steam. This can be convenient to keep the game up-to-date automatically. But the consumers do not have the choice whether they are going to allow it or not. This lack of control is especially critical, because Valve does not guarantee that the downloads will be virus-free or secure (Steam 2005, section 9b).

Even though playing the game does not require a connection to Steam after the initial activation process, the default setting of Half-Life 2 automatically establishes an online connection to Half-Life 2. Many game players are not aware of the possibility to play this game in offline mode and changing the default settings is rather complicated. The documentation about this function is limited.

### **How do the consumers react?**

However, Valve's online usage control system and its restrictive EULA did not result in low sales of the game. Quite the opposite can be observed: Between November 2004 and January 2005 Half-Life 2 has been sold more than 1.7 million times. Currently it is still one of the best sold games worldwide.

Looking at different game forums on Half-Life 2, the online activation via Steam and the continuous binding to this online platform is by far the most discussed topic. But although there are mostly massive complaints about Valve's rigid usage control system, most of the players would not forgo buying the game. In contrast, there are hardly any extensive discussions on how DRM systems might enforce amendments to the End User License Agreement. Therefore it can be assumed that most users of Half-Life 2 are not aware of the content of the EULA. Often users of games or other software products do not read EULAs. EULAs are considered too long and incomprehensible. Above that, Valve's EULA is only available in English, which is a hurdle for many non-English speakers. It can be assumed that most users are not aware of how amendments in the EULA can be enforced by Steam. Game players have so far no experience with this kind of extensive user control.

This case is also about transparency. Recently the Federation of German Consumer Organisations (VZBV) sent a cease and de-

sist order to Valve and its distributor Vivendi, complaining about their insufficient DRM information policy. The term „Internet connection“ as a requirement is merely listed in the “other” category on retail boxes. The need for online activation is not clearly indicated. Because the EULA is only available in English and cannot be read before the purchase it raises the question, whether it is at all legally valid. However, Steam is still in use and controls 1.7 million customer accounts at its will with its DRM.

### Bottom line

DRM-based usage control systems can be abused to violate consumer rights. It is alarming to see how little consumers have reacted to this practice and that it has not negatively affected sales of the game. This could pose an incentive for other developers on the game market to use online usage control system to restrict consumers' rights. DRM's developments on the game market, therefore, have to be closely watched in the future.

### Sources

- ▶ GfK (2004): Piracy-Study 3. Gesellschaft für Kosumforschung, Nürnberg, Germany; [http://www.ffa.de/start/download.php?file=publikationen/brenner\\_studie3\\_en.pdf](http://www.ffa.de/start/download.php?file=publikationen/brenner_studie3_en.pdf)
- ▶ Grimmelmann, James (2004): Two Skirmishes in the DRM Wars: Half-Life 2 and Halo 2. Yale Law School's LawMemeEST, Nov. the 14<sup>th</sup>; <http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1647>
- ▶ Harris, Wil (2005): Is the Half-Life 2 EULA illegal? In: The Inquirer, 05-02-06; <http://www.theinquirer.net/?article=21105>
- ▶ Jeges, Ernő (2004): Turning infringing users into paying customers - A new trend in anti-piracy. INDICARE Monitor Vol. 1, No 6/7, 17 December 2004; [http://www.indicare.org/tiki-read\\_article.php?articleId=64](http://www.indicare.org/tiki-read_article.php?articleId=64)
- ▶ Jensen, Lars (2003): Das Spiel geht weiter. In: Brand Eins, No 4, Berlin, pp. 46 – 50
- ▶ Newitz, Annalee (2005): Dangerous Terms - A User's Guide to EULAs. The Electronic Frontier Foundation; <http://eff.org/wp/eula.php>
- ▶ Steam (2005): STEAM SUBSCRIBER AGREEMENT; [http://www.steampowered.com/index.php?area=subscriber\\_agreement](http://www.steampowered.com/index.php?area=subscriber_agreement)
- ▶ VUD (2005): Computerspiele als Wirtschaftsfaktor. Verband der Unterhaltungssoftware Deutschland e.V. Paderborn, Germany; <http://www.vud.de>
- ▶ Wikipedia: Half-Life 2: [http://en.wikipedia.org/wiki/Half-life\\_2](http://en.wikipedia.org/wiki/Half-life_2)
- ▶ Wikipedia: Steam: [http://en.wikipedia.org/wiki/Steam\\_%28content\\_delivery%29](http://en.wikipedia.org/wiki/Steam_%28content_delivery%29)
- ▶ Wirtz, Bernd (2003): Medien- und Internetmanagement. Wiesbaden, Germany

**About the author:** Danny Vogeley is an intern at Berlecon Research. He has been analysing several digital markets like Internet broadcasting, mobile music and M-Business strategies of media companies. Currently, he works in the field "digital consumer". He is a member of the INDICARE project team.

