The KnowRight Conferences, held since 1995, intend to resume the general interest of the Knowledge Rights, on the interaction of Intellectual Property Rights, related Information Rights, and information dependent technology. KnowRight provides strong emphasis on the social environment in which the intellectual and information property system, information services, mobile applications, e-commerce and the electronic civil society evolve.

This book gives an excellent overview on the current crisis of copyright in the emerging knowledge society. On the one hand, rights of copyright holders have been strengthened on demands of copyright industries. On the other hand, growing unease with copyright has lead to a countermovement providing alternative models like Creative Commons licenses. Human rights are endangered by data retention and on-line searching, restricting privacy and opening new enforcement options for knowledge business. Proper balancing of these interests requires intensive discussion. KnowRight08 constitutes a creative dialogue between academics, and representatives of business and the civil society.

Main topics of this book:
- New developments in the protection of Knowledge Rights in Europe
- Human rights, constitutional law & Knowledge Rights (e.g. new German fundamental right to the integrity and confidentiality of IT-systems)
- Knowledge Rights, competition law and standard setting (e.g. standards and competition policy)
- Open source & Knowledge Rights (e.g. Creative Commons license)
- Enforcement of Knowledge Rights (e.g. disputes on the Internet, use of patents and utility models)
- Database protection, digital heritage and open access to information (e.g. database protection and access to public sector information, longterm preservation of digital heritage, e-government and information)
- Data protection & Knowledge Rights (e.g. strong contrast with interests in free access to information and moves to strengthen enforcement)
- Future of copyright (e.g. re-user right, private coping and format shifting)

This volume helps to participate successfully in the debate about the future options concerning the creation, distribution and use of knowledge in the information society.

ISBN 978-3-85403-245-8
KnowRight 2008

Knowledge Rights –
Legal, Societal and Related Technological Aspects
Gedruckt mit Förderung des Bundesministeriums für Wissenschaft und Forschung in Wien.

Wissenschaftliches Redaktionskomitee

o.Univ.Prof.Dr.G.Chroust
o.Univ.Prof.Dr.G.Haring
Univ.Prof.Dr.G.Kotsis
Univ.Doz.Dr.V.Risak
o.Univ.Prof.Dr.P.Zinterhof
Jens Gaster, Erich Schweighofer and Peter Sint (eds.)

KnowRight 2008

Knowledge Rights –
Legal, Societal and Related Technological Aspects

© Österreichische Computer Gesellschaft 2008
The KnowRight Conferences, held since 1995, intend to resume the general interest of the KnowRight, on the interaction of Intellectual Property Rights, related Information Rights, and information dependent technology. KnowRight provides strong emphasis on the social environment in which the intellectual and information property system, information services, mobile applications, e-commerce and the electronic civil society evolve.

This 5th Symposium on the Interaction of Informational Rights, Information Technology and Knowledge Management takes place in Krakow, a town with a rich history, former capital of Poland and the first university town north of the Alps.

This time, KnowRight is organised by the Austrian Computer Society (Oesterreichische Computer Gesellschaft OCG) jointly with the Intellectual Property Law Institute of the Jagiellonian University in Krakow, the German Society for Informatics (Gesellschaft für Informatik GI) and the German Society for Law and Informatics (Deutsche Gesellschaft für Recht und Informatik DGRI).

Focus of this year conference is the future of knowledge rights in the information society. These subjects will be discussed in a creative dialog between academics and representatives of business and the civil society. All the papers going beyond an abstract are refereed papers.

The conference addresses in particular the following topics concerning Knowledge Rights (KR):

- KR, competition law and standard setting
- Open source & KR
- Data protection & KR
- Human rights & KR
- Enforcement of KR
- Database protection, digital heritage & open access to information
- Future of copyright
- New Commission package on intellectual property

Many persons worked to form the conference and to prepare the programme and the proceedings. Special recognition has to go to the work of the Program Committee. Further, the work of the Intellectual Property Law Institute of the Jagiellonian University Krakow and the Centre for Computers and Law of Vienna University deserves acknowledgement. Last but not least, the financial support of the Business Software Alliance (BSA), the OCG Austrian Computing Society and the DGRI German Society for Law and Informatics should be gratefully acknowledged.

Vienna, in August 2008

Jens Gaster, Erich Schweighofer, Peter Paul Sint
PROGRAM COMMITTEE

(co-chairs bold)
Jon Bing, University of Oslo, NO
Daniele Bourcier, University of Paris II, FR
Alfred Büllesbach, University of Bremen, DE
Joseph A. Cannataci, University of Central Lancashire, UK
Estelle Derclaye, University of Nottingham, UK
Séverine Dusollier, CRID, University of Namur, BE
Michal du Vall, Intellectual Property Law Institute, Jagiellonian University, PL
Local Chair)
Gunter Ertl, Regional Court of Appeal, AT
Fernando Galindo, University of Zaragoza, ES
Jens Gaster, European Commission, EU
Co-ordinator)
Lucie Guibault, University of Amsterdam, NL
Thomas Hoeren, University of Münster, DE
Philip Leith, Queen's University Belfast, UK
Thomas Riis, Copenhagen Business School, DK
Rimantes Petrauskas, Mykolo Romerio University, LT
Ahti Saarenpää, University of Lapland, FI
Peter P. Sint, OCG, AT
Erich Schweighofer, University of Vienna, OCG & Vienna Center for Computers and Law, AT
Co-ordinator)
Sybilla Stanislawska-Kloc, Intellectual Property Law Institute, Jagiellonian University, PL
Local Organisation)
Alain Strowel, Facultés Saint-Louis-Bruxelles, BE
Peter Wahlgren, University of Stockholm, SE
Andreas Wiebe, Vienna University of Economics and Business Administration, AT
# TABLE OF CONTENTS

## Keynote lectures

*Jens Gaster*
New Developments in the Protection of Knowledge Rights in Europe

*Andreas Wiebe*
The way ahead for knowledge rights?

## Human rights, constitutional law and Knowledge Rights

*Agata Dimmich*
Copyright as a Human Right under the European Convention on Human Rights

*Andreas Wiebe*
Constitutional Protection in the Information Age

*Christian Czychowski, Jan Nordemann*
Use of retained data and intellectual property rights – Balancing act between data protection, telecommunication and copyright law

## Knowledge Rights, competition law & standard setting

*Grażyna Piesiewicz*
Competition and IP issues in standard setting

*Benoît Müller*
Standards Policy

*Dariusz Kasprzycki*
The abuse of dominant position in context of the refusal to license

*Hans-Werner Moritz*
The EU Microsoft Case and its Impact on High Tech Businesses Possessing IPRs

## Open source & Knowledge Rights

*Lucie Guibault*
Creative Commons: Struggling to ‘keep it simple’

*Yann Dietrich*
LiMo Foundation: How to benefit from openness while being inclusive of all licensing models in the mobile world?

*Maciej Barczewski*
European Union Public License - Key Problems and Challenges for the Future
Benoît Müller
Open Source Software Policy  

**Enforcement of Knowledge Rights**

*Michal Koščík*
IP infringement in internet - a tort or a crime?  

*Justyna Ożegalska-Trybalska*
Resolving IP disputes on the Internet – is a court litigation the only option?  

*Georg Jakob, Hartmut Pilch*
On the grammar of patent claims  

*Knut Wimberger*
Unfair competition caused by bad faith utility model registration  

*Benjamin Henrion*
Software patents: software authors lost their rights  

*Richard Schlötter*
Patent Policy  

**Database protection, digital heritage & open access to information**

*Estelle Derclaye*
Does the Directive on the Re-use of Public Sector Information affect the State’s database *sui generis* right?  

*Erich Schweighofer, Andreas Rauber*
Digital heritage & copyright  

*Ahti Saarenpää*
Information Government and Legal Information  

**Data protection and Knowledge Rights**

*Judith Rauhofer*
Is all gossip created equal? - Privacy, reputation and harmful speech on the internet  

*Radim Polčák*
The Global Information Assembling: Viewing the Data Retention Just as a Child Play  

*Mikołaj Sowinski*
The Processing of Traffic Data in the Privacy Debate  

*Ricardo Cristof Remmert-Fontes*
Data retention: the hunt for "copyright infringers" is raping freedom
Future of copyright

Robin Elizabeth Herr
Should a new re-user right be created in copyright law and how can it be operationalized?

Dinusha Mendis
A Private Affair in the UK: Copyright Law in Transition - Private Copying and Format Shifting Exceptions

Index of authors
NEW DEVELOPMENTS IN THE PROTECTION OF KNOWLEDGE RIGHTS IN EUROPE

Jens Gaster¹

Extended abstract

The topics of KnowRight 2008 cover a broad range of basic issues affecting knowledge rights in the 21st century. Such issues involve, inter alia, the inherent conflict between the exercise of intellectual property rights (IPRs) and competition law, which requires further discussion in the wake of the ECJ's Microsoft case and the ongoing European Commission pharmaceutical sector inquiry, both concerning alleged abuses of IPRs to the detriment of competitors and consumers. The antitrust / IP interface is also at issue in complaints alleging unlawful monopolisation of the market for computer memory technologies incorporated into industry standards such as in the Rambus case.

Whilst it is thus obvious that IPRs and knowledge rights per se require an appropriate balancing with public policy considerations we must bear in mind that copyright is a human right since the French revolution, protected by a number of international covenants and national constitutions. Moreover, industrial property rights such as patents and trademarks are governed by international arrangements including the Paris Convention of 1883 or more recently the TRIPs Agreement of 1994. There is thus a need for taking full account of the specific nature of IPRs addressed in the relevant international instruments as well as in pertinent EU legislation, apart from considering the diverging interests of the 27 EU Member States, various stakeholder organisations, users, consumers and civil society groups. Whilst this statement holds in particular true as regards the situation de lege lata this does not exclude to embark upon a lively debate about ongoing reforms and ex post evaluations of the corpus iuris.

Apart from the creation (at EU level) and correct implementation (at Member State level) of legislation affecting knowledge rights in Europe there is a need for a homogenous application of such laws on the ground. Specific concerns in this area are the spreading phenomenon of IP piracy in the digital age and the large scale distribution of counterfeit goods, involving organised crime. Other perceived threats involve growing levels of computer crime. IP related crime has major repercussions not only economically and socially, but also in terms of consumer protection, public health and safety. Civil law enforcement of EU and national IP legislation has been addressed by Directive 2004/48/EC² and most Member States have at last complied with their implementation requirements. By contrast the draft penal law IP enforcement Directive remains still controversial. In particular whether and to what extent it is necessary to penalise patent infringements still requires further reflection.

¹ Dr. iur., European Commission, DG Internal Market and Financial Services, Industrial Property unit, Brussels. The views expressed in this contribution are solely those of the author and do not commit the institution to which he belongs.

The pending Anti-Counterfeiting Agreement (ACTA) to be concluded at the international level has also sparked a lot of frequently polemic debate. Whilst most interested parties agree upon the need for providing appropriate deterrents curtailing IP related crime there are still divergent views whether it is required to provide for pre-established damages, unlimited pre-trial discovery, punitive damages or presumptions for determining the award of damages. From the EU perspective a (draft) Council Resolution on a comprehensive European anti-counterfeiting plan\(^3\) is intended to address the issue at the Community level.

Further to the failure in 2005 of the proposed EU Directive on computer implemented inventions\(^4\) (CIIs) interested circles are still lively debating so-called software patents and business method patents. Whilst the EU Commissioner in charge of this issue has rejected requests for new proposals harmonising patentability criteria for CIIs some lobbies suggest excluding patentability in this area whereas others propose consolidating the practice of patent authorities of granting CII patents by codifying and harmonising the different EU national patent laws, whereas still others prefer to maintain the status quo. Open source software policy remains thus an open and very controversial issue but will for the foreseeable future not be addressed by European law makers.

In relation to the issue of *sui generis* protection of databases versus open access to information the dust has somewhat settled since the ECJ ruling in the case of *British Horseracing Board v William Hill\(^5\)*. The Court had actually ruled that the cost and effort related to the generating of data does not constitute substantial investment required for giving right to database right. As regards the interface between the legal protection of databases under Directive 96/9/EC\(^6\) and the re-use of public sector information under Directive 2003/98/EC\(^7\) interesting cases concerning the re-use of databases generated by public authorities have recently been brought before the ECJ. We are thus likely to learn later this year whether the copyright exemption for public sector works may be extended *mutatis mutandis* to the protection of non-creative databases.

Turning to data protection and knowledge rights due account should be paid to Directive 2002/58/EC on privacy and electronic communications\(^8\). The Directive concerns the processing of personal data and the protection of privacy in the electronic communications sector. In this context data protection, e-privacy, secrecy of communications and the freedom of expression on the internet are frequently challenged on grounds of counter-terrorism and criminal law enforcement. Recent measures imposed by the U.S. Ministry for Homeland Security described as "electronic strip search" of foreign travellers’ mobile phones and laptops by U.S. border police have added to a hot debate concerning these issues also in Europe.

Since knowledge rights also concern the promotion and protection of innovation recently intensified work on patent reforms should also be mentioned. Since 2000 the EU institutions are attempting to make progress on a comprehensive reform of the European patent system. The main deficiencies of the current system are the prohibitive costs for EU-wide patent protection requiring translations into all EU languages and the lack of an appropriate system for (cross-border) patent litigation. In August 2000 the Commission submitted a proposal for a Council Regulation with the aim of

\(^{3}\) Council document 12370/08.
\(^{5}\) Case C-203/02, ECR 2004, p. I-10415.
\(^{7}\) OJ No. L 345, 31 December 2003, p. 90.
creating a Community patent ("COMPAT"). A COMPAT would have a unitary character and the same effect throughout the EU. Litigation would take place before a single specialised Community patent jurisdiction. The European Patent Office would grant Community patents. The Council reached a common political approach on COMPAT on 3 March 2003\(^9\) but discussions mainly on the effects of translations of patent claims have blocked final adoption of the Community patent Regulation.

In parallel, the European Patent Organisation (EPO) has begun reform aimed at tackling shortcomings of the current European patent system based upon the European Patent Convention (EPC). For a number of years EPO working parties on translation requirements and litigation have been preparing side agreements to the EPC. This work lead to the London Agreement on translation costs being signed in 2000 and to a draft European Patent Litigation Agreement (EPLA) which would have created a new international organisation, the European Patent Judiciary, to provide for a unified litigation system on infringement and validity of European patents involving a limited number of like-minded Member States. EPLA finally failed as a result of insufficient political support and concerns related to its compliance with the EU’s legal order.

The difficulties in making progress in the field of patent reforms led the Commission to launch, in January 2006, a broad consultation on the future patent system in Europe. Responses have shown that industry favours the introduction of a COMPAT and the improvement of the existing European patent system. However, the Common political approach of the Council in 2003 on COMPAT was strongly criticised in relation to translation requirements (where translations of the patent claims are required into all EU languages) and the jurisdictional system.

As a follow-up to the consultation, the Commission adopted a Communication titled "Enhancing the patent system in Europe" on 3 April 2007\(^{10}\). This Communication was intended to draw operational conclusions from the 2006 stakeholder consultation and to allow the Council to launch deliberations on patent reforms, in particular jurisdictional arrangements. It set out three options: (1) the EPLA approach, (2) the creation of a Community jurisdictional system for both European and future Community patents (like the French model above), and (3) an integrated approach involving elements from options (1) and (2) (see "a possible compromise" above). Moreover it suggested a fresh look at the Council's 3 March 2003 political approach on the translation arrangements for COMPAT and proposed the consideration of various "flanking measures".

Since mid 2007 the patent reform file has re-gained considerable momentum. On the patent litigation system, a model has been developed for a jurisdictional system covering both European and future Community Patents. There is broad agreement on the overall structure. The proposed jurisdiction would involve at first instance decentralised divisions in Member States working in the local language to ensure proximity to the parties, and one central division working in the languages of the patent. Uniform rules of procedure on basic substantive law would ensure consistency of jurisprudence. Judgments would have EU-wide effect. Appeals would be dealt with by a central appeal instance. Judgments given on appeal could be reviewed by the ECJ in order to with ensure the uniformity of the Community legal order. Although some detail remains to be sorted out, there seems to be broad consensus among Member States concerning the main features and architecture of the system. The required legal basis for the new jurisdiction is likely to be created by a treaty - a

---

\(^9\) Council document 7159/03, 7 March 2003, Community patent - Common political approach.

\(^{10}\) COM (2007) 165 final.
mixed agreement between the Community and Member States - that would be open for accession to third countries which are parties to the EPC.

On the Community Patent, the EU's Council Working Party has also discussed the two main unresolved issues on the Community Patent: translation arrangements and the distribution of revenue from maintenance (or renewal) fees for the patent. On translation arrangements, it has been proposed to provide for machine translation of patents performed by a central service. This would provide a Community patent that avoids the high costs and complexity currently resulting from translations for the users, but would also improve access to patent information by users in all Community languages. The translation system would make use of work already in progress in automated technical translation by the EPO which would have to be further developed and extended. Automated translations would be for information purposes only and have no legal effect. This approach has been welcomed by industry, especially associations representing SMEs. EU Member States are also broadly supportive of this idea.

Member States also seem to accept the principle of 50% of income from COMPAT renewal fees being distributed between national patent offices and on the basic criteria for distribution, but need to agree on detailed criteria.

Progress made so far gives reason for hopes for a political agreement on a package including the patent jurisdiction and the Community patent in the course of 2009. This would require a high-level political compromise considering some sensitive issues to be sorted out, in particular, the language regime.