**Status:** first posted 10/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=85](http://www.indicare.org/tiki-read_article.php?articleId=85)

# How to implement copyright exceptions in DRM systems

## A proposal substantiated for the copyright exceptions in German law

By: Dominik Knopf, Institute of Information Law, Karlsruhe, Germany

**Abstract:** This article is based on a diploma thesis (Knopf 2004) in "information engineering and management", which has been submitted to Prof. Thomas Dreier at the University of Karlsruhe. Copyright exceptions and DRM systems (DRMs) normally do not interact very well. The approach presented in this article describes a way to achieve a win-win situation for both - consumers interested in copyright exceptions and content providers wishing to protect their content -, by implementing the exceptions demanded by law directly in the DRMs. Benefits are a higher level of trust and an extended global protection of the content, because the content never leaves the protection of the DRMs.

**Keywords:** technical analysis, copyright law, DRMS design, fair use, private copy, trust

### Introduction

Currently DRMs are yet unable to reconcile the conflict between rightsholders' interests and public access interests. They restrict use possibilities and thus curtail the freedom granted to users under exceptions to the exclusive rights of copyright holders. Not surprisingly, consumers have begun to develop distrust to any new invention regarding content and rights management.

So how can trust be regained? To begin with, consumers must be assured that their personal data are as safe as they would be in a normal store in the "real" world. Only very few consumers would supply information on how often and when they hear a piece of music. In addition, there is more personal and private information at stake, e.g. information about a handicap someone has. Next consumers will not accept a new system if they feel unnecessarily intruded, i.e. if they are limited to freely use content once they have bought it. Thirdly the ability of DRMs to override legal provision, in particular the exceptions granted, creates further distrust. Obviously there is no easy solution to implement DRMs fulfilling these consumer requirements.

The approach outlined here starts from a paradigm shift: from object-oriented DRMs to user-specific DRMs. It is proposed to link the content to the person, who acquired the rights to use the content, and not to the object the content is used with. Due to this switch in

perspective, the implementation of copyright exceptions becomes possible.

### The main elements of the approach

#### *Trusted third parties*

This approach is based on an infrastructure which includes a set of trusted third parties (TTP). These TTPs work as mediators between the consumers and the companies. Their tasks are:

- ▶ anonymization of the consumers' data
- ▶ bearing witness to the consumers' characteristics regarding copyright exceptions (e.g. "person A is a student")

To guarantee the TTPs' impartiality, TTPs should be state-run or they should be run by an independent commission. Exactly which TTP is chosen depends on the particular exception.

#### *Dongle for identification*

The second part of the infrastructure would be a safe way to identify the consumer sitting in front of the computer. A system which could work well would be a combination of a computer dongle as a physical component (e.g. an USB device with cryptographic capabilities) and a personal code to access the private key on the dongle. Every dongle is unique and can essentially not be copied.

#### *Technical Protection Measures (TPM) / watermarks*

It should be noted that watermarks – as a safe way for linking content to the consumer – are

also an essential part of the user specific DRMs. Watermarks fulfil an important function in this approach. It is assumed that watermarks can be integrated in every format the consumer wants to use, even in already existing standard data formats. Watermarks are the essential way to maintain the link between the consumer and the content he controls.

### How it could work for different kinds of exceptions

The concept outlined above will be demonstrated by the following three examples. The first of these examples describes its realization with respect to § 45a UrhG. This exception was introduced into the German Copyright Act in order to protect the access to information for handicapped people. The second example describes the implementation of § 52a UrhG which protects the access to content for scientific use and use in teaching. The third example is about the implementation of the much discussed private copy exception contained in § 53 UrhG. Ideally all examples described will become fully automated.

#### *Implementation of § 45 UrhG (exception for disabled people)*

For this scenario a public office should be chosen as TTP, which has already access to information regarding the degree and the kind of the handicap of the consumer. Consumers, who fall under this exception normally buy content and contact the TTP afterwards and supply a certificate of the content provider which proves that they bought the rights to use the content. The TTP verifies this certificate and asks the content owner for a copy of the content, which can be used by the consumer. The copy gets personalized to a new ID and is resent to the TTP, which also resends it to the consumer. The consumer can now use the content. In the case of a copyright infringement, the TTP has a connection between the new ID and the personal data of the consumer.

#### *Implementation of § 52a UrhG (exception for scientific use and the use in teaching)*

Other TTPs are universities and comparable institutions, which have access to information regarding students, teachers and lessons

held. Students are required to register for lectures at the TTP to minimize the efforts for the participants. The teacher giving the lecture registers all relevant content at the TTP. When a student needs access to content, he contacts the TTP, which then contacts the content owner. The procedure then follows the steps as set out with regard to the implementation of § 45 UrhG.

A second way of implementation is to add the watermark of the student – if he has one – to the watermarked version of the professor. This can be done by the DRM-application itself and there would be no need for a TTP. So, students presumably would not distribute their copy with their personal data in the watermark.

#### *Implementation of § 53 UrhG (exception regarding the private copy)*

This implementation of the private copying exception is a little bit more sophisticated. Before even implementing this exception, a preliminary question has to be asked: Why should this exception get implemented at all? Well, users have become accustomed to making copies of the copyrighted material they have bought or accessed for purposes of time and place shifting, for format change and also for archiving and security reasons. By implementing the private copy directly in the DRMs, a private copy continues to be possible for the consumers and is used more reasonably.

In general, consumers obtain the data protected by DRM over the internet or in a store. In the first case, in the model proposed, data gets marked with a personalized watermark at the moment of the sale. In the second case, data gets personalized when it is used for the first time. When a consumer would like to copy his data within the limits of the private copying exception, depending of the use of the data, the consumer uses his or her DRMs to generate a copy, which supports the intended use. For example, if the user wants to hear a song in a DRM-protected format on his MP3-player, his DRM-application converts the data, embeds a watermark and copies it on the MP3-players, tagging it in such a way that it can't get copied back. If the MP3-player already supports a proprietary DRMs,

the application should be able to convert the data to this format.

A way to use the internet in the last scenario could again involve a TTP, which requests a DRM-protected, newly watermarked copy of the content from the content owner. Consequently there is no need to change watermarks.

For the consumer, the private copy still exists, but in the case of copyright infringement, his name or ID is on the copy. This will limit the consumer's interest in distributing the content. But the consumer is still able to use his content like he was used to, when it wasn't DRM-protected.

### Discussion

As with all DRM-approaches, there are some advantages and some disadvantages. The most evident problem of the present proposal is the creation of the infrastructure. The implementation will only be affordable if there is a standard system which is usable for a broad variety of services. Most likely the infrastructure required has to make use of other infrastructures being build up, e.g. the infrastructure for the German health system relying on a health card (Gesundheitskarte) with cryptographic abilities. However, if a combined system can be violated, the damage would be much greater. Therefore a safeguard has to be available.

A second problem is the dongle. The dongle provides more security for the content owner and makes content mobile for the consumer, but it is also a cost factor. Moreover, the consumers' comfort is somewhat limited by a dongle. It may generate technical problems and consumers would have to attach it to the computer every time they want to use their data.

A third and minor problem is the fact that under the model proposed, the TTP gets information about consumers' access to the services of the content owner. Therefore it must be ensured that the TTP adheres to data protection and privacy policies.

Finally, there is a problem that all DRMs have in common: The system works only as long as cryptographic security (including

watermarks) can be warranted and if consumers use the system in a responsible way. But if, e.g. a dongle gets lost, this will be like losing a credit card. This, users will have to understand.

However, as already mentioned in the introduction, there are also some positive elements in this approach, which compensate for the negative ones.

First of all, because of the effort which the content owner undertakes with such a system, he demonstrates that he does not really want to limit the rights of the consumer any further than defined by statutory provisions. This brings at least some credibility back and should increase the trust on the part of the consumers. A certification of such a DRM system could further increase this effect. Also, consumers' personal data regarding handicaps or relationships between consumers remain safe at the TTPs. Finally the content owner can be sure that his content never leaves the protected circle even if private copying is allowed.

While it is doubtful, that the system will be implemented very soon due to the high cost factor, it may be an option in the near future, when an identification infrastructure exists. As more and more people, companies and public offices are relying on the new digital technologies, the cost of adding TTP-capabilities in an office or a commission will be reduced. It is also imaginable that future laws will *require* the implementation of copyright exceptions in DRMs as a prerequisite to the granting of legal protection.

While this approach has been discussed with respect to the German copyright exceptions, it is possible to use it with minor changes for other national transpositions of the European copyright directive too.

### Bottom line

Intellectual property entails rights and responsibilities. At the moment code tends to substitute law. Therefore, code – in this case code of DRMs – cannot stay uncontrolled. There will be a control instance, either by law or by self-regulation. The approach presented here can be a way to allow for a well-balanced technical regulation. The paradigm

shift proposed should help to represent the law more correctly, because the law in fact links rights to persons and not to objects. Any technology should enable consumers to enjoy their rights on whichever device they

like. DRMs are a great opportunity to solve the problem of intellectual property if it is used right. But it must work for both sides. Due to today's (dis)abilities of TPMs, the natural way of using the content is blocked.