On 16 July 2008 the European Commission adopted three initiatives described as "forward-looking package". This package involves two initiatives in the field of copyright and a communication concerning industrial property. All three are expected to spark a lively debate on IP reforms and strategies.

As to the two initiatives in the area of copyright, first, the Commission proposes to align the copyright term for performers with that applicable to authors. Secondly, the Commission proposes to fully harmonise the copyright term that applies to co-written musical compositions\(^{11}\). In parallel, the Commission also adopted a Green Paper on Copyright in the Knowledge Economy\(^{12}\). The consultation document focuses on topics that appear relevant for the development of a modern economy, driven by the rapid dissemination of knowledge and information.

The proposal on term extension envisages extending the term of protection for recorded performances and the record itself from 50 to 95 years. In this way, the proposal would benefit both the performer and the record producer.

In its review of the Single Market\(^{13}\) the Commission highlighted the need to promote free movement of knowledge and innovation as the "Fifth freedom" in the single market. The Green Paper will now focus on how research, science and educational materials are disseminated to the public and whether knowledge is circulating freely in the internal market. The consultation


document will also look at the issue of whether the current copyright framework is sufficiently robust to protect knowledge products and whether authors and publishers are sufficiently encouraged to create and disseminate electronic versions of these products.

With the Green Paper, the European Commission plans to have a structured debate on the long-term future of copyright policy in the knowledge intensive areas. In particular, the Green Paper is an attempt to structure the copyright debate as it relates to scientific publishing, the digital preservation of Europe's cultural heritage, orphan works, consumer access to protected works and the special needs for the disabled to participate in the information society.

The Communication on a new industrial property rights strategy for Europe\textsuperscript{14} outlines a number of actions as the keystone to maintain a high quality industrial property rights system for the EU in the 21st century. It sets out to support inventors in making informed choices on the protection of their industrial property rights and calls for robust enforcement against counterfeiting and piracy. The Communication also aims to ensure that industrial property rights in Europe are of high quality and that they are accessible to all innovators, particularly small- and medium-sized enterprises (SMEs).

Along with the urgent adoption of the Community patent proposal and creation of an integrated EU-wide jurisdiction for patents, the actions proposed by the Communication are intended to ensure Europe has a high quality industrial property rights system in the years to come. Apart from issues related to the effective enforcement on the ground against counterfeiting and piracy, the commissioning of studies on the quality of the patent system and on the overall functioning of the trademark systems in the EU, a particular focus of the Communication is on facilitating exploitation by SMEs of industrial property rights. The Communication outlines measures to facilitate access to industrial property rights and dispute resolution procedures, and to improve awareness among SMEs of the management of industrial property as an integral element within an overall business plan.

\textsuperscript{14} COM (2008) 465 final.
THE WAY AHEAD FOR KNOWLEDGE RIGHTS?

Andreas Wiebe

Abstract

Many developments cumulated to produce the current crisis of copyright: the developing information and knowledge society, the growing importance of copyright industries, digitisation and the advent of the internet. Legislators adapted to the new technical systems of distribution of works and strengthened the protection of copyright holders. In addition, technical means of protection granted rightholders an even more effective and unlimited scope of protection. On a fundamental level this cast doubt on the principal of intellectual property. Open Source, open access and creative commons are symptoms of this countermovement purporting to provide alternative models hinging on ideas of cooperation and participation.

Hence, the first question to be addressed is the basic one whether intellectual property is still a valid concept against a background of digitised networks. From an economic point of view the internet economy shows some special features, esp. the presence of network effects. However, while empirical research in the field of copyright in general shows no conclusive answer it appears that intellectual property is a valid concept in the network economy as well which can be demonstrated even by looking at the open source model. It may turn out that different areas of knowledge production and dissemination may need different regimes. Open access and creative commons may be the appropriate model in the field of research and education. On the other side, use of DRM shows that regulation should not be left to the contractual level but copyright is needed to provide a balance of interests. Moreover, the failure of DRM systems teaches a lesson consumer acceptance is an important parameter in the market place.

The second basic question turns to how copyright should be framed to live up to its objectives of creating incentives, providing access and contributing to enriching the cultural and knowledge sphere. Legislative models are being discussed putting more emphasis on access of the user and consumer, e.g., within the A2K initiative. This is not only relevant on a national level but on a global scale with respect to developing communities. However, more fundamental changes should be discussed. With traditional copyright being intertwined with the medium of distribution courts still struggle to find what may constitute a “copy” in the digital environment. This is not only true on the internet but also in more traditional areas like software protection. Modern software metrics relating to diversified criteria are hard to accommodate to existing copyright systems (“software as service”).

While legal practice tries to cope with this problem in a pragmatic way in the long run new models of copyright are needed. One suggestion to adapt to the shift from conventional carriers to digital transmission is to switch from the control of copies to the definition of usage rights. This could on the one hand turn out to be more appropriate considering the developing forms of usage of works in a digital environment. On the other hand it would allow for new ways of implementing a new balance of interests by defining these rights and their limitations.

1 Prof. Dr. Andreas Wiebe, LL.M., Information Law and Intellectual Property Law Group, Vienna University of Economics and Business Administration, www.infolaw.at.
Another long time problem of copyright may be alleviated by the spread of information networks and the accompanying decline of intermediaries: the protection of the authors. Empirical evidence shows that most authors only get a very small share of the revenues of copyright industries putting the incentive function as to creative work into question. This may change with the internet where intermediaries disappear giving way to new business models. However web 2.0 creates new problems of enforcement as well as acceptance of copyright. In this respect a renewed copyright may be supplemented by self regulatory regimes. The recent agreement on principles for user generated content between industry and internet service providers may serve as an example for a new regulatory mix. All in all the future will look more diverse while more emphasis will be put on a fair balance of interests.
COPYRIGHT AS A HUMAN RIGHT UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Agata Dimmich¹

Abstract
The article examines the possibilities of understanding copyright as a human right under the European Convention on Human Rights. Firstly, Article 1 of Protocol No. 1 guaranteeing peaceful enjoyment of possessions is considered. It is argued that this provision does not account for the distinction between economic and moral rights of authors. Secondly, Article 10 of the Convention guaranteeing freedom of expression is considered. As under this provision not only the substance of ideas and information is protected but also the form in which they are conveyed, the possibility of understanding this provision as guaranteeing the protection of moral rights of authors who contribute to the public debate is examined.

1. Introduction

In an information-based economy intellectual property is regarded as a central asset. Therefore, it is of great importance to consider also the ethical and human-rights dimensions of intellectual property regimes. Moreover, a recent crisis of legitimacy that the copyright (and intellectual property in general) is going through has to be taken into account². Consequently, a human-rights approach to intellectual property cannot be limited to regarding intellectual property rights and human rights solely as two sets of distinct rights, whose interaction can be identified as either a conflict or a consensus. Rather there is a need to examine whether there are indications in human rights instruments that allow us to define copyright as a human right, and whether this applies to all aspects of copyright in the same way.³ Regarding intellectual property rights through the lens of human rights instruments may also help us realize which values shall be at the center of the process of shaping modern intellectual property law. It may help us realize that this process shall be shaped not only by the supposedly conflicting interests of holders of copyright and users of copyrighted works but also by the collective good of flourishing public sphere.

The Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) and the case-law of the European Court of Human Rights (“the Court”) may not be an obvious choice for such scholarly investigations, as the Convention, contrary to some other international human rights instruments (such as the Universal Declaration of Human Rights⁴ and the

¹ University of Wroclaw, PL.
⁴ Article 27 of the Universal Declaration of Human Rights: "(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author."
International Covenant on Economic, Social and Cultural Rights\(^5\) contains no provision explicitly guaranteeing the right to copyright (or more generally - the right to intellectual property). However, according to the Court’s well established case-law, Article 1 of Protocol No. 1\(^6\) guaranteeing the right to property (or more accurately: the right to the peaceful enjoyment of one’s possessions) is applicable to intellectual property (and to copyright) as well\(^7\).

What is more, the role of the Court as a quasi-constitutional pan-European court has to be taken into account\(^8\), particularly in the context of harmonization of copyright law in the European Union\(^9\). The harmonization of copyright law in the European Union and the growing body of Directives obviously constitute a significant context for the judicial decisions of the European Court of Human Rights, as one of the circumstances the Court carefully assesses is the degree of consensus or dissonance in the laws of the Convention's member states. However, it should also be noted that the bigger the consensus and the lesser the “margin of appreciation” the member states are afforded, the bigger is the need for such a harmonization to be accompanied by a counterpart of common European understanding of copyright as a human right.

2. Copyright as a subject of the right to property under Article 1 of Protocol No. 1 to the Convention

Although the case-law concerning the violations of copyright under Article 1 of Protocol No. 1 is surprisingly scarce\(^10\) and the Convention institutions have been called upon to rule on questions of intellectual property only very rarely, some of the key issues may already be identified.\(^11\) Firstly, the reasons for including intellectual property (and copyright) among possessions should be considered. According to the interpretation of the Court intellectual property rights can quite reasonably be regarded as an essential element of an economic activity.\(^12\) Moreover, they have two characteristics

\(^5\) Article 15 of the International Covenant on Economic, Social and Cultural Rights: „1. The States Parties to the present Covenant recognize the right of everyone: (a) To take part in cultural life; (b) To enjoy the benefits of scientific progress and its applications; (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author. 2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture. 3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity. 4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields.”

\(^6\) Article 1 of the Protocol No. 1 to the Convention: “Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.”

\(^7\) Decision of the European Court of Human Rights 05 July 2005, Application no. 28743/03, Melnychuk v. Ukraine.


– exclusiveness and transferability – which are also hallmarks of property, and this clearly shows that they are possessions. This is the reasoning that the Commission applied in its admissibility decision in the case Smith Kline & French Laboratories Ltd. v. the Netherlands. As this first intellectual property decision under Article 1 of Protocol No. 1 concerned patents, the Commission stated that since under Dutch law the patents are deemed personal property which is transferable and assignable, they fall within the scope of the possessions.

The Court referred to this decision in its subsequent case law, treating other intellectual property rights (trademarks, copyright) analogically and drawing from the fact that the concept of “possessions” under Article 1 of Protocol No. 1 has an autonomous meaning which is not limited to ownership of physical goods and is independent from the formal classifications in domestic laws. Consequently, certain other rights and interests constituting assets can also be regarded as “property rights”, and thus as “possessions” for the purposes of this provision. The Court's conclusion is that Article 1 of Protocol No. 1 is applicable to intellectual property as such.

This essentially economic understanding of the subject of the protection afforded by Article 1 of Protocol No. 1 is of particular importance in the light of recognition (both in the international intellectual property law and in domestic law of numerous European countries) of moral rights of authors. It is argued that moral rights have a stronger claim to protection as human rights than the copyright's economic exploitation rights, as they protect the personal link between the creator and his or her intellectual creations. However, moral rights of creators have not been addressed yet by the Court and, as a recent case of Balan v. Moldova has demonstrated, they may even be unaddressable under Article 1 of Protocol No. 1. This case concerned the violation of both moral and economic rights of the applicant. The photographs taken by the applicant were unlawfully used by Moldovan authorities as a background for the identity cards. According to the applicant domestic courts failed to recognize this infringement of his rights and did not award him compensation.

Interestingly enough, the moral rights of the applicant were addressed by the Court only indirectly – since the applicant alleged that his rights under Article 1 of Protocol No. 1 had been infringed as a result of the refusal of the domestic courts to compensate him for the unlawful use of his work. Consequently, although the Court referred in its reasoning to the aforementioned distinction between economic and moral rights of creators (stating that according to domestic law the author’s moral rights can never be transmitted to third persons), this characteristics of moral rights of the applicant was used by the Court only to reinforce the argument that there was an interference with the applicant’s rights, rather than to consider whether national authorities deserved less deference since they restricted creator’s moral rights as well.

3. Copyright and freedom of expression under Article 10 of the Convention

3.1. The concept

It is argued that since moral rights refer to the author and the personal link between him or her and the creation, a fundamental right basis for them should be construed from the right to privacy

---

15 L. R. Helfer, supra note 10, at 18.
guaranteed by Article 8 of the Convention. However, it might be particularly fruitful to consider the freedom of expression protected under Article 10 of the Convention not only as conflicting with the protection of the human right to copyright, but also as potentially coinciding with the protection of copyright. This approach may seem as a somewhat reverse application of the conception that both copyright law and freedom of expression may be viewed as concerned with the same fundamental question: defining the scope of private monopoly power that gives authors a sufficient incentive to create while ensuring that the consuming public has adequate access to the fruits of these efforts. However, the lack of provision explicitly guaranteeing the protection of the moral rights of authors in the Convention enables us to examine an entirely different problem as well: what is the relation between the freedom of expression and copyright in today's society of consumers who are not only users but are also increasingly becoming creators of content and play a more active and collaborative role in content creation and knowledge dissemination.

Paradoxically, the lack of provision explicitly guaranteeing the protection of moral rights of creators may thus be viewed as providing a framework for conceptualizing an alternative to the dominant private property paradigm of copyright. Instead of the market balance of information availability and the incentive to create, the potential of the public to become critical and creative participants in the production of their information environment is accentuated. If these newly discovered public of creators and participants in the public debate were to invoke moral rights of authors (especially the right to integrity of the work understood under the Berne Convention as the right to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the work, which would be prejudicial to the author’s honor or reputation) under Article 10 of the Convention, what would be the requirements for the protection to be afforded?

Firstly, freedom of artistic expression should be considered, as according to the Court’s well established case-law those who create, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions which is essential for a democratic society. Consequently, artistic

---

17 Article 8 of the Convention: “1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”


19 Article 10 of the Convention: “Everyone has the right to freedom of expression. this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”


freedom goes very far, as protection is extended to the dissemination of the creation.\(^{23}\) Secondly, the Court's interpretation of the right of the public to be properly informed as a corollary of the freedom of the media and a manifestation of the public interest behind the freedom of expression shall be taken into account.

### 3.2. The interpretation

According to the Court's jurisprudence, Article 10 protects not only the *substance* of ideas and information but also the *form* in which they are conveyed. In the case *Jersild v. Denmark\(^{24}\)* the Court stated that news reporting based on interviews, whether edited or not, constitutes one of the most important means whereby the press is able to play its vital role of "public watchdog". The Court recognized that the methods of objective and balanced reporting may vary considerably, depending among other things on the media in question concluding that it is not for the Court, nor for the national courts, to substitute their own views for those of the press as to what technique of reporting should be adopted by journalists. This line of reasoning was applied by the Court in multiple cases regarding the prohibition of publication of pictures of persons suspected of committing a crime, for example in a recent case *Verlagsgruppe News GmbH v. Austria\(^{25}\).* The applicant - the publisher of a weekly magazine - was prohibited from accompanying a report on pending investigations of tax evasion with a picture of the person suspected of committing this crime. Consequently, as the case was not concerned with a restriction on the *contents* of reporting but with the prohibition to accompany a report with a *picture* of the person concerned, the Court found that the public interest to have the information on the proceedings for tax evasion pending against the suspected accompanied by his picture had to be weighed against the interest of this person to have his identity protected. The Court's conclusion was that there is very little scope for an absolute prohibition to publish a public person’s picture in an article contributing to the public debate.

In the case *Vereinigung Bildender Künstler v. Austria\(^{26}\)* a similar problem was examined by the Court in relation to the freedom of artistic expression. The applicant, the association of artists with its seat in Vienna, was prohibited from exhibiting and publishing a painting showing a collage of various public figures in sexual positions after one of the depicted persons instituted proceedings on the ground that such a publication of his picture had violated his legitimate interest. However, when examining the necessity of this inference with the applicant’s right to freedom of expression the Court emphasized that the painting obviously did not aim to reflect or even to suggest reality and such a portrayal amounted to a caricature of the persons concerned using satirical elements. The Court noted that satire is a form of artistic expression and social commentary and, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. Accordingly, any interference with the artist’s right to such expression must be examined with particular care.

However, it is worth noting that in its reasoning the Court emphasized the fact that interference complained of was aimed only at the protection of *the rights of the individual* (and not public

---


morals – which are considered a matter of wide margin of appreciation). Consequently in this judgment the recognition of a specific characteristic of artistic expression coincides with the aim of restriction on this expression: protection of the individual rights of others, which is particularly significant in the context of commodification of information. In that context it is also important to note that, since the real and effective exercise of freedom of expression does not depend simply on the duty of the state to refrain from any interference but may require positive protective measures, the right to freedom of expression applies horizontally in the relationships between individuals as well.27

The aforementioned judgments in cases Jersild v. Denmark28 and Verlagsgruppe News GmbH v. Austria29 both emphasize the contribution to the public debate and the right of the public to be properly informed about matters of public interest, which may help reestablish the forgotten link between the author and his rights and the society. Also in the case Vereinigung Bildender Künstler v. Austria30 the Court found that satire is a form of artistic expression and social commentary, by its inherent features of exaggeration and distortion of reality aiming to provoke and agitate, clearly referring to the understanding of the character of freedom of expression as one of the essential foundations of a democratic society introduced in the judgment in the case Handyside v. the United Kingdom31. In this famous judgment the Court stated that freedom of expression is applicable not only to information or ideas that are favourably received or regarded as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness, without which there is no democratic society.

4. Conclusion

Consequently, Article 10 of the Convention may be regarded as potentially guaranteeing the protection of moral rights of authors (or rather – certain attributes of these rights) particularly under certain circumstances – when the works in question contribute to the public debate. Moreover, as the social reality of information society combines commodification of information with further blurring of the term “author”, the notion of the contribution to the public debate may appear to be quite fruitful both for the discussion on freedom to create understood as freedom to override this commodification of information and moral rights understood as protecting the personal link between the creator and his creation.