### Sources

- ▶ German Copyright Act; <http://bundesrecht.juris.de/bundesrecht/urhg/>
- ▶ German "Gesundheitskarte" (health card); <http://www.bmgs.bund.de/deu/gra/themen/gesundheit/geskarte/index.cfm>
- ▶ Knopf, Dominik (2004): Diploma Thesis (unpublished): Durchsetzung rechtlich geschützter Zugangsinteressen durch nutzergruppenspezifisches Digital Rights Management (Enforcement of the legitimate interest for access via user group specific Digital Rights Management); <http://www.dknopf.de/papers/diploma%20thesis.pdf>

**About the author:** Dominik Knopf finished his studies in information engineering and management at the University of Karlsruhe by the end of 2004. Currently he is working with Prof. Thomas Dreier at the Institute of Information Law at the University of Karlsruhe, and is preparing his doctoral thesis.

**Status:** first posted 21/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=87](http://www.indicare.org/tiki-read_article.php?articleId=87)

## Comparing the EUCD implementation of various Member States

**Reviewed publication:** Urs Gasser and Michael Girsberger, *Transposing the copyright directive: Legal protection of technological measures in EU Member States*. Cambridge, MA: Berkman Center for Internet & Society Research Publication Series (no 2004-10), November 2004

By: Margreet Groenenboom, IViR, Amsterdam, The Netherlands

**Abstract:** The paper reviewed analyses how the EU Member States have implemented the anti-circumvention rules provided for in the European Copyright Directive (EUCD). It focuses on three main issues: (1) definitions, (2) the relationship between the protection of technological measures and exceptions to copyright as described in Article 6 of the EUCD, and (3) sanctions and remedies according to Article 8 of the EUCD. The review compiles the main findings of the excellent paper giving rise to only minor points of criticism.

**Keywords:** review, legal analysis, policy analysis, EUCD, content protection, EU

### Introduction

In November 2004 two affiliates of the Berkman Center for Internet & Society, Urs Gasser and Michael Girsberger, published a research paper on the transposition of the Articles on technological protection measures (TPM) of the European Copyright Directive (EUCD) by various European Union Member States (Member States). In particular it gives an overview of the current state of implementation of Article 6 (circumvention of TPM) and Article 8 (sanctions and remedies) EUCD. Countries that had already im-

plemented the EUCD in the last quarter of 2004 were: Austria, Denmark, Germany, Greece, Hungary, Ireland, Italy, Luxemburg, Malta, The Netherlands, Poland, Slovak Republic, Slovenia and the United Kingdom. The aim of the report is neither to describe every single country nor to come up with a critical assessment of all approaches taken, but to present a representative selection of interesting models and to take a critical look at the level of harmonization reached in the Member States.

The report consists of three parts: *Part one*, "how the Genie got in the bottle", describes the history of the EUCD and the current state of implementation of the EUCD. *Part two*, "Overview of Article 6 and Article 8 EUCD", describes the subject matters that the report investigates. *Part three*, "Country-specific analysis", describes the implementation of the EUCD per subject matter in several Member States.

In this review, the first two parts of the report are introduced briefly. As part three is the one where it all comes to a head, most attention is paid to this part.

### Part 1: How the Genie got in the bottle

The report goes back to the adoption of the WIPO Copyright Treaty (WCT) in 1996 and to the WIPO Performances and Phonograms Treaty (WPPT). Very relevantly, the report observes that already in the Articles 11 WCT and 18 WPPT, the provisions that deal with the circumvention of TPMs, do not define the terms "effective" and "technological measures". Was this the moment where it already went wrong? In my opinion the lack of definitions allowed for rather different approaches, the major ones being the DMCA (1998) and the EUCD (2001). This part also describes the current state of implementation of the EUCD. Since several countries still have not implemented the Directive and are thus still struggling with it, the report concludes saying that "the Genie is stuck in the bottle".

### Part 2: Overview of the Articles 6 and 8 EUCD

The second part forms the necessary basis for the country specific analysis in the third part. It describes the Articles 6 (TPM) and 8 (sanctions) of the EUCD focussing on (a) definitions, (b) the relationship between TPMs and exceptions to copyright law, and (c) sanctions & remedies.

(a) *Questioning the definitions of the EUCD*  
Article 6 EUCD protects TPM against circumvention and against the trafficking of circumvention devices and services.

When describing Article 6 (3) (the devices), attention is paid to the lack of an explicit

distinction between "access control" and "copy control" devices. Where Article 6 (3) mentions "through application of an access control or protection process such as encryption, scrambling" this leads according to the report to "the presumption that the EUCD does analytically distinguish between access and copy controls but – unlike the DMCA – grants equal treatment to both types of technology". The report mentions later (page 13) that §1201 of the DMCA makes this distinction. Indeed, the distinction between "*access control*" (measures that effectively control access to a copyrighted work) and "*copy control*" (measures that effectively protect a right of a copyright owner) is essential in the United States ( see DMCA § 1201; see also Reese 2003).

*Circumvention* ( § 1201 (a) (1) (A) DMCA ) as well as *trafficking* in circumvention devices ( § 1201 (a) (2) DMCA) is not allowed with regard to **access control mechanisms**. In this case, civil remedies and criminal provisions under § 1203 and § 1204 DMCA are possible. It is *not* forbidden to *circumvent copy controls*. *Trafficking* in circumvention devices with regard to copy controls is forbidden and is subject to the provisions § 1203 and § 1204 DMCA ( § 1201 (b) (A) DMCA). Although *circumvention* of copy controls is not forbidden, remedies are still possible for copyright owners. The *circumvention* of copy controls can still lead to liability for copyright infringement under § 501(a) DMCA because an unlawful reproduction or distribution might have taken place, but this depends on what is done by the circumventor after the circumvention.

(b) *Protection of technological measures and exceptions to copyright*

Member States have to take appropriate measures to make sure that it is possible for beneficiaries to benefit from the exceptions that are applicable to the exclusive right of the copyright owner (see also Helberger et al 2004, p.49). The report identifies two main categories of exceptions:

- Public policy exceptions (such as exceptions in relation to photocopying, copy and archive purposes of educational facilities). Although these exceptions are

mandatory, recital 51 EU CD states that appropriate measures should only be taken in absence of voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties.

- Private copying exception. In this case Member States may, but are not obliged to take measures to make sure that people are able to make a copy for private use.

The public policy exception as well as the private copying exception do not apply to on-demand services. On demand services are defined in article 6 (4) as "works made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them". What "appropriate measures" are or can include, is not specified by the EU CD.

(c) *Sanctions and remedies (Article 8 EU CD)*  
Important here, is that Member States are obliged to "provide appropriate sanctions and remedies", to "take all the measures necessary to ensure that those sanctions and remedies are applied" and "sanctions have to be effective, proportionate and dissuasive".

### Part 3: Country specific analysis

The report describes the implementations of the Articles 6 and 8 EU CD by several Member States. The three aspects introduced in the second part in a general way are used here again for the country comparison. The report convincingly shows the difference of national approaches when implementing the EU CD in Member States.

Unfortunately it is not clear what criteria were used to select the countries that are described per subject matter. Sometimes a country is mentioned only in relation to one aspect (Austria, Ireland, Hungary and Italy), sometimes to two (Greece and the Netherlands), and sometimes in relation to all three aspects (Germany, Denmark and the UK). In this review, only countries that have been described for that particular subject matter are mentioned.

(a) *Problems related to the definition of TPM*  
The report perfectly clarifies why definitions are very important. As an example, region coding of a DVD is used. In practice, two main approaches exist in the area of what acts the EU CD prohibits:

1. Only TPMs that prevent or restrain uses that are relevant under the copyright law and that would result in copyrights infringements are protected. This is called the *narrow interpretation*.

2. TPMs aimed at preventing or restricting any act are protected. This is the *broad interpretation*. In this scenario there is no connection with the acts that are relevant under copyright law. A connection is made with "the acts that are not authorized by the rightholder". Thus, the acts that are not authorized by the rightholder, are protected against circumvention.

Hungary and Denmark are examples for the *narrow* interpretation of the definition of TPM. The Danish Act is applicable to TPMs "that are designed to protect works from copying" and the act *excludes* mere access controls from the protection because access control technologies do not necessarily prevent an act that would constitute an infringement by copyright law. This approach is quite interesting because if a user circumvents a TPM solely to make use of a lawfully acquired work (for instance: breaking the region code of a lawfully acquired DVD to play it on the computer), this circumvention is allowed.

Other countries, like Germany, the UK, and the Netherlands, adopted the *broad* interpretation. Consequently, in these countries control mechanisms can be protected against circumvention even if the mechanisms are not designed to prevent exclusively acts that are relevant under copyright law.

(b) *TPM and exceptions to copyright, Article 6(4) EU CD*

With regard to the exceptions to copyright, there are major differences between Member States. I will have a look at the private copying exception, the public policy exception, what if voluntary measures fail and finally at the definition of "on demand services".

► Private copying exception?

The approach to the private copying exception is different among Member States. In Denmark private copying is not mentioned at all. In the UK the act expressively refers to "time-shifting" as the only private copying exception permitted and in Greece only reproduction for private use on paper or any similar medium is mentioned. In Italy it is possible to make one copy for personal use provided that a) the user has obtained legal access to the work and b) the act neither conflicts with the normal exploitation of the work nor unreasonably prejudices the legitimate interests of the rightholder.

► Public policy exceptions?