This aspect of fundamental rights protection of copyright has to be put together with other fundamental rights aspects (such as the protection afforded by the the provision of Article 1 of Protocol No. 1 to the Convention) to achieve the overall protection of copyright as a fundamental right.32 However, as these separate aspects of fundamental rights protection represent different interests, the protection they afford may both overlap and enter into conflict with one another. Therefore, instead of a simple adding up, a balancing of these different fundamental rights will be required.

28 Supra note 23.
29 Supra note 24.
30 Supra note 25.
31 Judgment of the European Court of Human Rights 7 December 1976, Application no. 5493/72, Handyside v. the United Kingdom.
32 P.L.C. Torremans, supra note 3.
5. References


CONSTITUTIONAL PROTECTION IN THE
INFORMATION AGE –

The invention of a new Fundamental Right to the Integrity and Confidentiality of Information Technology Systems by the German Constitutional Court

Andreas Wiebe¹

Abstract
A very recent Decision of the German Federal Constitutional Court from February 2008 sheds light on the constitutional side of the intersection of law and technology. 25 years after its landmark “Census” decision promulgating the fundamental right to information self-determination the Court “invented” a new fundamental right to the integrity and confidentiality of IT systems. On the background of rapid technological development and especially the rising of the internet as a new medium of communication the Court consistently expanded its line of constitutional protection to fill the gap that has arisen. This decision further opens the gap to the restrictive stance of the U.S. Supreme Court on the constitutional foundation of privacy while at the same time providing some comparative insights into the interpretation of the Constitution in the information age.

Overview

1. Background: Data Protection in Europe
   1. Warren/Brandeis and technological developments
   2. Three phases of legislation
      a) 1st phase – mainframes
      b) 2nd phase – integrated information systems
      c) 3rd phase – transborder data flow, European harmonization, and the internet
   3. Alternatives to legal regulation
2. The new Constitutional Court decision in context
   1. Preceding Constitutional Court decisions
   2. Key elements of the Decision
      a) Background
      b) New dangers
      c) Existing fundamental rights protection
      d) Contours of the new fundamental right to the confidentiality and integrity of IT systems
      e) First evaluation
   3. Ramifications
3. A comparative view to the U.S.

1 Austrian Visiting Professor, Stanford Law School, Professor for Information Law and Intellectual Property Law, Vienna University of Economics and Business Administration (www.infolaw.at).
1. Background: Data Protection in Europe

1.1. Warren/Brandeis and technological developments

The history of data protection law in Europe can be perceived as a reaction to technological developments. It started off in the beginning of the 1970’s. However, the dangers it sought to remedy were being perceived much earlier. Warren and Brandeis wrote in their famous article from 1890: “Instantaneous photographs and newspaper enterprises have invaded the sacred precinct of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’”.

Photography came up and made it possible to take pictures against a person’s will. While earlier you had to sit still for a portrait, the law of contract or trust might have provided protection against the improper circulation of the portrait. Now, an absolute right was needed and found in the extension of the right to privacy to the personal appearance, and the personal relation.

Warren and Brandeis regarded the changing structure of publicity as well as the appearance of new technologies as the basis for the need for a right to privacy. Already at that time it was regarded as part of a general personality right. Going beyond the notion of protecting proprietary rights, the protection of the individual and his autonomy was acknowledged.

George Orwell’s 1984 also shows an early awareness of the dangers inherent in new technological means. But only in the 1960’s technology caught up with his utopia. Before that surveillance technology was expensive and not very sophisticated. You had to type and file the documents. The East German Stasi employed 500,000 people as informers, and 10,000 were needed to listen and transcribe phone calls of citizens.

In this sense there were natural barriers to fast and comprehensive processing of personal data. When these barriers eroded with the advent and use of computer technology in the 1960’s it was time for the law to step in.

1.2. Three phases of legislation

a) 1st phase - mainframes

The development of data protection law can be distinguished into three phases. In the sixties was the time when large mainframe computers were used by large companies and administrations, still very expensive and with a very limited processing capacity judged by today’s standards. It was considered efficient to store data in one place for several organisations and to use identifier codes when connecting data bases. Data controllers were mostly state administrations having to cope with the requirements of social administration. The first generation of data protection laws was directed mostly at technology and institutionally limited the state’s power in the sense of “informational

---


division of power”. Their objective was to create transparency and characterized by the use of general clauses. An obligation to register data bases with personal data was established. Some individual rights were granted.

b) 2nd phase – integrated information systems

The second generation of data protection laws in the 1980’s was sparked by the “Census” Decision of the German Constitutional Court in 1983, a landmark decision with worldwide ramifications. It also involved more sector specific regulation. The general personality right is guaranteed in Art. 2 para. 1 of the German Constitution (“Grundgesetz”) and was seen as core by the framers of the German Constitution considering the experiences of the Nazi era. Art. 2 Grundgesetz serves as a kind of “mother right” from which specific constitutional guarantees can be derived.

This happened when the Court established the fundamental right of informational self-determination in the Census decision. It acknowledged the authority of the individual to decide himself when and within what limits information about his private life should be communicated to others and to what extent. The principle of self-determination deserved increased protection due to technological developments in the form of automated data processing. Especially integrating different data bases provided the opportunity to create a complete picture of the individual without his informed consent. This systems aspect of IT poses a threat to the individual self-determination but also to democracy. If you are not sure if your attitudes, actions are recorded and permanently stored you will not stand out with your behavior or you will abandon practicing your basic rights.

The right to informational self-determination is not without limitations. But to invoke them there has to be a compelling public interest and limitations in legislation need to be explicit. Data management has to relate to the purpose of collection and data has to be deleted once the objective is fulfilled. The Court also strengthened the role of data protection commissioners.

This decision had a severe impact on data protection laws in Germany as well as in several other countries. Legislation put emphasis now on ensuring individual rights with respect to the whole processing of personal data. It included rights of correction and deletion of data. Legislation was more sector specific. With its emphasis on individual enforcement it also became less technology specific.

c) 3rd phase – transborder data flow, European harmonization, and the internet

The third generation of data protection laws is characterized by the need to adapt to the EU Directive of 1995 while at the same time looking for answers to the crisis caused by the spread of digital networks with respect to conventional data protection concepts. The need for transnational data flows had become very pressing. Differing national rules required international harmonization on a level that would not excessively impede transborder data flow. Steps in the international field include the OECD Guidelines of 1980 and the Council of Europe Convention of 1981.

As it became clear that the Convention would not work towards harmonization in Europe with special resistance by the U.K., the EU Directive was adopted in 1995 to create a unified level of

---

protection and ensure the free flow of data in the single market. The Directive established individual rights, principles for lawful processing of personal data, obligates the data controller to notify the supervisory authority and establishes the concept of “adequate level” of protection with respect to transfer to third countries. The Directive had a huge global impact and the safe harbor concept was very influential on business practice in the U.S.

While the Census Decision gave data protection a big boost it also gave way to legislation legitimizing the status of data processing and providing a legal basis for it. This formalization often had a contrary effect. On the other hand, it proved to be a “toothless paper tiger”. This can be seen with the core concept of informed consent which is not effective against data controllers with a superior economic position. For the consumer it was not even effective as a bargaining chip to achieve a higher price in negotiations. Market oriented solutions suffer from the information problem that data subjects are not aware of the uses their data is being made of, and often are voluntary only in a formal sense when the data subject in fact has no choice if he wants to enjoy a service.

The crisis of data protection was enhanced by the spread of personal computers and the development of the internet that changed the environment of data protection completely as compared to the old world of centralized data banks. Adding to the information problems it became increasingly difficult to enforce data protection rules based on the concept of a data controller. Rules that require a registration of the data controllers seem completely outdated in this environment. As an example it suffices to mention that servers keep a logfile on the content and time of files downloaded on a user’s computer. Specialized companies increasingly collect this kind of data on the net and sell it for individualized advertising purposes. Should these logfiles be registered with data protection authorities by server operators? It is no surprise that the view is prevailing that data protection has actually disappeared.

3rd generation data protection laws have tried to find different answers to the technological challenges. New institutions like data protection audits are discussed. The German Data Protection law for Teleservices Data Protection Act (TDDSG) of 1997 introduced the basic principle that technological tools used by telecommunications service providers should be framed as to use as little personal data as possible already in the process of its construction. The General Data Protection Law was amended to include this principle of data economy. Europe followed suit with the Data Protection Directive for Electronic Communications Services of 2002 replacing Directive 97/66/EC. The Directive establishes the basic principle that Member States must ensure the confidentiality of communications made over a public electronic communications network (Art. 5). They must prohibit listening, tapping and storage of communications by persons other than users without the consent of the users concerned. Traffic data relating to subscribers and users processed and stored by the provider of a relevant service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication (Art. 6). Traffic data

---

necessary for the purposes of subscriber billing and interconnection payments may be processed, but such processing is allowed only up to the end of the period during which the bill may lawfully be challenged or payment pursued. Location data other than traffic data relating to users or subscribers of relevant services may only be processed in anonymous form, or with the consent of the users. Another issues raised by electronic commerce is the data protection implications of small programs that are installed on the user’s computer to collect and transmit data related to the transaction (“cookies”). The Directive confers upon users the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. Users must also be provided with clear and precise information on the purposes of cookies.

1.3. Alternatives to legal regulation

Increasingly the use of technologies is being discussed as a solution to the conceptual and enforcement problems of data protection law. It will provide the data subject with tools to protect his interests by himself. These include methods of encryption and other instruments of Privacy Enhancing Technology (PET) like P3P. But at best these tools can only be a supplement to legal protection, not a substitution. They are not widely applied and face technological problems. Although their use may contribute to enhancing the preconditions of individual choice they cannot abolish the basic problems of informed consent.

Another supplementary regulatory mechanism is self-regulation. In Europe, is it not perceived as a method to avoid state regulation but more like an additional measure taking account of the specifics of certain sectors and providing best practices. However, self-regulation has serious limitations as well. E.g., the system TRUSTe is based on the use of a certification mark. The sanction for unlawful data protection practices is withdrawal of the right to use the mark. However, no user actually will miss the mark.

In light of the deficiencies of technology and self-regulation the need for state regulation persists. Schwartz sees a default rule of prohibiting the use of personal data as a basis for creating a market with “privacy price discrimination”. Others propose similar solutions of creating real choices for the consumer basically resulting in a higher price for a higher degree of privacy. Still, the question remains, whether market solutions work efficiently at least within certain limits.

2. The new Constitutional Court decision in context

2.1. Preceding Constitutional Court decisions

The new Constitutional Court decision has to be viewed in the context of the preceding case law. In 1969, the Court distinguished three spheres of personality with different level of protection: a social sphere with information on the open social interaction with other persons; a private sphere concerning the private life that is usually not accessible to the public; a personal sphere relating to the private life as well, but to confidential and secret information. The personal sphere was held to be almost absolutely protected.

10 An example is BBBOnline: http//www.bbbonline.com.
11 Schwartz (n. 7) p. 79.
12 Schwartz (n. 7) p. 81 et.seq.
14 See Nehf, 78 Wash. L. Rev. 1, 61 et seq. (2003), listing factors why market failures are too great.
In the Census Decision of 1983\textsuperscript{16} went beyond the scaled protection relating to the different spheres but acknowledged a general right to control the flow of information relating to his person. In light of the technological means of data processing the Court argued that there are no more inconsequential data which renders the distinction of different spheres moot in this respect. The new fundamental right of informational self-determination was derived from the general right of protection of personality under Art. 2 of the German Constitution in connection with the protection of human dignity under Art. 1 of the Constitution. It includes the right of the individual to decide when and under which conditions personal information is disclosed and used. However, it does not create a property interest or exclusive control in the data. It rather aims at protecting the communication that is necessary for a person to develop a personality within a social community. It is an obligation of the state to organise data processing in a way that respects this personal autonomy; “Inconsistent with the right of informational self-determination would be a societal order and assisting legal order in which the citizen no longer knew the who, what, when and how of knowledge about him”.\textsuperscript{17} So he must have knowledge about who will use his data and to what purpose. This requires organisational and procedural regulations for the processing of personal data by the state as well as private industry. Also independent monitoring by data protection commissioners is part of the framework.

The new fundamental right is not granted unconditionally but countervailing public interests are weighed under a proportionality test and within this test it is of relevance which sphere is touched upon by the measure. Legislation limiting the new fundamental right must have a clear legislative basis, include clear norms and comply with the principle of proportionality.

The contours of privacy protection were further specified in a 2004 decision\textsuperscript{18} where the Court identified a core area of the private conduct of life that may not be encroached upon even in superseding interests of the public. This core area is absolutely protected and includes the possibility to express interior feelings and highly personal thoughts and experiences without fear of state surveillance.

2.2. Key elements of the Decision

a) Background
25 years have passed since the Census decision and technology has developed with the advent of the internet being the most visible innovation. The Federal Constitutional Court decision of 27 February 2008\textsuperscript{19} is an effort by the Court to provide constitutional guarantees appropriate to the new environment.

Subject of the decision was a December 2006 amendment to the law about the domestic intelligence service of the federal state of North-Rhine Westfalia allowing state surveillance of private computers. As this is done by placing a Trojan horse on the person’s computer it was also discussed as a law about “Federal trojans”. Journalists and lawyers had challenged the constitutionality of the amendment. The amendment had introduced a right for the intelligence service to “covertly observe and otherwise reconnoitre the Internet, especially the covert participation in its communication

\textsuperscript{16} BVerfGE 65, 1 (1983) - Volkszählungsurteil.
\textsuperscript{17} Id. at 42-43.
\textsuperscript{18} BVerfGE 109, 279 – Großer Lauschangriff.
devices and the search for these, as well as the clandestine access to information-technological systems among others by technical means" (paragraph 5, number 11). Parts of the challenges also addressed other amendments which are not covered here.

b) New dangers
Let me elaborate on the reasoning of the Court in detail. At the core of the decision is the development of a new fundamental right to the Integrity and Confidentiality of Information Technology Systems. The Court identifies a gap in protection that was caused mainly by the spread of personal computers that have gained an enormous importance for the development of personality in the information age. The Court stresses three major factors that effectuate new dangers for the right of personality:

On today’s PC’s there are a lot of data with relation to personal life with some of them automatically created without intentionally being stored by the user. Access by third parties to this data may allow for far reaching conclusions about the personality of the user and may be used to create personality profiles.

In interconnected systems these dangers are deepened in different respects. The enhanced usage leads to even more data being created and stored. This includes data relating to content as well as to the communication procedure.

Interconnection of systems allows third parties technical access to the data to spy out and to manipulate it. The user is often not aware of this third party access. Information systems have acquired such a high degree of complexity that the average user is not able to effectively protect himself on a social or technical level. Technical protection may also gravely impede the working of the system or be inefficient.

c) Existing fundamental rights protection
These enhanced dangers for personality are not completely accounted for by pre-existing fundamental rights. The Court reviews the existing fundamental rights and their limits and finds that they cover only part of the need for fundamental rights protection. These fundamental rights are specifically:

Telecommunications secrecy (Art. 10 I of the German Constitution “Grundgesetz”)
Inviolability of the home (Art. 13 I Grundgesetz)
General personality right (Art. 2, 1 Grundgesetz), especially
Right to informational self-determination

The guarantee of telecommunications secrecy protects the immaterial transmission of information to individual recipients by way of telecommunications. It relates to the content as well as to the question of whether, when, and how often communication has taken place. As far as data is collected to these matters regardless of whether on the transmission phase or at an end device this constitutional right is pertinent. However, it is directed only at the specific dangers inherent in the ongoing distant communication and does not extend to data stored in the sphere of a participant after conclusion of the communication. It also does not cover the case that a state agency surveys the use of the systems itself or searches the storage media even if telecommunications connections are used to transmit the collected data to the agency. The secret placing of a Trojan horse by far exceeds the dangers to be covered by the telecommunications secrecy. This action would allow for collecting data on a broad scale, ranging from the use of internet services to the steering of household appliances which also have some meaning as to the user’s behaviour.
The guarantee of the inviolability of the home is intended to secure a private space of living to develop a person’s private life. It is related to the physical space of private homes or business premises and dependent on the modalities of the intrusion. It covers not only physical trespassing but also means of surveillance not directly perceivable by the citizen such as acoustic or optical surveillance or the measuring of electromagnetic radiation. It also covers entering of a home to manipulate information systems physically. In addition, the infiltration of such a system is covered, e.g., if an end user device is used as a microphone or camera. However, there must be a relation to the physical sphere. Hence, using a computer network for infiltration purposes does not touch upon the right against interference with home because it is not related to the physical space in which the computer is located. This is especially obvious in cases of laptops, PDA, or cell phones. Also, the collection of data from storage media in a home enabled by the infiltration is not covered by the guarantee.

The general personality right ramifies to several specifications. One relates to the protection of a private sphere and would cover the collection of data relating to that private sphere. However, connecting data to that private sphere is not always easily done as it depends on the context in which it was created or put. Even data not clearly relating to the private sphere in the outset may be used to create personality profiles.