In Ireland and Greece, rightholders should make available means to beneficiaries to benefit from the exceptions. The Austrian and the Dutch approach is the wait and see strategy (using recital 51 EUCD) and therefore there are no exceptions to the anti-circumvention provision. In Austria a recently conducted survey shows that the voluntary measures taken by rightholders are in compliance with the EUCD (Bericht Bundesministerin für Justiz, 2004). Although there are problematic areas (i.e. access and copy protection technology on CDs and DVDs) no legislative measures have been announced.

► What if voluntary measures fail?

In case rightholders do not take voluntary measures or when the measures do not allow the use of an exemption in the eyes of the beneficiaries, it depends on the country which steps need to be taken by beneficiaries. Sometimes beneficiaries may apply directly to the Copyright License Tribunal (Denmark), High Court (Ireland) or Secretary of State (UK). In Denmark, when rightholders do not comply with the order within four weeks, beneficiaries may legally circumvent the TPM, as long as the consumer has gained legal access to the work. They don't need approval of the Tribunal or anyone else to do this. In other countries, like Greece, the solution is sought in mediation (with the possibility to go to Court of Appeal of Athens).

► On-demand service

What is noteworthy with regard to the exclusion of the "on demand services" from the applicability of Article 6 (4) par 1 and 2, is that the countries that implemented exceptions (Ireland, UK, Denmark and Greece), all use the exact sentence used in the EUCD to describe "on demand services" as "works made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them".

*(c) Sanctions and remedies, Article 8 EUCD*

The implementation of Article 8 is very diverse, in some countries huge criminal sanctions are possible (imprisonment or a fine of 2,900 – 15,000 Euro in Greece or 10,000 – 50,000 Euro in Germany), whilst in other countries there is no imprisonment and only a small fine (Denmark).

There is a difference in what acts can be subject to penalties. In the UK, there are no criminal sanctions for the circumvention of TPMs as long as it is conducted for private and non-commercial use. The UK also has a special Article in which is stated that the infringement that occurs in the course of business or "to an extent that prejudicially affects the rightholder" can be qualified as a criminal offence.

In Denmark, Greece and Germany, circumvention of TPMs as well as the trafficking in circumvention devices can be punished under civil and criminal law. Imprisonment for these acts in Denmark is not possible. In Greece imprisonment of at least one year is possible. Germany makes a distinction between the circumvention of TPMs (imprisonment up to one year or a fine) and the trafficking in circumvention devices (imprisonment up to three years in case of professional purposes or a fine). Remarkable is the fact that in Germany (similar to the UK) no criminal sanctions are applied in case the act has been exclusively performed for, or in relation, to private use by the offender or individuals personally connected with him.

### Conclusions of the report

The report ends with two concluding remarks. First of all, the report draws the con-

clusion that the Member States are still struggling "with some problems already identified at the level of the EUCD, such as the definition of TPMs, scope of protection and the interface to exceptions, and the question of effective , but also adequate sanctions and remedies". Most countries leave it to the national courts and the European Court of Justice to "fine tune the new legislation".

Secondly, the authors conclude that although the EUCD has led to a certain level of harmonization, significant differences remain. Also, it remains to be seen what the ramifications of these differences will be, for instance with regard to the further development of digital media markets, technological innovation, and the evolution of the "regulatory ecosystem".

### A bit of discussion

Overall the report gives a good idea of how different some implementations work out when they are applied to the examples mentioned in the report. The comparison between the DMCA and the EUCD regarding the distinction between access and copy control is interesting and certainly deserves more research and discussion in Europe.

One point of criticism; the report notes in the section about the private copy exception, that Italy "might stand alone in this issue" because some recent court rulings in France, Belgium and Germany all decided against a "right to private copying". Against this opinion, one could argue that although there may not exist a right that consumers can enforce as consumer in court, this does not mean that the private copying exception ceases to exist.

### Sources

- ▶ Gasser, Urs; Girsberger, Michael (2004): Transposing the copyright directive: Legal protection of technological measures in EU Member States. Cambridge, MA: Berkman Center for Internet & Society Research Publication Series (no 2004-10), November 2004, <http://cyber.law.harvard.edu/publications>
- ▶ Bundesministerin für Justiz, Bericht der Bundesministerin für Justiz im Einvernehmen mit dem Bundesministerium für soziale Sicherheit, Generationen und Konsumentenschutz an den Nationalrat betreffend die Nutzung freier Werknutzungen, July 1, 2004, available at [http://www.justiz.gv.at/\\_cms\\_upload/\\_docs/bericht\\_freie\\_werknutzung.pdf](http://www.justiz.gv.at/_cms_upload/_docs/bericht_freie_werknutzung.pdf)
- ▶ DMCA (1998): Digital Millennium Copyright Act of 28 October 1998; [http://www.eff.org/IP/DMCA/hr2281\\_dmca\\_law\\_19981020\\_pl105-304.html](http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html)
- ▶ EUCD (2001): European Copyright Directive, [http://europa.eu.int/information\\_society/topics/multi/digital\\_rights/doc/directive\\_copyright\\_en.pdf](http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf)
- ▶ Helberger et al (2004): Helberger, Natali (ed.); Dufft, Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer ac-

Unfortunately (besides the fact that the selection criteria for the countries chosen are not explained) the consequence of working with a selection of countries is that it is not possible to make an overall schedule of which countries use a narrow approach, and which countries use a broad approach, or to make any profound aggregation at all of the implementations of the articles 6 and 8 EUCD, because the selected countries for the subject matters vary. An overall view of the implementations would be helpful when assessing the implementations of the articles 6 and 8 EUCD in the Member States.