Another specification of the general personality right is the right to informational self-determination already elaborated upon. It extends beyond the private sphere and already is invoked in the forefront of the stage where concrete danger to protected legal interests can be identified, especially in the case of a collection of personal data. It is not confined to sensitive data, either. However, even the contours of this guarantee do not completely cover the dangers arising out of new technological developments. Today everybody is forced to use IT systems which inevitably produce personal data. The Court hints to the case that a third party accesses the system and has a great amount of data at hand without having to resort to additional measures of data collection and processing. The Court points out that this access and the accompanying inherent dangers to personality by far exceed the dangers inherent in single data collections targeted by the right of informational self-determination. This is the central argument why the Court regards the right of informational self-determination as not being sufficient to cope with new technological realities. The dangers are aggravated by the breadth of the measures; it may also affect the communication partners as third parties without the preconditions of surveillance being present as to them. In addition, the long-term character of surveillance, the overcoming of self-protection measures, as well as its secrecy contribute to the specific dangers inherent. The integrity of the target computer may also be encroached upon by damage to the stored data or the spread of security gaps.

d) Contours of the new fundamental right to the confidentiality and integrity of IT systems
The gap resulting from the review of the pertinent fundamental rights as applied to the realities of the information age is defined by the Court as: protecting the personal and private sphere of life not only against access to single communications or stored data but also against accessing the whole information system and the enhanced dangers resulting from it. The threshold level is surmounted if personal data can be collected in an amount and variety to allow for a view on substantial part of the conduct of life of a person or even to create an extensive picture of the personality. The Court cites access to a PC as the standard case where data even about professional use may be taken to draw conclusions on personal traits. The Court also mentions cell phones and electronic calendars that today store personal data in various ways.

The new fundamental right is derived from the general guarantee of personality rights by way of interpretation and judicial development of the constitution. It is supplementary in the sense that it
only covers the gap left by the pre-existing fundamental rights. Its protection works in two
directions. First, the confidentiality of data created, collected, processed, and stored by an
information system if the amount and variety of data collection and processing is not covered by the
right to informational self-determination. Second, it protects the integrity of such systems. The
fundamental right is encroached upon if the system can be accessed by third parties in a way that
they can use the data. This is enough to allow for them to spy out, survey, or manipulate the system.
Special focus is on covert access to spy out data in the temporary as well as the permanent storage.
It also includes keylogging as a more indirect spying measure. The constitutional protection is not
dependant upon the ease of difficulty of accessing the system.

The guarantee is not an unlimited one but subject to limitations. The decision establishes very strict
hurdles for limiting this basic right. There has to be a statutory basis providing for clear and specific
exceptions. It has to live up to the principle of proportionality. This requires a legitimate objective
as well as that the means used are suitable, necessary and appropriate with respect to this
objective. This also includes a weighing of the opposing interests. The gravity of the encroachment
results in the requirement that a paramount public interest has to be present to warrant it. The Court
provides a short list including life, personal integrity and freedom, and the foundations of the state
or of institutions essential for the existence of humans. It does not require, however, a sufficient
probability that the danger will materialize in the near future. But there must be "factual indications
for a concrete danger" in a specific case. Government agencies may use secret infiltration only after
approval by a judge. Online searches can therefore not be used for normal criminal investigations or
general surveillance.

Even if these rare conditions are met, the Court prescribes further procedural safeguards to protect a
core area of private life that is absolutely protected. This core area of the private conduct of life
includes communication and information about inner feelings or deep relationships. There has to be
a two-step procedure to protect this core area. First, the statute has to provide for technical measures
that aim as far as possible at avoiding the collection of data from this core area. However, from a
practical point of view it is unavoidable that data from this core area may be accidentally collected.
The requirement then is that data collected has to be screened for the presence of core area data and
this has to be deleted immediately and can not be used or forwarded in any case.

What is outside the scope? The government agency is free to search the web, public mailing lists or
an open chat. Information that is publicly accessible can be obtained without encroachment on the
right of informational self-determination or the right to the confidentiality and integrity of IT
systems. The agency may even take part in internet communication with a hidden identity. Also, no
violation is in place if one of the participants of a communications provides access for the agency
under his access data. There is generally no warranted personal trust in the identity of the
communication partner even if this communication goes on for some time and “electronic
communities” are established. Each communication partner is aware that he does not know the
identity of his partner and cannot verify it. No protected trust can be derived from that. In this
respect fundamental protection also is resorting to a reasonable expectations test.

e) First evaluation
If you look at the essence of the decision it is the establishment of a fundamental right to
information security. What does IT security or data/information security have to do with data
protection? Data security has always been an integral part of data protection. Art. 17 of the EU
Directive on Data Protection 1995 also included data security principles.\textsuperscript{20} Both concepts are intertwined: Integrity is essential to preserve confidentiality. Hence, the two parts of the new fundamental right do not stand separately from each other but mutually draw upon each other.

However, one is wondering as the confidentiality of information was already covered by the right to informational self-determination what’s really new? What the Court emphasizes is the systems aspect. The decision provides the bridge between the systems security and constitutional protection of the user. The unauthorised access by third parties alone already poses serious threats to the personality interests of the user without any data collection having taken place. Hence, the security of IT systems achieves legal significance not only as part of a broader data protection concept but is being lifted by the Court to become a fundamental right of the user has the right to unhampered development of her/his personality in the information age.

In contrast the second new element relating to the confidentiality could as well have been covered by the already existing right to informational self-determination. However, while the Court is not really clear on the delineation it seems to be the enhanced possibilities of data collection, interconnection of systems and user profiling that far exceed what the right to informational self-determination as well as data protection laws had envisioned as their factual basis. Considering this it seems in the interest of legal clarity for the Court to put this aspect under the new fundamental right which makes it easier to establish strict procedural rules.

In resume while “traditional” data protection laws are still struggling with the crisis caused by digital networks the Constitutional Court went ahead and did the necessary step on the constitutional level. The intention is also to spark off the necessary adaptations on the legislative and judicial level.

\textbf{2.3. Ramifications}

So what will be the consequences of this decision? The new fundamental right is at first a right of the citizen as against measures by the government. However, the institutional side of fundamental rights under German constitutional law demands active protection by the state. This is especially true in light of the emphasis the Court put on the fact that the citizen is not sufficiently capable to protect himself effectively. It will be seen in the future development of the new fundamental right in which areas and to what extent an active duty of the state to protect the integrity of information systems may be derived. Already there are calls to adapt the existing laws relating to information security to the new realities of technology, stressing the European preference for legal requirements to technology.\textsuperscript{21}

In German constitutional doctrine the fundamental rights as written down in the Constitution establish an “objective order of values” having effect on all parts of the law and especially civil law

\begin{itemize}
\item \textsuperscript{20} See also Recital 46: “Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;
\end{itemize}
with general clauses being a main gateway. The effects on the construction of civil law is at least of equal practical significance than those in public law. All parts of law related to information security will be affected. E.g., product liability or the liability of service providers and the resulting duties are concerned. A software producer or service provider that opens up a security gap may be liable even if this happens only negligently.

A civil law area where the use of information systems has been subject to controversy has been the employer-employee-relationship. The controversy centers around the extent to which the employer is allowed to survey the use of email as well as the WWW by the employee. The European Court of Human Rights has found a violation of Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedom and demanded a statutory basis and a proper notice to the employee. National law in Europe is divergent on this question but leans towards prohibiting the surveillance. With enhanced protection especially in the confidentiality aspect it may become an established default rule in labor law as well as in data protection law now that such surveillance is not permitted. Whether a strict prohibition on the private use of such systems by the employer may exclude the effects of the new fundamental right is at least doubtful considering the fact that even inadvertent private communication may not be avoided, e.g., receiving an email from a friend. Moreover, it is not always easy to distinguish professional from private content.

More far-reaching it may be necessary to review existing laws whether the protection they grant is consistent with the high requirements of the new fundamental right and the emphasis on systems security. Many activities on the internet touch upon data protection laws while the discussion about the extent and limits of its application is just beginning. Search engines are now coming into the focus of data protection authorities in Europe, with effects also on U.S. companies. One example may be the practice of internet services to collect user data by placing cookies on the user’s computer. From this data user profiles can be derived. These data are then sold for purposes of personalised advertising and behavioral targeting. This practice was also raised as legally problematic in the merger proceedings of Google and DoubleClick but was not taken into consideration in Europe as well as in the U.S. It seems clear that this activity is covered by the new fundamental right that would have to be effectuated either by a pertinent interpretation of existing data protection laws or by legislative action. It doesn’t necessarily mean that this practice is illegal in any case. But it means that it cannot be done in secrecy but the user has to be provided with a clear notice and an opt-out option. Furthermore, security measures have to be put in place to protect against unauthorized access by third parties.

23 See Press Release of the EU Article 29 Working Group of Feb. 19, 2008, http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr 18 19 02 08 en.pdf: “As the use of search engines becomes a daily routine for an ever growing number of citizens, the protection of the users’ privacy and the guaranteeing of their rights, such as the right to access to their data and the right to information as provided for by the applicable data protection regulations, remain the core issues of the ongoing debate. Search engines fall under the EU Data Protection Directive 95/46/EC if there are controllers collecting users’ IP addresses or search history information, and therefore have to comply with relevant provisions. These provisions also apply to such controllers who have their headquarters outside the EU, but only an establishment in one of the EU Member States, or who use automated equipment based in one of the Member States for the purposes of processing personal data.”
3. A comparative view to the U.S.

3.1. The constitutional side

One of the differences between the European and the U.S. approach relates to the preconditions of the right to privacy vs. data protection laws. In the U.S. the right to privacy is invoked when there is a subjective expectation of privacy and this is reasonable in the sense of objectively warranted. This approach is also related to the idea of confidentiality and of a private domain as the object of protection. Whereas the European approach focuses on personal data and their processing in its effects on human autonomy.

In a decision marking the peak of the constitutional privacy protection the Supreme Court reviewed constitutional principles that had been invoked to protect the right to privacy: 1st, 4th, 5th Amendment. It concluded that the Due Process Clause of the 14th Amendment was the most appropriate basis. In Whalen v. Roe the Court followed this reasoning and distinguished two interests: the individual interest in avoiding disclosure of personal matters, and the interest in making certain kinds of important decisions. However, later case law is less assertive and while protection is granted in certain areas, on the whole no comprehensive constitutional right to privacy can be assumed in U.S. law. Also 4th Amendment analysis while promising to shift the focus from the protection of “places” to “people” was limited to secrecy and confined to protecting the private home. Still, some commentators see the 4th Amendment as the focus point to anchor the constitutional right to privacy, also favoring a “sliding scale” of protection.

While the 14th Amendment would be broad enough to derive a comprehensive constitutional right to privacy one of the reasons is a narrow construction of the Constitution clinging more to the wording. In Bowers v. Hardwick Justice White expressed this concern: "Nor are we inclined to take a more expansive view of our authority to discover new fundamental rights imbedded in the Due Process Clause. The Court is most vulnerable and comes nearest to illegitimacy when it deals with judge-made constitutional law having little or no cognizable roots in the language or design of the Constitution…There should be, therefore, great resistance to expand the substantive reach of those Clauses, particularly if it requires redefining the category of rights deemed to be fundamental. Otherwise, the Judiciary necessarily takes to itself further authority to govern the country without express constitutional authority. The claimed right pressed on us today falls far short of overcoming this resistance".

Of course, there are different approaches to the Court’s role and methods. Constitutional law has to be developed in the light of the objectives and principles of the framers and the guarantees entrenched in the Constitution can only be effectuated if interpreted in light of new social facts.

29 See the analysis of Casey, 41 U.C.Davis L. Rev. 977, 983 et seq. (2008).
30 Simmons, 97 J Crim. L. & Criminology 531, 554 (2007).
32 See Rehm (n. 28) p. 77; Schwarz, 37 Am.J.Comp.L. 675, 683 et. seq. (1989); Casey, 41 U.C.Davis L. Rev. 977, 1033 (2008).
This view is not without support in the U.S. Specifically, some state constitutions grant constitutional privacy protection implicitly or explicitly. There is an interesting case decided by the New Jersey Supreme Court on April 21, 2008. The facts provide a good example of the issue of confidentiality and integrity of IT systems in the internet age. In 2004 the owner of a website was informed that the shipping address and password had been changed on his website. For that purpose someone had accessed the website using the owner’s username and password. The hacker’s IP address had been recorded by the website, and the owner asked Comcast to provide the user’s data but Comcast refused. The owner obtained a Municipal Court subpoena on Comcast to which Comcast submitted the information sought and identified Shirley Reid as the subscriber of the IP address. The owner was suspicious of her as a former employee who left the owner’s company in conflict and knew the company’s access data.

The New Jersey Supreme Court emphasized that while the U.S. Supreme Court had found no expectation of privacy in information exposed to third parties under the 4th Amendment the New Jersey Constitution – under nearly identical language - granted greater protection of “informational privacy”. The Court cited preceding case law relating to telephone bills. It found that use of the internet equally is an integral part of today’s society. As users are forced to disclose their identity to obtain services from ISP’s, but not for the purpose of disclosing it to others, the Court found a reasonable expectation of privacy under the New Jersey Constitution in the subscriber information they reveal to ISP’s. While the IP address does not reveal the contents of communications it may be used to track the user’s searches and make a profile. The Court also linked the reasonableness of the privacy expectations to the development of technology; as long as IP addresses are only known to ISP’s this expectation may be protected. The Court ruled that a grand jury subpoena would be needed instead of a municipal subpoena.

While this case still hinges on traditional concepts of privacy the recent discussion on electronic surveillance in the U.S. has for once shown that courts should no longer hesitate confronting the constitutional issue posed by electronic communications. On the other hand the traditional reasonable expectations test does not fit the realities of computer networks.

What advantage would a constitutional commitment to privacy have over the current state? A constitutional right would provide a firm basis and strengthen the privacy interest in civil law cases as well if it comes to a weighing of opposing interests. It would be more difficult to contract your privacy rights away given the inalienability of fundamental rights that might also enhance requirements for assuming consent to giving up rights. It would help make privacy protection more solid and permanent avoiding short term changes of political preferences.

3.2. Data protection and information security regulations

Certainly the wording of the 4th Amendment would be open to integrate information security on a constitutional level. On the legislative level there are a number of statutes in place that aim at providing information security. Among them are the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 that provides criminal and civil liability for acts compromising the security of computer systems. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22 and 2701-12 prohibits

34 State of New Jersey v. Shirley Reid (A-105-06), http://www.judiciary.state.nj.us/opinions/supreme/A-105-06%20State%20v%20Shirley%20Reid.pdf,
35 See Freiwald, 2007 Stan. Tech. L. Rev. 3, (2007), applying a four factor test that in many ways is consistent with the criteria employed by the German Constitutional Court.
the unauthorized and unjustified interception, disclosure, or use of communications including electronic communications. Its first part relates to the interception of ongoing communications during transmission, its second part to communications stored. The DMCA, 17 U.S.C. § 1201, provides sanctions for the circumvention of technological protection measures. Gaps are filled by state computer crime laws and common law theories like trespass to chattels. Also, trade secret law creates incentives to provide information security. In addition there are laws and regulations in place protecting the national security infrastructure.

The overview demonstrates that the legislative basis for extracting a fundamental right to the confidentiality and integrity of IT systems is also firmly established in the U.S. That there may be loopholes that could be covered by such a constitutional right is demonstrated by a case relating to the practice of DoubleClick that was quoted as a candidate for a similar loophole under German law supra. In 2001, a U.S. District Court found that neither the ECPA nor the Stored Communications Act prohibited this activity, due to the consent of the Affiliated Sites with which the users had communicated on whose websites cookies had been placed. The same argument that the consent of one communication partner to access by third parties abrogates constitutional protection, is also acknowledged in German constitutional law, so this reasoning may also be found in a German Court decision. Still a question remains as to whether this is an overstretch. This case should not be viewed as being about the question of whether protected trust was present in the communication but more as a case about reasonable security expectations from a systems point of view. There are now different business models in use increasingly involving ISP’s as a mediator for placing cookies on the user’s computer. This poses new threads also in terms of security.

Data protection in the U.S. is happening more on a self-regulatory level. The EU Directive and the Safe Harbor concept were quite successful in at least bringing bigger companies to adhere to a European level of data protection. The reason is not only pressure from the EU but also the perception that data protection is an important element in gaining consumer confidence. The FTC is increasingly following privacy issues. With respect to behavioural advertising the FTC issued principles as a guidance to self-regulatory measures. To address the need for greater transparency and consumer control regarding privacy issues raised by behavioral advertising, the FTC staff proposes:

Every Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose.

To address the concern that data collected for behavioral advertising may find its way into the hands of criminals or other wrongdoers, and concerns about the length of time companies are retaining consumer data, the FTC staff proposes:

40 In re DoubleClick Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y. 2001).
Any company that collects or stores consumer data for behavioral advertising should provide reasonable security for that data and should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

While these rules seem appropriate on the merits they may suffer from the problems of enforcement of self-regulatory measures already mentioned.

4. Resume

The decision of Feb. 27, 2008 can be expected to have similar impact than the Census decision of 1983. Given the framework of German constitutional law a review of data protection laws as well as ramifications in various areas of civil law may be expected. On an international level other countries may follow suit. This is not only likely due to the fact that the German judiciary and legislation has always played a leading role in the development of data protection law and concepts. It is development of technology that made adaptation of constitutional protection necessary. While the limitations of law in internet governance are acknowledged alternative and supplementary instruments are also freight with shortcomings. Given the importance of constitutional law and the power of judicial review that extends beyond the legal sphere it can be expected that this decision not only created a “paper tiger” but will have important practical effects. Courts in the U.S. will be increasingly confronted with similar questions as well.43 The path the German Constitutional Court has taken may be one way of coping with the realities of the information age.