Lastly, the issue of region coding mentioned by the report is quite interesting. How can region coding be qualified and what are the consequences of the qualification in combination with the approach of a Member State with regard to the definitions of TPM in the EUCD, i.e. does a country use a broad or a narrow definition. At the moment, the difference in treatment regarding region coding in different Member States does not result in harmonization of "a European approach" at all.

### Bottom line

Overall, the report is very well written and easy to read for lawyers and non-lawyers. The report also draws an interesting picture of the implementation struggle and the diversity of implementation paths with respect to the focus chosen. Finally, it invites to further investigate the consequences of a narrow or a broad interpretation of what TPMs are protected by the EUCD.

ceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report. Amsterdam; available at <http://www.indicare.org/soareport>

- ▶ Reese R. Anthony (2003): Legal Incentives for adopting Digital Rights Management Systems: Merging access controls and rights controls; available at <https://www.law.berkeley.edu/institutes/bclt/drm/papers/reese-drm-btj2003.pdf>

**About the author:** Margreet Groenenboom is project researcher at the Institute for Information Law, University of Amsterdam. She specialises in copyright law, patent law and law & information technology. Contact: + 31 20 525 7382, [groenenboom@jur.uva.nl](mailto:groenenboom@jur.uva.nl)

**Status:** first posted 21/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=88](http://www.indicare.org/tiki-read_article.php?articleId=88)

## Better take a long tail look... Three remarks on the INDICARE state-of-the-art-report

By: Timo Ruikka, Nokia Corporation, Espoo, Finland

**Abstract:** The INDICARE report is regarded overall a good reading and highly useful. However three issues shall be highlighted where the author of this review disagrees with INDICARE and does propose a broader and longer term perspective of the changes we witness.

**Keywords:** review, INDICARE, business models, consumer expectations, innovation, privacy

### New business models and flexibility offered by DRM

I found the issue of new business models and flexibility offered by DRM to be incompletely articulated in the report. I personally believe that there can be HUGE value to users in getting something less (in usage rights) than what the content industry is afraid to distribute in wide circulation (that being the freely copiable personal copy like the CD disk is today). If it is a good deal, users can accept something less than permanent and something that is less than freely transferable. This does assume that prices also come down from the early trial phase that we are witnessing now. In fact, I expect the prices to go down so far that users will consume content like they consume electricity: without thinking how much a minute costs but turning it off when finished – like they turn off lights when they go out.

Also, the flexibility will be in the incredible selection (see on this the Wired magazine article by Chris Anderson 2004 "The Long Tail") and in the tailoring to changing needs and tastes: having a constantly updated top 100 songs in your pocket is flexibility even if

you cannot transfer any of those tracks to another device...

Now, if prices do not come down so far, then I trust the consumer advocates will make a big noise... .

### Consumer expectations that really matter

Consumers do not really need detailed transparency, they do not want to dread the small print of what consumption possibilities are offered when they buy content online. Instead, they need simplicity and predictability of stable, balanced, well defined typical consumption offerings. In my view, the "small print" and the detailed scope of the typical offerings should be negotiated by all stakeholders. The result should be as familiar as a train ticket: you do not read the fine print when you buy one. But you have a pretty clear idea about the main variables: monthly pass, 2nd class return, 2nd class one way. Or all-you-can-eat Eurailpass etc! You get the idea. Now 3,000 service providers are inventing the same packages in s-l-i-g-h-t-l-y different ways and it will drive consumers crazy.

### Against the myth that DRM is a privacy issue

Privacy is relevant for DRM-enabled services. But this concern is generic to all digital services, it is not DRM specific. The INDICARE paper has far too great emphasis on privacy aspects, as if DRM was a bigger threat to privacy than (for instance) eBay or electronic banking or credit card statements. The privacy aspect is whether a service accumulates personally identifiable information and how it handles that information. DRM per se does not generate PII (Personally Identifiable Information). Nor do DRM systems typically “track” users and what they do with the content – instead they just limit the functionality of content received by users. The main linkage DRM has to privacy is that it includes support for digital identities: Device

identity, domain identity (e.g. a home of several devices) and even personal identity (if a person's name is linked to a subscription ID like an Internet username and PIN). But similar identities are in use in almost all Internet services. So let's not continue the myth that DRM necessarily is a privacy issue. Some SERVICE models can be BIG privacy issues (like TiVo which collects viewing habits and begins to suggest similar programs; Amazon does this too). But these are based on non-DRM aspects of those services.