43 See Lin, 17 Berkeley Tech. L. J. 1085, 1118 et seq. (2002), calling for a strong constitutional foundation of the right to informational privacy in light of information technology development.
1. BASIC RIGHTS

Article 1 (Protection of human dignity). (1) The dignity of man is inviolable. To respect and protect it is the duty of all state authority. (2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world. (3) The following basic rights bind the legislature, the executive and the judiciary as directly enforceable law.

Article 2 (Rights of liberty). (1) Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral code. (2) Everyone has the right to life and to inviolability of his person. The freedom of the individual is inviolable. These rights may only be encroached upon pursuant to a law.

Article 3 (Equality before the law). (1) All persons are equal before the law. (2) Men and women have equal rights. (3) No one may be prejudiced or favored because of his sex, his parentage, his race, his language, his homeland and origin, his faith or his religious or political opinions.

Article 4 (Freedom of faith, of conscience and of creed). (1) Freedom of faith and of conscience, and freedom of creed religious or ideological, are inviolable. (2) The undisturbed practice of religion is guaranteed. (3) No one may be compelled against his conscience to render war service as an armed combatant. Details will be regulated by a Federal law.

Article 5 (Freedom of expression). (1) Everyone has the right freely to express and to disseminate his opinion by speech, writing and pictures and freely to inform himself from generally accessible sources. Freedom of the press and freedom of reporting by radio and motion pictures are guaranteed. There shall be no censorship. (2) These rights are limited by the provisions of the general laws, the provisions of law for the protection of youth and by the right to inviolability of personal honor.
(3) Art and science, research and teaching are free. Freedom of teaching does not absolve from
loyalty to the constitution.

Article 6 (Marriage and the family; children born outside of marriage).

....

Article 7 (Education).

....

Article 8 (Freedom of assembly).

(1) All Germans have the right to assemble peacefully and
unarmed without prior notification or permission.
(2) With regard to open-air meetings this right may be restricted by or
pursuant to a law.

Article 9 (Freedom of association).

(1) All Germans have the right to form associations and
societies.
(2) Associations, the objects or activities of which conflict
with the criminal laws or which are directed against the constitutional
order or the concept of international understanding, are prohibited.
(3) The right to form associations to safeguard and improve working and
economic conditions is guaranteed to everyone and to all trades and
professions. Agreements which restrict or seek to hinder this right are
null and void; measures directed to this end are illegal.

Article 10 (Privacy of letters, posts, and telecommunications).
(amended 24 June 1968)

(1) Privacy of letters, posts, and telecommunications shall be inviolable.
(2) Restrictions may only be ordered pursuant to a statute. Where a
restriction serves to protect the free democratic basic order or the existence
or security of the Federation, the statute may stipulate that the person
affected shall not be informed of such restriction and that recourse to the
courts shall be replaced by a review of the case by bodies and auxiliary
bodies appointed by Parliament.

Article 11 (Freedom of movement).

(1) All Germans enjoy freedom of movement throughout the
Federal territory.
(2) This right may be restricted only by or pursuant to a statute, and only in cases in which an
adequate basis of existence is lacking and special burdens would arise to the community, or in
which the restriction is necessary to avert an imminent danger to the existence or the free
democratic basic order of the Federation or a Land, to combat the danger of epidemics, to deal with
natural disasters or particularly grave accidents, to protect young people from neglect or to prevent crime.

Article 12 (Right to choose an occupation, prohibition of forced).

(1) All Germans have the right freely to choose their trade or profession their place of work and their place of training. The practice of trades and professions may be regulated by law.
(2) No one may be compelled to perform a particular work except within the framework of a traditional compulsory public service which applies generally and equally to all. Anyone who refuses on conscientious grounds to render war service involving the use of arms may be required to render an alternative service. The duration of this alternative service shall not exceed the duration of military service. Details shall be regulated by a law which shall not prejudice freedom of conscience and shall provide also for the possibility of an alternative service having no connection with any unit of the Armed Forces.
(3) Women shall not be required by law to render service in any unit of the Armed Forces. On no account shall they be employed in any service involving the use of arms.
(4) Forced labor may be imposed only in the event that a person is deprived of his freedom by the sentence of a court.

Article 12a (Liability to military and other service)
(added 24 June 1968)
....

Article 13 (Inviolability of the home).

(1) The home is inviolable.
(2) Searches may be ordered only by a judge or, in the event of danger in delay, by other organs as provided by law and may be carried out only in the form prescribed by law.
(3) Otherwise, this inviolability may be encroached upon or restricted only to avert a common danger or a mortal danger to individuals, or, pursuant to a law, to prevent imminent danger to public security and order, especially to alleviate the housing shortage, to combat the danger of epidemics or to protect endangered juveniles.

Article 14 (Property, right of inheritance, taking of property)

(1) Property and the rights of inheritance are guaranteed. Their content and limits are determined by the laws.
(2) Property imposes duties. Its use should also serve the public weal.
(3) Expropriation is permitted only in the public weal. It may take place only by or pursuant to law which provides for kind and extent of the compensation. The compensation shall be determined upon just consideration of the public interest and of the interests of the persons affected. In case of dispute regarding the amount of compensation, recourse may be had to the ordinary courts.
Article 15 (Socialization).

Land, natural resources and means of production may for the purpose of socialization be transferred into public ownership or other forms of publicly controlled economy by a law which provides for kind and extent of the compensation. With respect to such compensation Article 14, para. 3, sentences 3 and 4, apply mutatis mutandis.

Article 16 (Deprivation of citizenship, extradition, right of asylum).

(1) No one may be deprived of his German citizenship. Loss of citizenship may arise only pursuant to a law, and against the will of the person affected it may arise only if such person does not thereby become stateless.
(2) No German may be extradited to a foreign country. Persons persecuted for political reasons enjoy the right of asylum

Article 17 (Right of petition).

...

Article 17a (Restriction of individual basic rights through legislation enacted for defense purposes and concerning substitute service).
As amended March 19 1956.

...

Article 18 (Forfeiture of basic rights).

Whoever abuses freedom of opinion, in particular freedom of the press (Article 5, paragraph 1) freedom of teaching (Article 5, paragraph 3), freedom of assembly (Article 8), freedom of association (Article 9), the secrecy of mail posts and telecommunications (Article 10), property (Article 14), or the right of asylum (Article 16, paragraph 2) in order to attack the free democratic basic order, forfeits these basic rights. The forfeiture and its extent are pronounced by the Federal Constitutional Court.

Article 19 (Restriction of Basic Rights).
(1) Insofar as under this Basic Law a basic right may be restricted by or pursuant to a law, the law must apply generally and not solely to an individual case. Furthermore the law must name the basic right, indicating the Article.
(2) In no case may a basic right be infringed upon in its essential content.
(3) The basic rights apply also to corporations established under German Public law to the extent that the nature of such rights permits.
(4) Should any person's right be violated by public authority, recourse to the court shall be open to him. If no other court has jurisdiction, recourse shall be to the ordinary courts.
USE OF RETAINED DATA AND INTELLECTUAL PROPERTY RIGHTS – BALANCING ACT BETWEEN DATA PROTECTION, TELECOMMUNICATION AND COPYRIGHT LAW

Christian Czychowski¹, Jan Nordemann²

Abstract
In its decision from 11 March 2008, the BVerfG delivered a much discussed judgement in respect of the new §§ 113a and 113b TKG (Telecommunications Act) as part of interim proceedings. The effect of the judgement is not to restrict data retention in accordance with §113a TKG. All the same, providers compelled to retain data may only pass data to prosecution authorities in the case of serious crimes as determined by §110a(2) StPO (German Code of Criminal Procedure) and on fulfilment of the conditions set down in § 100a(1) StPO. In respect of other requests, the data are to be stored but not passed on¹. The BVerfG has reserved final judgement for the proceedings in the main issue following the provision of further information from Federal Government. Much less attention in Germany has been received by a decision of the ECJ delivered on 29.01.2008, just a few weeks before the decision of the BVerfG. The case before the ECJ concerned the use of person-related data saved by providers. The decision contains interesting aspects in respect of the relationship between data protection law on the one hand and intellectual property rights, in particular copyright, on the other, which could become relevant for the BVerfG in its final decision on the constitutionality of §§113a, 113b TKG.

1. The (copyright) problem

Infringement of intellectual property rights, in particular copyright infringements, occurs on the internet in various forms. An especially “popular” forum for copyright infringements is provided by so-called internet exchange networks (also “file-sharing” through peer to peer networks). Users of such forums upload copyright protected music, software and films thus making them publicly accessible in the sense of §19a UrhG (Copyright Act). Making such protected works accessible to the public is – where approval from the affected holder of right has not been given – illegal. It is irrelevant whether such works were uploaded for purely private or commercial reasons⁴; the privilege contained in §52 UrhG after all extends only to public performance of a work without pecuniary reward and not to the making of such works accessible to the public as defined by §19a UrhG. As a result of such illegal uploads, other users are able to download the music or film on to a data carrier – which at the very latest since the 2nd Round amendment of §53(1)(1) UrhG effective as of 1 January 2008 is also illegal, even where the download is made as private act⁵. The reason for

¹ Dr. Christian Cychowski, Solicitor in Berlin and specialist in IT-law, Boehmert & Boehmert Chambers, Lecturer at the University of Potsdam.
² Solicitor in Berlin, Boehmert & Boehmert Chambers; Honorary Professor at the Humboldt University, Berlin.
³ BVerfG decision from 11 March 2008, file no. 1 BvR 256/08 568 et. seg.
⁴ For detailed treatment see Jan Bernd Nordemann/Dustmann CR 2004, 380
⁵ On the 2nd Round: Czychowski GRUR 2008.
this is that music, software and films of commercial value made available free of charge on file-sharing networks are “obviously made available illegally” under §53(1) (1) UrhG. According to the findings of a recent university study, illegal file-sharing results in damage to the German film industry alone in the amount of some € 193 million per year, the German music industry assumes that for every one legal music download, ten are made illegally (in total 312 million illegal music downloads in 2007).

Uploaders and downloaders require access to the internet which they acquire through the internet access provider (hereinafter: provider). Providers generally do not ascribe non-corporate clients a fixed IP address. The general practice is to ascribe a so-called dynamic IP address each time afresh when logging on to the internet. This dynamic IP address is generally capable of being ascertained by third parties. The identity of the client, however, remains anonymous. The client can only be traced by the provider consulting client data to determine which client was ascribed the relevant dynamic IP address at the time of the infringement in question. Without the provider consulting data on who received which dynamic IP address and at what time, the identity of the person committing copyright infringement cannot be ascertained and the infringement, be this a criminal or civil infringement of copyright, cannot be pursued.

However, the identification of the client by the provider – and where necessary the passing on of findings to third parties –, is a significant act from the perspective of data protection law. Since data here concerned (name, address, dynamic IP address, begin and end of internet connection) are person-related data in the sense of the Data Protection Act (§3 BDSG) and accordingly the prohibition on passing of such data without approval as set down in §4 BDSG applies.

a) Authority and obligation to save data

From the perspective of the provider, authority must exist for it to save these data – if not, from the perspective of the right holder, it even be obligatory to do so. To this end, it is clear that such data retention by the provider falls under the law of telecommunications data protection and not the former TDDSG, now contained in the law of tele-services data protection in the TMG, as § 1(1) TMG ascribes this to the law of telecommunications, which – put simply – involves the pure transmission of signals, where here the transport of signals stands in the foreground. This is true of provision of access to the internet. The TKG differentiates between stock data (§ 3 No. 3 TKG) and traffic data (§3 No. 30 TKG). Upon conclusion of the contract for provision of internet access, the provider records the name and address of the client. These are unquestionably stock data. Both the dynamic IP address and data held with respect to beginning and end of the internet sitting are, on the other hand, traffic data. Whether the two in conjunction (dynamic IP address at a certain time) as well as name and address of the client (stock data) are covered by the rules for stock data or by the rules for traffic data seems to us to be an open question. For the purposes of this opinion we assume the more stringent rules for traffic data.
Traffic data may be used for the purposes listed in § 96 TKG. In accordance with § 96(2) TKG, traffic data retained (it is unclear here whether this subsection refers only to the data retained under the conditions set down in the previous subsection) may only be used beyond the point of disconnection where it is necessary to use them for the purpose of reconnecting, the purposes set down in §§ 97, 98, 100 and 101 TKG (in particular fee calculation and interference, not of interest here) or other purposes founded in other statutory provisions (author’s emphasis). We will return to the latter in the discussion below. Alongside this concession, §113a also contains a duty to retain data. This duty falls to the provider and extends for a period of six months for the purpose of public security.

b) Authority to pass on data

Further, authority must also exist to pass on data. This depends on the type of infringement.

aa) Criminal prosecution

Where a criminal prosecution is commenced (§ 106 UrhG, alternately § 108a UrhG), the prosecuting authorities may demand the provider identify the user and further require that the user’s identity be communicated to them (§100a(1) No. 2 StPO). § 100g StPO supplies here a sufficient basis of authority for the prosecuting authorities, at least with respect to traffic data retained in accordance with § 96 TKG. At the latest since the decision of the BVerfG here discussed, the question as to whether data retained under § 113a TKG may be included remains open. Asserting a criminal prosecution also meets with additional resistance from prosecution authorities which, in the case of mass assertion of owner rights, often feel that such attempts at justice are burdensome and inappropriate given the extent of infringement12.

bb) Civil action

In practice, the route via prosecution authorities is the only way of finding out the identity of the person committing the infringement of copyright as up to present German High Regional Courts, for instance, OLG Frankfurt13, OLG Hamburg14 have rejected claims for disclosure of information capable of identifying users where such claims were based on analogue application of §101a UrhG15. With the implementation of Art 8 EU Enforcement Directive16, however, a basis of claim for disclosure of exactly this information will be included in the UrhG. The implementing act17 expressly states that with § 101(2) UrhG a claim for disclosure of information against the provider is to be introduced18. In order harmonise such claims with the principle of secrecy of telecommunications, special proceedings over which a judge must preside are set down in §101(9) UrhGE (Copyright Bill).

12 AG Offenburg, MMR 2007, 809; Communication StA to LG Wuppertal, see www.heise.de from 26 March 2008, 17:56
13 OLG Frankfurt, GRUR-RR 2005, 147, 148.
14 OLG Hamburg, GRUR-RR 2005, 209, 212 – Ramstein, see on similar opinions expressed by OLG Munich and OLG Cologne Czychowski/Jan Bernd Nordemann, NJW 2006, 580, 584 with footnote 65.
17 Recommendation and report of the legal committee on Act for Improvement of the Assertion of Intellectual Property Rights, BT-Drucks 16/8783.
18 RegE BT Drucks. 60/5048, page 49
Even with the introduction of the new § 101(2) in connection with (9) UrhGE, it is by no means certain that the road lays fully clear for a civil action for the disclosure of the identity of the person committing the copyright infringement and thus the actionability of mass infringement of copyright in file-sharing networks. Quite apart from the field of telemedia with its separate concession for the passing of data (contained in § 14(2) TMG)\(^{19}\), a similar express concession is missing in respect to the TMG. Nevertheless, in our opinion the above mentioned §96(2)(1) TKG with express reference to traffic data in §101(9) UrhGE can provide sufficient basis for the claim. Also possible would be the application of § 28(3)(1) BDSG, though this is disputed by some commentators\(^{20}\). Here too, therefore, it will be followed with interest how the BVerfG decides in the case on data retention in respect of the application of data saved in performance of and in accordance with the duty contained in §113a TKG with respect to the civil action for disclosure of information under § 101(2) UrhG and whether is draws a distinction between traffic data under § 96 TKG and traffic data under § 113a TKG.

2. Relevance of the BVerfG judgement in the main issue

With respect to criminal prosecution, centrally important will be whether the BVerfG decide to prevent the use of traffic data collected and retained in accordance with § 113a TKG in all cases except those serious crimes catalogued under § 100a(2) StPO and where the conditions set down in §100a(1) StPO are met. Breach of copyright in the form of uploading/downloading files to and from internet file-sharing sites - § 106 (and perhaps §108a) UrhG - is not a serious crime in the sense of §100a(2) StPO. Should the BVerfG assume a general prohibition of use – and not merely a prohibition on passing on of data – with respect to the traffic data retained in performance of duty under § 113a TKG, serious crimes as set down in §100a(1) and (2) StPO excepted, the identification of the person committing the copyright infringement for the purpose of criminal prosecution using traffic data under §113a TKG would no longer be possible. The copyright infringement would accordingly no longer be actionable.

The BVerfG has already indicated in its previous decision that the restrictive interpretation put on the authority to pass on data contained in §113b StPO affects only those traffic data which are stored in accordance with §113a StPO\(^{21}\). The fall-back on to traffic data stored under §96 TKG suggested by the BVerfG will, however, presumably be of no help in the majority of cases. After all, it is today very much the norm to secure internet access by way of monthly flat-rates. Accordingly to an ARD/ZDF online study, at least 69% held flat-rate deals for their internet use.\(^{22}\) As at first sight, §96 TKG only covers data for the purpose of fee calculation and fee invoicing, various courts have held the retention of traffic data under § 96 TKG to be unlawful with respect to flat rate tariffs\(^{23}\). Data protection authorities have also officially warned providers on several occasions after they were found to have saved traffic data under § 96 TKG. We doubt that this was ultra vires in view of the connection between § 96(2)(1) TKG and § 101(9) UrhGE, certainly after the introduction of § 101(9) UrhG. So long as flat-rates remain standard, it must, however, be expected

---

\(^{19}\) The Government Draft justifies this expressly with synchronisation with the Enforcement Directive: RegE EIVG BT Drucks. 16/3078, page 12; and this is also recognised in the literature: Spindler/Weber ZUM 2007, 257, 261.

\(^{20}\) For: Czychowski MMR 2004, 514, 517.; Jan Bernd Nordemann/Dustmann CR 2004, 380, 385; OLG Munich GRUR 2007, 419, 424; Against Kitz ZUM 2006, 448; Spindler/Dorschel CR 2006, 342; also for LG Hamburg, MMR 2005, 55; this decision was, however, changed by the OLG Hamburg with different justification.

\(^{21}\) BVerfG op cit, 173

\(^{22}\) [http://www.daserste.de/service/adronL.0407.pdf](http://www.daserste.de/service/adronL.0407.pdf), there table 5.

\(^{23}\) LG Darmstadt, judgement from 25.1.2006, 25 S 118/05, in criminal case; appeal to BGH rejected, but only on the grounds that the minimum claim value had not been achieved (!): BGH, MMR 2007, 37; AG Bonn, MMR 2008, 203; AG Berlin Mitte, ITRB 2008, 34; AG Darmstadt, CR 2006, 38; LG Darmstadt, CR 2007, 574 (7 days permitted).
that providers desist from retaining traffic data under §96 TKG, independent of whether the question as to whether – if they don’t want to store such data – whether they are obliged to retain data. In addition to this: The provider will certainly save the relevant traffic data only once, even where two legal provisions, §96 TKG and §113a TKG, expressly allow the storage of such data. It is therefore no longer clear, under what provision the data were saved. In cases of doubt as to the permissibility of data retention under §96 TKG in respect of flat-rates, the provider will be able to rely on §113a TKG to justify data retention so that for this reason too, § 96 TKG plays very much a secondary role.

With respect to a civil action, the prohibition on use of data saved under § 113a TKG is also likely to apply. Should the BVerfG hold that the use of traffic data retained under §113a TKG - and thus the identification of the person committing the infringement of right - only be allowed in the case of a §100a(2) StPO offence and where the conditions of §100a(1) StPO are fulfilled, it wouldn’t then be particularly consistent to then allow these data to be used for the identification of the person committing the infringement of copyright within the framework of a civil action. Obviously then – in comparison to copyright protection – the constitutional significance of use of data in accordance with § 113b TKG would be so high that even civil actions for disclosure of information would be appear to be excluded. The claim which § 101(2) UrhG purports to grant would accordingly fail on principles of constitutional law as far as it seeks to identify persons infringing copyright by uploading/downloading files from internet file-sharing sites. With this, the possibility of pursuing internet piracy through the civil courts in the fields discussed here would fail.

3. **Appropriate balance between data protection law and the law of copyright**

The impossibility of instigating legal actions, both criminal and civil, against persons committing copyright infringement through internet file-sharing sites, which has already reached dramatic proportions, would present quite a legal problem.

This is true first and foremost of German law. The law of copyright itself has a constitutional value which shouldn’t be underestimated; it falls within the ambit of the right of property under Art 14 GG24 (Basic Law). Copyright as property right is insofar to be balanced against other basic rights25. By virtue of Art 14 GG, copyright holders are entitled to demand that copyright protection and the interests of the general population are balanced fairly against each other26.

The same is true under EU law. As the BverfG expressly states in the decision on data retention here discussed, mandatory EU law lies outside the jurisdiction of the BVerfG provided - what is here the case – the European Communities generally provide effective protection for fundamental rights; protection which is essentially the same as the inalienable protection provided by German Basic Law27. In respect of European law, just a few weeks before the decision of the BVerfG, the ECJ stressed that in implementing the various directives in the field of protection of intellectual property rights, the Member States are obliged under Community Law to construe the directives so as to allow the Member States to achieve an “appropriate balance” between the various fundamental rights established under Community law28. In particular, the ECJ imposes a duty on state authorities

---

24 Established case law BVerfG GRUR 1990, 438 – Bob Dylan; BVerfG GRUR 1972, 5481 – Church and School Custom
26 BVerfG, GRUR 1972, 481, 484 – Church and School Custom
27 BVerfG, op cit, 135.
28 ECJ, GRUR 2008, 241 – Promusicae/Telefonica, there part of headnote.
and courts, to apply the principle of proportionality, which is a basic principle of Community law. The case at hand concerned the question of whether the Member States have a duty to provide for the legal possibility of supplying person-related data within the framework of civil proceedings as part of the requirement to secure effective protection of copyright. The ECJ rejected the existence of such a duty, though stressed – as described – the application of the principle of proportionality. In particular, the ECJ states that intellectual property rights – which include copyright – and the right to an effective legal remedy are general principles of Community law. These “general principles of Community law” have been repeatedly codified in directives relating to copyright. Art 8(1) of the European Copyright Directive thus foresees that that Member States provide for appropriate sanctions and remedies and implement all measures necessary to secure their application. It also stresses that sanctions must be “effective, proportionate and dissuasive”. This is reiterated in the Enforcement Directive in Art 3(2) which further stresses that measures, procedures and remedies must be applied so as to ensure “that barriers to legal trade are avoided and that there is guarantee against their misuse”.

Given such general principles of Community law with respect to the guarantee of intellectual property rights and effective remedy to their infringement, it is impossible to deny the actionability of mass infringement of copyright through internet file-sharing sites on the basis of the data protection legislation where users make use of dynamic IP addresses. Exactly this would be the effect of denying the prosecuting authorities the possibility of bringing a criminal action under §100g StPO) and the copyright holder the possibility of mounting a civil action under §101(2) UrhGE by preventing them demanding the release of the identity of the wrongdoer from the provider. Should such a claim for the disclose of the identity of the wrongdoer fail under points of constitutional law, both the constitutional guarantee for the protection of intellectual property rights afforded by Art 14 GG as well as general principles of Community law would be violated. In proceeding in the main issue, the BVerfG will be forced to find a way of allowing the use of traffic data stored under § 113a TKG in the investigation of copyright infringement, in particular through internet file-sharing, either in a criminal or civil context.

4. Possible mediative solution

The law of intellectual property has a remedy at its disposal which it would do to explain here, the border seizure procedure. The procedure works as follows: First, the owner of certain intellectual property rights makes a general application to customs authorities that certain goods are checked for legal violations. Should the authorities believe the goods are in breach, they are retained and the right owner is informed of this fact. The right owner can then make an assessment of its own and confirm that there has indeed been a violation of its rights. The person from whom the goods were seized, alternatively the recipient of these goods, is then offered the opportunity to make objection to the seizure. Should no objection be made, the goods will be destroyed. Should objection be made, the right owner must instigate appropriate proceedings before court.

One might consider whether such an arrangement could be applied mutatis mutandis to the balance of interests with respect to internet use: A right owner makes an application to the authorities in respect of certain works which it considers to be at particular risk of being illegally copied or illegally made available on the internet. In the case that the right holder determine a violation of right in respect of such works or other protected works, it informs the authorities which in turn inform the relevant internet provider. Of course, the authorities first thoroughly check whether the

---

29 ECJ, op cit.
30 ECJ op cit, 62
information matches with that given in the application, in respect of which, the right owner must also make a declaration of liability and release. The authorities forward the information to the internet provider which then informs its customer about the official request, allowing the customer an opportunity to object to the release of its data. Should the internet user fail to make objection, the data are sent by the provider to the authorities, which in turn send them on the right owner for plausibility assessment. Should the user object, the right owner must instigate court proceedings for the release of information. Experience of the border seizure procedure shows that in the majority of cases, the “violator” recognises the breach and does not object. Right owners are thus helped substantially by reason of the large number of further violations so prevented. Indeed the procedure has shown itself to provide very efficient legal protection of intellectual property rights. On the other hand, the legitimate interests of the user, also in the case of an unauthorised user, are protected and data are not released before it have the opportunity to object such.

Since the border seizure procedure has proved so successful, it makes sense to consider a solution to the third party information problem in light of experience gained here. The traditional border seizure procedure is so effective because it allows the party at whose disposal the goods are, that is, the party suspected of violating the intellectual property rights of another, the opportunity to do nothing, to refrain from objecting to the measures instigated by the authorities on the application of the right owner, and thus simply to allow the procedure to take its course. The violator accordingly retains the possibility of accepting its mistake without the risk of incurring unnecessary further costs and so to end the infringement immediately. At the same time, it remains in a position in which it can instigate court proceedings should it feel necessary. Practical experience shows that most violators make no use of their right of objection when they fear having to pay the costs of any ensuing legal action. The violator is generally aware of whether it’s in the right or in the wrong and reacts rationally when discovered. One could therefore consider whether it would be productive to insert an automated request procedure prior to any instigation of the § 101(9) Copyright Act procedure. This could follow the administrative procedure already used in border seizures, albeit with necessary changes.

This would first require that a state authority be established which would assume the function of customs authorities in border seizures. The work done would not be staff-intensive investigatory work, but would rather involve the operation of a fully automated electronic data processing system that would act as a puffer, as it were, between the interests of the party obliged to provide information to the access provider, the ‘violator’, and those of the ‘injured party’ demanding the information. Such an office could be established as part of the Federal Network Agency. Under these circumstances, the following procedure is suggested:

- The ‘injured party’ enters information of the suspected violation into a form on the authorities’ website, in particular including the (dynamic) IP address, time and duration of the connection, the object of the violation as well as an explanation of ownership of right.

- The information so provided will be automatically forwarded to the access provider which, in turn, will return connection data to the authorities also as part of a fully automated response.

- The authority then sends a machine generated notice to the putative violator based on the information provided by the ‘injured party’ and informs the ‘violator’ that proceedings for the release of information to a third party have been instigated.
• The ‘violator’ has the option of agreeing to the forwarding of its data to the ‘injured party’ (alternatively the consent could be deemed to have been given on failure to respond within a period of, for example, two weeks, in urgent cases less) or of objecting to the forwarding of information by the authorities, in which case the ‘injured party’ can be informed. It would be necessary to indicate to the ‘violator’ that in the case that it lose before court, it would have to bear the costs of gaining such information.

• Should the ‘violator’ object, the ‘injured party’ would be informed immediately. It would then, and only then, be in a position where it must instigate proceedings under §101(9) Copyright Act.

Experience from the physical border seizures show that such a procedure would be an efficient way of gaining authorisation from the ‘violator’ to release information and even to gain from it a voluntary undertaking to cease and desist from further infringement. Expensive and time-consuming proceedings can thus be shortened. Litigation would only follow where it really would be necessary.
COMPETITION AND IPR ISSUES IN STANDARD SETTING

Grazyna Piesiewicz

Abstract

The presentation will give an overview of the competition rules that apply to IPR-policies in standard setting. It will focus in particular on the discussions relating to ex ante disclosure and licensing policies developed by standard setting organisations.

The presentation is not intended to provide a full and detailed analysis of the application of Article 81 to standard setting agreements. It will start by providing a brief overview of Art 81 issues to then focus on specific problems that may arise when technologies protected by intellectual property rights (IPR) are incorporated in a standard.

Industry standards have a positive effect insofar as they drive economic interpenetration in the common market, encourage the development of new markets and promote efficiency, and consumer choice. Standards provide for improved supply conditions, for lower transaction costs, benefiting economies as a whole. These benefits are achieved as standards aid in ensuring interoperability, maintaining quality, and providing information.

Within the European internal market, standards provide additional benefits related specifically to the policy objective of market integration within the EU.

In spite of its benefits, the collaborative process of standard setting may therefore raise issues of collusion and exclusion if anti-competitive coordination is only disguised as standard setting and is aimed at suppressing competition and/or price fixing. Standardization agreements are caught by Article 81(1) but may be exempted under Article 81(3) if they “promote economic interpenetration in the common market or encourage the development of new markets and improved...”

---

1 Case Officer, Information Industries and consumer electronics, DG Competition, European Commission Brussels, EU. E-mail: Grazyna.PIESIEWICZ@ec.europa.eu.


4 Pursuant to the case law of the European Court of Justice following the Cassis de Dijon case, certain restrictions to the free movement of goods provided for in Article 28 of the EC Treaty are permissible. Common standards, governmental or private, help eliminate ensuing restrictions to trade among Member States.

supply conditions." The exemption is conditioned inter alia upon a finding that the agreements contain no restrictions of competition that are not indispensable to achieve the reasonable objectives of the standard, such as unnecessary restrictions on innovation and that access to the standard must be made available to new entrants on the market wishing to comply with the standard.

Other issues arise once a company's essential IPR has been incorporated into the standard, and once the industry has been locked in to the standard because the essential IPR holder might charge an artificially inflated ex post monopoly price which it would not have otherwise been able to charge ex ante due to availability of alternatives at the time the standard was being discussed. It can be difficult in practice for a commitment to licence on fair, reasonable and non-discriminatory terms to constrain the charged price.

The presentation will discuss a number of ongoing cases related inter alia to the so-called patent ambush. On that basis, it will shed some light on the principles, which standard setting organisations should abide by under EU competition rules when developing IPR-policies, to avoid problems stemming from the situation described above and to ensure that the economic and social benefits generally associated with standard setting are produced.

---

6 Ibid. para 169.
7 Ibid, para 173.
8 Ibid, para 169.
STANDARDS POLICY

Benoît Müller¹

Abstract

When addressing standards-related issues, competition authorities and other policy makers should consider that sound policy in this area involves a balancing of several important interests. An appropriate standardisation policy should ensure software innovation, promote interoperability, enable user choice, and protect intellectual property rights.

Market-lead standardisation is key to achieving these goals. When consumers have a choice of multiple standards that have been developed using a variety of methods, innovation will be rewarded and interoperability will be enhanced. Because it is impossible to predict how any specific solution will fare in the marketplace, policies should encourage competition between standards.

Protection of intellectual property is also important, as software companies make substantial investments in R&D that further innovation. Protection of IPRs creates an incentive to innovate. Market-led standardisation helps to balance the interests of licensors and licensees in this respect - by permitting RAND licensing terms, voluntary standards bodies encourage participation in standardisation and the contribution of essential technologies.

As policy makers, governments should promote innovation, technical neutrality, consumer choice and competition. As ICT customers, government agencies should have the same flexibility as other users to choose the solution that best meets their needs. Governments should select the most appropriate and cost effective solution, in accordance with the procurement law principles of technical neutrality, non-discrimination and best value for money.

¹ Director of Software Policy, BSA, Brussels. E-mail: BenoitM@bsa.org.
THE ABUSE OF DOMINANT POSITION IN CONTEXT OF THE REFUSAL TO LICENSE

Dariusz Kasprzycki

Abstract

Intellectual property rights constitute the legal monopoly which relates to the content of the right; however, the way in which the right is exercised may be the subject of antitrust proceedings and may be recognized as an infringement of competition law. In principle, the dominant trader, owner of the intellectual property right, is not obliged to license the right. Thus the refusal may constitute anticompetitive conduct only if it is combined with some other additional and exceptional requirements. The concept of essential facilities doctrine seems to be the basis for identifying aforementioned exceptional circumstances justifying the intervention of antimonopoly law. The European Court of Justice has confirmed that, as the “facility” could also be understood as the intellectual property right. However, the detailed requirements for applying the essential facilities doctrine seems to be still not precisely recognized. The article aims to summarize the conditions for limiting the exploitation of an exclusive right in cases of abusive conduct.

1. The abuse of dominant position and intellectual property rights

1.2. Principles of competition law

Article 82 of the EC Treaty prohibits any abuse by an undertaking of a dominant position within the common market or in a substantial part of it as incompatible with the common market in so far as it may affect trade between Member States providing further the most typical forms of such abuse. The structure of aforementioned provision requires first in every case the evidence of dominance. Such a finding must precede an infringement decision. Here it is extremely important to properly define the relevant market which constitutes the common ground for the activities of undertakings involved in the given case.

In 2005, the European Commission initiated discussion of the application of Article 82 of the EC Treaty to some exclusionary abuses. These abuses are understood as behaviours by dominants which are likely to have a foreclosure effect on the market, e.g. likely to deny access to a market to actual or potential competitors. The legislative framework covering the relevant market has been indicated as one of the entry barriers. Such legislation may limit the number of market participants, for example by granting special or exclusive rights in the shape of concessions, licenses or intellectual property rights. Legislative measures that grant a single undertaking the exclusive right to perform a certain activity excludes rivals and may lead to such an undertaking having a legal monopoly in a relevant market. [1]

---

1 Ph.D., Intellectual Property Law Institute, Jagiellonian University, Krakow, PL.
1.2. The nature of intellectual property rights

Intellectual property rights (IPRs) cover various creations of the human mind having an immaterial character like inventions, literary and artistic works, symbols, names, images, and designs used in commerce. All of them are built on a proprietary basis which gives the owner exclusivity of exploitation.\(^2\) It is fully justified to say that in terms of competition law intellectual property rights create the legal monopoly. However the monopoly relates only to the content of the right, the way in which the right is exercised may be the subject of antitrust proceedings and may be recognized as an infringement of competition law.

The central function of intellectual property rights is to protect the moral rights in a right-holder’s work and ensure a reward for the creative effort\(^3\). But it is also an essential objective for intellectual property law that creativity should be stimulated for the public good. A refusal by an undertaking to grant a licence may under exceptional circumstances be contrary to the general public good by constituting an abuse of a dominant position with harmful effects on innovation and on consumers.[2] Intellectual property rights may also prevent expansion and entry or make it more difficult, depending on the nature and actual strength of the intellectual property right held by the dominant firm.

Initially, it may be pointed out that there should be two form of IPR limitation resulting from competition law:
- preventing from refusing the licence
- limiting the terms and conditions included in the licence by IPR owner.