### Bottom line

Rethinking flexibility, transparency and privacy in a long term perspective would further improve the quality of the INDICARE State-of-the-Art-report.

### Sources

- ▶ Anderson, Chris: The Long Tail. Forget squeezing millions from a few megahits at the top of the charts. The future of entertainment is in the millions of niche markets at the shallow end of the bit-stream. Wired Magazine at [http://www.wired.com/wired/archive/12.10/tail\\_pr.html](http://www.wired.com/wired/archive/12.10/tail_pr.html)
- ▶ Helberger et al. (2004): Helberger Natali (ed.); Dufft Nicole; Gompel, Stef; Kerényi, Kristóf; Krings, Bettina; Lambers, Rik; Orwat, Carsten; Riehm, Ulrich: Digital rights management and consumer acceptability. A multi-disciplinary discussion of consumer concerns and expectations. State-of-the-art report, Amsterdam, December 2004; <http://www.indicare.org/soareport>

**About the author:** Timo Ruikka is Vice President, Industry Initiatives at Nokia's technology Platforms unit. Contact: [timo.ruikka@nokia.com](mailto:timo.ruikka@nokia.com)

**Status:** first posted 07/03/05; licensed under Creative Commons

**URL:** [http://www.indicare.org/tiki-read\\_article.php?articleId=83](http://www.indicare.org/tiki-read_article.php?articleId=83)

## Masthead

The INDICARE Monitor is an electronic periodical of the EU-funded project INDICARE being published every last Friday of a month. Articles having passed an internal review process are immediately posted at the INDICARE homepage for public debate. Authors are encouraged to revise their articles in the light of previous discussion before publication in the monthly issue.

- ▶ You can use the *RSS-feed* to get articles as soon as they are posted.
- ▶ You can *subscribe* to the INDICARE Monitor, and receive an *e-mail notification* containing the contents page (title, author, abstract, and URLs) and a link to the pdf-version (this service replaces the bi-weekly INDICARE newsletter). Just type in your e-mail address at the INDICARE Website and Go!, or send an empty e-mail to: [indicare-monitor-subscribe@indicare.org](mailto:indicare-monitor-subscribe@indicare.org)
- ▶ The *INDICARE Monitor Archive* offering all issues in HTM and PDF is available at <http://www.indicare.org/tiki-page.php?pageName=IndicareMonitor>
- ▶ The *INDICARE Homepage*: <http://www.indicare.org/>

**Editorial Team:** The Editorial Team currently consists of Knud Böhle, Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe, Germany (Editor); Michael Rader, also from ITAS (Copy-Editor); Nicole Dufft, Berlecon Research GmbH, Berlin, Germany (Co-Editor business); Natali Helberger, Institute for Information Law, Amsterdam, The Netherlands (Co-Editor legal), and Kristóf Kerényi, SEARCH Laboratory of Budapest University of Technology and Economics (Co-Editor technology).

**Editorial policy:** The INDICARE Monitor is an English language periodical publishing original works. The editorial policy attempts to be balanced, unbiased, neutral, and non-partisan, not excluding however provocative, pointing and sometimes even lopsiding contributions. Articles are written by INDICARE staff and external experts. The style is intended to be analytical, concise, compact, and written in a language comprehensible for non-experts. The expected length of an article is between 5000 and 10.000 characters. The INDICARE Monitor is available for free.

**Copyright:** All original works of the INDICARE Monitor unless otherwise noted are copyright protected and licensed under a Creative Commons License allowing others to copy, distribute, and display articles of the INDICARE Monitor a) if the author is credited, b) for non-commercial purposes only, and c) not with respect to derivative works based upon the original article.

**Disclaimer:** The views and opinions expressed in the articles of INDICARE Monitor do not necessarily reflect those of the European Commission and the INDICARE consortium or partners thereof. All articles are regarded as personal statements of the authors and do not necessarily reflect those of the organisation they work for.

**Acknowledgment:** The INDICARE Monitor is an activity of the INDICARE project, which is financially supported as an Accompanying Measure under the [eContent Programme](#) of [Directorate General Information Society](#) of the European Commission (Reference: EDC - 53042 INDICARE /28609).

### Contact

Knud Böhle (Editor)  
Institute for Technology Assessment and Systems Analysis (ITAS)  
Phone: +49 (0)7247/82-2989 (-2501)  
Fax : +49 (0)7247/82-4806  
E-Mail: [knud.boehle@itas.fzk.de](mailto:knud.boehle@itas.fzk.de)