The latter seems to be no controversial as far as it is clearly related not to the content but the pure exploitation of the right. It seems rather that the crucial issue in this context would be the question of whether Art. 82 of the EC Treaty limits the ability of an IPR owner to regulate the exploitation of his work and to refuse licences over his right?

2. Essential facilities doctrine

2.1. The concept of the doctrine

Over the last few decades we may observe the development and the application of the so-called essential facilities doctrine which has justified the far going intervention of antimonopoly law into the intellectual property rights exploitation. According to that doctrine, a company which has a dominant position in the provision of facilities which are essential for the supply of goods or services on another market abuses its dominant position where, without objective justification, it refuses access to those facilities. Thus in certain cases a dominant undertaking must not merely refrain from anti-competitive action but must actively promote competition by allowing potential competitors access to the facilities which it has developed. [3]

A facility could be understood as parts of infrastructure (bridges, railways, telephone networks) as well as intellectual property rights. Next, a facility, to be considered essential, must have an indispensable character for access to the market allowing them to compete with the controller of the facility. In order to qualify behavior as abusive, the denied access to the facility must be proved

---

\(^2\) The concept of so called trade secrets (or know-how) may be treated as exceptional and the basis for its protection is currently being discussed, specifically in Poland.

\(^3\) We have to be aware that focus on moral rights is not widely recognized in civil law systems.
while the practical duplication of the facility is not feasible. These are the simplified requirements of the doctrine which is still evolving. It may be added to as developed and the subsequent necessary condition in the form of the introduction of a new product, the appearance of which on the market is prevented by the dominant.

The doctrine has not so far been commonly recognized, however, its popularity is evident. Significantly, as a result of the first well-known judgements the increasing tendency for complainants to rely on the so-called "essential facilities" doctrine has appeared in any case where a competitor controls an asset to which they require access. The leading essential facility cases in reference to intellectual property rights are summarised below.

2.2. From Magill to IMS Health

Perhaps the most important engaging good deal of attention is the Magill case. [4] In 1995 the ECJ upheld the Commission decision recognizing the refusal to license by a copyright holder as an abuse of dominant position. The subject of copyright in this case were the TV listings conferred by national legislation. By refusing to grant a licence to copy this material, the plaintiffs were unable to publish a weekly TV guide containing comprehensive listings for the week ahead.

As already mentioned the exclusive right of reproduction forms part of an author’s copyright. In this case it has been confirmed that, in principle, the competition rules are applied without prejudice to legal monopolies and only exceptional circumstances may justify the intervention of competition law.

Firstly, the judgement pointed out that the refusal to grant a licence would breach the competition rules only when where the owner of copyright holds a dominant position. Interestingly, this position has been found not thanks to the mere fact of possessing the copyright but by the monopoly over information needed to compile the listings of TV programme. [4] This finding suggests that the exact subject of the legal monopoly granted by IPR should not be automatically treated as the subject of relevant market.

Secondly, the ECJ found the following exceptional circumstances in this case:
- programme scheduling was an indispensable raw material for preparing the TV guide;
- the alleged abuser had prevented the appearance of new product;
- there was evidence that the consumer demand for a new product existed and dominants failed to meet this demand;
- foreclosing of secondary market.
As a result of the refusal to licence the dominants had reserved to themselves the benefits of a downstream market for a derivative product (a weekly TV guide).

The unusual nature of Irish and UK copyright which offers the protection of compilations of information must be stressed in this case. In the continental copyright system such protection probably cannot be granted and the discussion of applying the essential facility doctrine to intellectual property has not started so early. However, the fact that the facility had been recognized as basic information, this favoured applying the findings developed in judgements where the access to raw materials was in the spotlight. In Commercial Solvents the ECJ held that that "an undertaking which has a dominant position in the market in raw materials and which, with the object of reserving such raw materials for manufacturing its own derivatives, refuses to supply a customer, which is itself a manufacturer of these derivatives, and therefore risks eliminating all
competition on the part of this customer, is abusing its dominant position within the meaning of Article 82". [5]

The refusal to grant access has been the subject of many more ECJ judgements⁴, however, the IMS Health case [6] seems to be more significant in context of mutual relation of intellectual property and competition law.

The IMS Health has developed a so-called “brick structure” for providing the reports informing pharmaceutical companies on their products’ regional sales. The “brick structure” divided Germany into 1860 parts or geographical zones facilitating handling with the reports. This structure has been developed following the suggestions of IMS clients, i.e. pharmaceutical companies. Brick modules became successfully adopted in Germany by the whole pharmaceutical sector (including doctors and pharmacies). A rival to IMS (Pharma Intranet) devised their own structure different from IMS’s but it was declined by the market because companies had become accustomed to the IMS’s brick structure. Attempts to use a similar structure has faced the IMS’s response who has sued competitors for copyright infringement and obtained the judgements prohibiting the use of the structure derived from the said “brick modules”.

As the result of the proceeding launched by the NDC (successor to Pharma Intranet), alleging the abuse of dominant position, the European Commission has ordered IMS to grant a licence. The EC pointed out the following criteria:
- the refusal of a licence is likely to eliminate all competition from the relevant market;
- the refusal is not capable of being objectively justified;
- the IPR itself is indispensable to carrying on business as far as there is no substitute (actual or potential).

In contrast to the Magill case, the EC did not find it necessary to prove that the refusal prevented the emergence of new product and that dominant tried to control the related market. It was not therefore clear, taking into account even all former ECJ rulings, whether this criteria should be read cumulatively or disjunctively on case by case basis. [7] Furthermore, because of the absence of two different markets and in consequence no market power from dominated market transferred to downstream market - there was no leverage in this case. [8]

The ECJ has determined that four cumulative conditions are necessary for a refusal to licence copyright to be abusive:
- the copyright work must be indispensable to operate in the secondary market; The Court held that there might be economic obstacles for making the alternative products or services impossible or at least unreasonably difficult, clarifying further that “in order to accept the existence of economic obstacles, it must be established, that the creation of those products or services is not economically viable (…)” In fact, the indispensability means in this case that the copyrighted material must

---

⁴ It is worth citing the ECJ in Volvo v. Veng (Case 238/87) where the Court said that “an obligation imposed upon the proprietor of a protected design to grant to third parties, even in return for a reasonable royalty, a licence for the supply of products incorporating the design would lead to the proprietor thereof being deprived of the substance of his exclusive rights, and a refusal to grant such a licence cannot in itself constitute an abuse of a dominant position. It must, however, be noted that the exercise of an exclusive right may be prohibited by Article 82 if it includes, on the part of the undertaking holding a dominant position, certain abusive conduct such as the arbitrary refusal to supply spare parts to independent repairers, the fixing of prices for spare parts at an unfaire level or a decision no longer to produce spare parts for a particular model even though many cars of that model are still in circulation, provided that such conduct is liable to affect trade between Member States”
constitute a standard. In other words, there could not appear the other protected by exclusive right material which could satisfy the market expectations.

- the person asking the licence must intend to create a new product for which there is a potential consumer demand; The Court, however, did not define the concept of a new product. In this case we should rather talk about services or products of a similar nature rather than completely “new”.
- the refusal must not be justified by objective considerations; It has been left to the national court to examine whether the refusal could be justified.
- refusal is likely to eliminate all competition in the secondary market; the Court has distinguished the upstream market (1860 brick structure) and the secondary/downstream market (supply of reports of regional sales)

I quite agree with comments saying that the decision strikes the right balance between competition and copyright laws by making the difference between copyright and other forms of property in the conditions required for abuse. [9] The identification of upstream market which has been made equal to subject of possessed copyright seems dubious to me. If so, every IPR’s subject would automatically constitute a separate market. This step is a rather questionable way of taking into account the traditional way of defying the relevant market by criteria of assortment and territory. It is more convincing that there are simply no two distinct markets.

3. Microsoft case

Among the cases classified with the keyword “refusal to licence” may be placed also the Microsoft [10] although there is no compulsory licence to IPR involved. However, one may find many analogies.

The proceedings before the European Commission regarded a practice of Microsoft of integrating a separate product (Windows Media Player) with the Windows OS. The proceedings commenced with Sun Microsystem’s complaint about the refusal by Microsoft to share information indispensable to secure its ‘interoperability’ of its products with the Windows OS. The Commission expanded the proceedings to include ‘tying’ of Windows Media Player with the OS. The Court of the First Instance has finally upheld the Commission decision confirming that Microsoft had infringed Art. 82 of the EC Treaty by abusing dominant position on the operating system market by:
- refusing to supply the interoperability information and allow its use for the purpose of developing and distributing work group server operating system products;
- making the availability of the Windows Client PC Operating System conditional on the simultaneous acquisition of Windows Media Player.

The most interesting issue is the Microsoft’s refusal to supply its rivals with the information they need to offer compatible products. Once it was recognized as an abuse of dominant position the application of essential facility doctrine may be here considered. In order to justify this pleading there is a need to prove that the information on the Windows interface is the essential facility and denying access to the information leads to leveraging and foreclosure conduct. As it was several times underlined the refusal may constitute the anticompetitive conduct only if it is combined with some other additional requirements. The interoperability information should be regarded as indispensable for creating new product in the downstream market and the dominant’s refusal to grant the access to it could not be objectively justified.

On the other hand, this “additional abusive conduct” may consist in the dominant refusal to license, except on anticompetitive or exploitative terms, or if the trader refused to license a right which it
had committed to license for the purposes of a standard. If so, Microsoft could not be classified as the “essential facility case”. [11]
However, it does not mean that we could not observe the anticompetitive conduct in this case like the leverage issue. Microsoft denying the access for the interoperability information makes the other software markets easier for leveraging, even if we cannot currently observe any attempts to enter the markets with a new Windows application.

There is another interesting issue related to the exact scope of the required information to be shared with others. The upheld EC decision aimed at disclosing some information about its operating system that would be sufficient to allow interoperability with other pieces of software in the meaning of Article 6 of the Directive 91/250/EEC on the legal protection of computer programs. This article allows decompilation insofar as it is necessary for interoperability, which is defined in its preamble as the ability to exchange information and mutually to use the information which has been exchanged. This means that an independently created program cannot be a clone of a decompiled program but it can use interfaces resulting from decompilation of interfaces necessary to ensure functionality on condition that it itself offers similar functions. On the other hand, the EC decision defined interoperability information as a complete and precise specification of all protocols included in a Microsoft operating system necessary to run file exchange, printing and system administration services. There are interesting opinions that this step may be considered as a transgression the lawful limits of decompilation included in Directive 91/250/EEC. [12] However, one may argue that access to source code is not being required. There is rather strong need to disclose the raw information allowing to introduce new product as it was the case in other aforementioned judgements. It seems that only the exaggerated scope of information required for interoperability may cause possible interference with the content of exclusive rights.

4. Conclusions

There is no doubt in the light of aforementioned judgements that the essential facilities doctrine could be applied to intellectual property rights if exceptional circumstances were proven. In order to be abusive a refusal to license an intellectual property right must be combined with some other factor, anti-competitive behaviour or intent. A pure refusal to deal could not itself amount to an abuse.

Both first cases relate to the unusual copyrighted material. The level of creativity presented in these works was rather legal if any. The first (TV program listings) could be treated as composition of information, the second (brick structure) was created by incorporating the German postal code system with the considerable help of others. In both these cases, it has been shown that the dominants tolerated the usage of protected material by others unless they were not competitors for them. These two circumstances lead to the statement that the competition authorities were seeking rather a sort of unfair behaviour of undertakings which attempted to justify it by the presence of legal monopoly granted by intellectual property right. And the economic rationale for punishment of such behaviours has been pushing the authorities to use their antitrust instruments.
5. References


Extended abstract

Legal experts in the United States complain that there is a growing divergence in applying Anti-trust Law in the U.S. and in the EU. To demonstrate this, these experts refer particularly to the European Commission’s rejection of the merger between General Electric and Honeywell in 2001 and the Microsoft decision of the European Commission in 2004.

On March 24, 2004, the Commission concluded that Microsoft broke EU competition law by leveraging its dominance in the market for PC operating systems to the markets for work group server operating systems and media players. The Commission found that Microsoft had abused its dominant position by refusing to supply critical interoperability information to competitors and by unlawfully tying the sale of Windows Media Player ("WMP") to its dominant Windows client PC operating system ("Windows"). The Commission imposed record fines of EUR 497.2 million and required Microsoft to disclose certain interoperability information to competitors to enable them to produce work group server operating systems that can be fully integrated with Windows and to offer a version of Windows without the WMP preinstalled.

In the United States, lawyers and economists have found no evidence to support the idea that the "tying" of one product to another has inherently harmed competition, except when it is specifically used to extend an existing monopoly. It is only within this narrow set of circumstances that Microsoft was found to have violated the Antitrust rules of the United States. U.S. Courts have rejected claims that Microsoft was trying to leverage its dominance of Windows into new markets like internet browsers, media players and other software. Moreover, the D.C. Circuit Court of Appeals reaffirmed its holding that dominant companies should be allowed to innovate when it rejected appeals of the lower court decisions.

The opposite approach is taken by the European Commission. The Commission argues not only that tying WMP to Windows is illegal but also that the addition of any new functionality to a dominant product is inherently illegal.

Microsoft appealed the European Commission’s decision to the European Court of First Instance (CFI) and lodged an application to suspend the decision until the CFI rules on its annulment application.

On December 22, 2004, the President of the CFI unequivocally rejected Microsoft’s application to suspend the decision.

1 Dr. Hans-Werner Moritz, European Counsel, Jones Day
On September 17, 2008 the CFI delivered its judgment. This judgment rejected on almost every ground Microsoft’s appeal against the March 24, 2004 decision of the Commission, finding that Microsoft had infringed Art. 82 of the EC Treaty by refusing to supply competitors with inter-operability information and by tying the sale of WMP to the sale of Windows.

The CFI did, however, find that the Commission had exceeded its powers by delegating the task of overseeing the interoperability remedy to an independent trustee paid for by Microsoft.

1. The General Approach Adopted by the CFI

The CFI has been criticized in recent years for its willingness to overturn Commission factual findings, particularly in merger cases.

In the Microsoft judgment, the CFI emphasizes that where the Commission has given thorough consideration to complex technical or economic issues, the Commission’s factual conclusions will only be overturned when the Commission has committed a manifest error in its assessment.

But the greater part of the judgment is devoted to the consideration of challenges by Microsoft to the factual assessments made by the Commission in the March 2004 decision.

In each case, the CFI upheld the Commission under the “manifest error” standard.

The CFI also rejected several arguments put forward by Microsoft because it took the stance that they were based on a mischaracterization of the 2004 decision. In particular, the CFI rejected Microsoft’s contention that the 2004 decision was intended to allow rivals to create “clones” of Microsoft products in the work group servers market. On this basis, the CFI rejected arguments made by Microsoft regarding both the application of the Magill / IMS test and the utility of the remedy.

2. Legal Issues Addressed by the CFI

2.1. Refusal to supply interoperability information

In respect to the refusal to supply interoperability information, the CFI addressed important aspects of the Magill / IMS test. The CFI, however, did not determine whether the Microsoft interoperability information was in fact protected by IP rights since the Commission’s decision was not based on the absence of such rights. The CFI therefore assessed the case on the basis that the interoperability information was protected by IP rights, which meant that the “exceptional circumstances” test established by the Court of Justice in Volvo, Magill and IMS was applicable. As supplied in Magill and IMS, this test has three elements: (i) the input protected by IP must be “indispensable” for competition in a neighboring market; (ii) refusal to supply the input must create the risk that competition in that market will be eliminated; and (iii) the party seeking the input must supply an “unmet need.”.
The CFI ruled that an input is “indispensable” for purposes of this test where it is necessary for firms seeking the input to be fully effective competitors in the affected market.

The CFI further ruled that “the risk of elimination of competition” does not require a “high probability” that all competition in the affected market will be eliminated, and that the “risk” relates to “effective competition” not all competition.

Most importantly, the CFI ruled that the “unmet consumer need” requirement did not necessarily relate to the production of a new type of product, but could also extend to similar products incorporating significant technical developments that benefit consumers.

2.2. Bundling

In respect to bundling the WMP, the CFI endorsed the legal assessment of the 2004 decision. In particular, the CFI approved the application of Art. 82 (d) EC to bundling through the physical design of a product.

The CFI also ruled that the fact that the additional “product” is provided at no additional charge did not affect the bundling analysis.

2.3. Burden of Proof

The CFI clarified the burden of proof regarding “objective justification” under Art. 82 EC; according to the judgment, a dominant firm has the obligation to assert any grounds on which its conduct is objectively justified and to provide the evidence supporting this assertion.

The Commission is required, however, “to show that the arguments and evidence relied on by the undertaking cannot prevail.”

Thus, the CFI has imposed a “burden of production” on the dominant firm, but the burden of proof remains on the Commission.

2.4. Irrelevance of Secondary Community Legislation

The CFI rejected arguments by Microsoft that secondary community legislation (Directive 91/ 250) or international agreements of which the EU is a party (TRIPS) were relevant to assessment of a dominant firm’s obligations under Art. 82 or to the remedies formulated by the Commission under Art. 82 EC.

The Court based its ruling on the status of Art. 82 EC as primary legislation that can only be altered through an amendment of the Treaty itself.
3. Penalty Payments Levied on Microsoft

On July 12, 2006 the Commission levied a penalty of EUR 280,5 million on Microsoft for failing to comply with the technical disclosure requirements imposed in the Commission’s 2004 decision covering the period of up to June 20, 2006.

On February 27, 2008 the Commission levied a further penalty of EUR 899 million concluding that the royalties that Microsoft charged for the information license – i.e. access to the inter-operability information - between June 26, 2006 and Oct. 21, 2007 were unreasonable. The Commission has based its conclusions as to the unreasonableness of Microsoft’s royalties prior to Oct. 22, 2007 on the lack of innovation in a very large proportion of the unpatented interoperability information and a comparison with the pricing of a similar interoperability technology.

The 899 million EUR penalty brings the total fines imposed on Microsoft to EUR 1.68 billion.

4. Impact of the Judgment

Based on the above, it is obvious that global information technology companies will be held to drastically different standards in Europe and the United States. This may constitute a threat to the future of global business.

Such threats have already materialized recently. In the wake of the announcement of Microsoft’s new Windows Vista operating system and its Office 2007 application software, U.S. IT companies (e.g. Google, Adobe, Symantec, Apple), that did not succeed in gaining the support of the U.S. DOJ for their complaints that Microsoft violated U.S. anti-trust laws by adding features to Vista and Office 2007 that allegedly undermined rival technologies and constrained innovations, turned to the EU Commission for support by invoking its decision of March 24, 2004. The Commission has taken up their complaints and has initiated investigations against Microsoft.

Moreover, a growing transatlantic rift also becomes visible in the area of merger cases. Mergers that were approved by the FTC or DOJ in the U.S., but were rejected by the EU Commission include Boeing/McDonald Douglas (1997) and GE/Honeywell Bull (2001). Furthermore, even an EU member state has rejected a merger approved by the U.S. authorities (the German Cartel Office rejected the merger of Coherent, Inc./Excel Technology, Inc. on October 10, 2006).

5. Outlook

The Commission will see the CFI judgment as a robust and far reaching legal precedent that will impact the Commission’s Art. 82 EC enforcement agenda. A hint of that can be seen in the investigation of a complaint lodged by Opera Software ASA after the issuance of the CFI judgment alleging illegal bundling of Windows with the Internet Explorer.

Is there a chance that U.S. competition law and EU competition law may get more in synch in the near future? Probably not.
However, there is hope that through cooperation in the International Competition Network (ICN) the U.S. and EU enforcement agencies may better understand their respective positions and eventually achieve to avoid decisions that are diametrically opposed.
CREATIVE COMMONS: STRUGGLING TO ‘KEEP IT SIMPLE’

Lucie Guibault

Abstract

Contrary to other open content or open source licences, like the GNU General Public Licence and the Licence Art Libre, the Creative Commons (CC) licensing system gives authors the choice to decide which rights they wish to reserve for themselves or grant under license. Also, contrary to other types of open content licences, CC licenses are intended to be translated and adapted to the laws of a maximum of jurisdictions in the world. The rationale behind this structure is the belief that in this way the CC licenses are better accepted among users, better admissible in court, better adaptable to new techniques or situations and that they better empower the authors. The result, however, is that the CC licensing system tends to become increasingly complex both for authors and users, with a high risk of incompatibility between licences. The aim of this paper is twofold: first, to highlight the areas where problems of incompatibility may arise; and second to discuss the potential legal consequences of such incompatibility.

1. Introduction

Among the numerous licensing models based on the ‘open content’ ideology, the most successful application so far is the Creative Commons initiative (creativecommons.org), which was set up initially in the United States, but is now rapidly spreading across the globe. While the current copyright regime is serving the needs of intermediaries, the open content licensing model, especially the Creative Commons licence, is directed mostly to individual authors. Creative Commons (CC) has developed a series of standard-form licenses that allow authors of literary, musical or audiovisual works to permit wide dissemination and transformative uses of their works, without forfeiting copyright. While copyright law creates the default rule of All Rights Reserved, making permission necessary for each and every use of a work, CC seeks to facilitate an environment in which Some Rights Reserved or even No Rights Reserved become the norm. The CC licensing scheme is designed to meet the diverse preferences of authors and at the same time keep it simple and easy to employ for both authors and users of copyrighted material. The mechanism for achieving this goal is through a standardized and automated licensing infrastructure.

Contrary to other open content or open source licences, like the GNU General Public Licence and the Licence Art Libre, the Creative Commons (CC) licensing system gives authors the choice to decide which rights they wish to reserve for themselves or grant under license. Also, contrary to other types of open content licences, CC licenses are intended to be translated and adapted to the laws of a maximum of jurisdictions in the world. The rationale behind this structure is the belief that in this way the CC licenses are better accepted among users, better admissible in court, better adaptable to new techniques

1 Dr., Assistant Professor, Institute for Information Law, University of Amsterdam, e-mail: L.Guibault@uva.nl.
or situations and that they better empower the authors. The result, however, is that the CC licensing system tends to become increasingly complex both for authors and users, with a high risk of incompatibility between licences.

The aim of this paper is twofold: first, to highlight the areas where problems of incompatibility may arise; and second to discuss the potential legal consequences of such incompatibility. There are at least four areas of possible incompatibility between licenses: between versions of the CC licences; between the licenses themselves; between the licenses of the different jurisdictions; and between CC licences and other ‘compatible’ licenses. Problems of incompatibility may seem primarily theoretical at this point, but not all consequences may be currently foreseeable. The issue should not be neglected, since the resulting legal uncertainty may ultimately affect the acceptance and use of the licenses by both authors and users of creative works. This paper is further divided in three sections: section 2 introduces the main characteristics of the CC licences, while section 3 identifies a number of potential areas of incompatibility between the licences. Section 4 discusses the possible consequences that specific situations of incompatibility may bring about for authors and users.

2. Creative Commons licences in a nutshell

The Creative Commons licensing system offers a set of standardised and automated licences that authors can affix to their work in order to indicate under which conditions the work may be used. Thanks to these licences, it is no longer necessary for users to contact the rights holder prior to every use of the work to find out what can or cannot be done with the work. The work is therefore made available to everyone in accordance with the conditions of the chosen Creative Commons licence.

The CC core licensing suite also lets authors mix and match conditions from the list of options below. There are a total of six Creative Commons licenses to choose from the core licensing suite.

- **Attribution** Authorizes others to copy, distribute, display, and perform the copyrighted work — and derivative works based upon it — but only if they give credit in the way the author requests.

- **Noncommercial** Authorizes others to copy, distribute, display, and perform the work — and derivative works based upon it — but for noncommercial purposes only.

- **No Derivative Works** Authorizes others to copy, distribute, display, and perform only verbatim copies of the work, not derivative works based upon it.

- **Share Alike** Allows others to distribute derivative works only under a license identical to the license that governs the work. **Note:** A license cannot feature both the Share Alike and No Derivative Works options. The Share Alike requirement applies only to derivative works.
From the statistics available, it appears that the most popular combination of terms is the CC-Attribution-Non-Commercial-ShareAlike licence. One can therefore infer that most authors who apply CC licences to their works find it important to be credited as author of the work, that it not be used commercially, and that if it leads to the making of a derivative work, this work also be distributed under a CC-Attribution-Non-Commercial-ShareAlike licence.²

Beside the four aforesaid core stipulations, a number of fundamental principles lie at the basis of each Creative Commons licence. Taking into account the conditions of the chosen licence, the licensor grants the user a worldwide, non-exclusive, perpetual (for the duration of the applicable copyright) license to reproduce, display, perform, communicate, and distribute copies of the work. All rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. In principle, all rights not expressly granted by Licensor are reserved. All CC licences are irrevocable. This means that the moment the work is distributed under CC a licence on the Internet, the author can no longer change his mind or withdraw the licence. In addition, the user is required to join a copy of, or the uniform Resource Identifier for, the applicable CC-licence to each copy of the work that he distributes, communicates or makes available to the public.

It is also important to note that the Creative Commons licence system makes in principle no difference between digital and analogous work, nor between several types copyright relevant acts, such as the act of reproduction or communication to the public. Article 2 of each CC licence provides that nothing in the license is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws. Moreover the licensor may not apply any effective technological measures to the work that restrict the ability of a recipient of the work to exercise the rights granted under the terms of the license.

To facilitate the widest possible use of the Creative Commons license system makes in principle no difference between digital and analogous work, nor between several types copyright relevant acts, such as the act of reproduction or communication to the public. Article 2 of each CC licence provides that nothing in the license is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws. Moreover the licensor may not apply any effective technological measures to the work that restrict the ability of a recipient of the work to exercise the rights granted under the terms of the license.

To facilitate the widest possible use of the Creative Commons licenses, the Legal Code has been translated and adapted to the legal system of an increasing number of national jurisdictions worldwide. To date, close to fifty jurisdictions have ‘ported’ the licences in their legal systems and more than ten other jurisdictions are currently involved in the porting process.³

3. Areas of potential incompatibility

Since the launch of version 1.0 in the United States in 2002, the Creative Commons licences have been tweaked, improved, ported and adapted with a view of making them better suited to the needs of authors, more acceptable to users, better admissible in court, and better adaptable to new techniques or situations. As we shall see below, the Creative Commons (CC) licensing system tends to become increasingly complex both for authors and users, with a high risk of incompatibility between licences. The improvement of the CC tools therefore comes at the cost of simplicity and easiness of use, which constitutes one of the main objectives of the CC movement.

² See: http://wiki.creativecommons.org/License_statistics
³ See: http://creativecommons.org/international/
3.1. Incompatibility between different versions of the CC licences

Four versions of the core CC-licenses are currently in use: versions 1.0, 2.0, 2.5 and 3.0. Only the first upgrade of the licences, e.g. from version 1.0 to version 2.0, involved a change in the core stipulations. One year into the existence of the licensing tools, it had already become obvious that the vast majority of authors who licensed their work under a CC licence wanted to be credited for their work. Upon implementing version 2.0 of the licences, the Attribution clause became the only mandatory stipulation in the CC licences. Versioning from 1.0 to 2.0 also brought a change to the Share Alike provision which was made more flexible. The version 1.0 licenses required that derivative be published under the exact same license only. The provision in version 2.0 allows licensees to license resulting derivative works under Creative Commons licenses that feature the same license restrictions/permissions, including future and iCommons versions of the same license. The Share Alike provision will also be clearer about what happens when different kinds of Share Alike content is mixed together (e.g., How to license a collage made from an SA photograph combined with an NC-SA photograph). This tweak means much better compatibility across future jurisdiction-specific licenses and across versions.4

Subsequent modifications and improvements were brought to the text of the licences itself either to clarify some key concepts or to make the licence easier to use. Version 3.0 introduced the following amendments:

- a new generic license was created, now known as the “unported” license;
- all CC jurisdiction licenses and the CC unported license have consistent, express treatment of the issues of moral rights and collecting society royalties (subject to national differences);5
- to avoid that a person not misuse the attribution requirement of a CC license to improperly assert or imply an association or relationship with the licensor or author, an explicit statement was introduced in both the Legal Code and the Commons Deed to ensure that there will be no confusion for either the licensor or licensee about endorsement issues;
- the CC Attribution-ShareAlike 3.0 licenses now include the ability for derivatives to be relicensed under a “Creative Commons Compatible License”. This structure realizes CC’s long-held objective of ensuring that there are no legal barriers to people being able to remix creativity in the way that flexible licenses are intended to enable
- finally, Version 3.0 of the licenses include minor clarifications to the language of the licenses to take account of the concerns of Debian and MIT regarding the release of CC-licensed works under Digital Rights Management by licensees on certain conditions.

---

3.2. Incompatibility between the licences themselves

Six core licences allow authors to choose the degree of ‘some rights reserved’. The table below shows how the licences can be used and how they are compatible with one another.

<table>
<thead>
<tr>
<th></th>
<th>by</th>
<th>by-nc</th>
<th>by-nc-nd</th>
<th>by-nc-sa</th>
<th>by-nd</th>
<th>by-sa</th>
<th>nc-sampling+</th>
<th>publicdomain</th>
<th>sampling+</th>
</tr>
</thead>
<tbody>
<tr>
<td>by</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by-nc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by-nc-nd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by-nc-sa</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by-nd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>by-sa</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nc-sampling+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sampling+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>publicdomain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1 Source: [http://wiki.creativecommons.org/FAQ#I_used_part_of_a_Creative_CommonsLicensed_work.2C](http://wiki.creativecommons.org/FAQ#I_used_part_of_a_Creative_CommonsLicensed_work.2C)

As the table above also shows, the CC organisation has also issued besides the six core licences, a number of specific licences. The deployment of new licenses show a constant need to arbitrate between promoting the use of generic licenses and the tendency to adapt to special needs. Creative Commons has also attempted to devise other tools by which a copyright owner could limit his ownership to a shorter length of time or relinquish ownership rights entirely.

Under its “Founders' Copyright” (named for the Constitution's Framers), the copyright owner enters a contract with Creative Commons to sell her copyright for one dollar. In return, Creative Commons grants back to the owner exclusive rights to control the work for a term of fourteen or twenty-eight years, and agrees to release the work into the public domain at the expiration of the term, as well as list the work in a registry. Under its “Public Domain Dedication,” Creative Commons provides a form for a copyright owner to create a certificate that they are dedicating a particular work to the public domain, “for the benefit of the public at large and to the detriment of the Dedicator's heirs and successors. . . . an overt act of relinquishment in perpetuity of all present and future rights under copyright law, whether vested or contingent, in the Work.” However, by their very nature, these two instruments are inherently linked to the American copyright system, and they can hardly be exported elsewhere in the world.

---

6 A.K. Goss, ‘Codifying A Commons: Copyright, Copyleft, And The Creative Commons Project’, 82 Chi.-Kent L. Rev. 963, p. 980.
In December 2007, in conjunction with the Creative Commons 5th Birthday celebration, Science Commons announced the Protocol for Implementing Open Access Data ("the Protocol"). The Protocol is a method for ensuring that scientific databases can be legally integrated with one another. The Protocol is built on the public domain status of data in many countries (including the United States) and provides legal certainty to both data deposit and data use. The protocol is not a license or legal tool in itself, but instead a methodology for a) creating such legal tools and b) marking data already in the public domain for machine-assisted discovery.

On August 29, 2008, CC released for public comment a revised beta draft of CC0 Waiver. The laws of various jurisdictions throughout the world automatically confer certain exclusive rights upon the creator of an original work of authorship and/or a database (each, a "Work"), and the subsequent owners thereof. Some owners of these exclusive rights wish to permanently remove these restrictions from a Work for the purpose of contributing to a commons that the public can reliably build upon, modify, reuse and redistribute as freely as possible from such restrictions for any purposes and in any form whatsoever, whether modified or unmodified, in whole or in part. Such owners therefore wish to fully, permanently, irrevocably and unconditionally waive, abandon and relinquish their Copyright Related Rights (defined below) with respect to a Work to the fullest extent permitted by applicable law. CC0 is meant to serve as a "Universal" legal tool, capable of being used in all jurisdictions without the formal porting process CC traditionally uses for its core licenses. However, the legal effect of CC0 will likely differ depending on the jurisdiction, especially since issues of enforceability and differences between legal systems still have to be solved.7

3.3. Incompatibility between the licences of different jurisdictions

National jurisdictions are able to ‘port’ the CC licences to their local legal system based on ‘unported’ licenses, which are in principle jurisdiction-agnostic: they do not mention any particular jurisdiction's laws or statutes or contain any sort of choice-of-law provision. While versions 1.0, 2.0 and 2.5 of the ‘unported’ licence (previously known as the ‘generic’ licence) were based on the provisions of the U.S. Copyright Act, version 3.0 of the ‘unported’ licenses is instead based on the provisions of the Conventions of Berne and Rome. This means that, though there is no reason to believe that the licenses would not function in legal systems across the world, it is at least conceivable that some aspects of the licenses will not align perfectly to a particular jurisdiction's laws.

Local peculiarities of the copyright regime can sometimes require an adaptation to the licenses that would disrupt their worldwide similarity. Specific issues have arisen during the national porting process with respect to moral rights, neighbouring and related rights, as well as the European sui generis database rights. With respect to moral rights, the difficulty lies in the fact that not all jurisdictions recognize these rights or at least to the same extent, thereby affecting the user’s freedom to make a derivative work based on an original CC licensed work. More discussion is still needed in order to even out the problems relating to the moral rights issue. Based on the wording of the ‘unported’ licence, it remained unclear whether the CC licences were meant to include neighbouring and related rights. The issue was recently clarified in the affirmative. Finally, some European countries had taken the stance to include the sui generis right in a database within the ambit of the CC licences. After much discussion on the desirability of including these rights at all within the scope of the CC

licences and taking account of the opposition voiced especially in the United States against such rights, a compromise was reached with the European jurisdictions according to which the right owners waive their sui generis database right.

Moreover, it is important to point out that besides the difficulties raised by the specificities of the national laws, problems of incompatibility may also arise either because national courts may give different judicial interpretation of key concepts at the root of the CC licences, like the ‘non-commercial’ clause, or because the porting process itself is at different stages in the national jurisdictions: the French CC-licences are still at version 2.0 while the Dutch CC-licences have been upgraded to version 3.0.

3.4. Incompatibility with other open content licences

The CC-ShareAlike licence provides that the user may distribute a derivative work only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US)); (iv) a Creative Commons Compatible License.

"Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

This clause was introduced in version 3.0 to address the issue raised by the Wikimedia Foundation of compatibility between the CC-ShareAlike licenses and the GNU Free Documentation Licence. However, the new provision in the CC licence does not specify what constitutes a compatible license and refers back to the CC website where there is so far no definition of what constitutes a ‘Compatible License’.

4. Impact of incompatibility

Discussions on the potential incompatibility between licences is only starting to emerge within the CC community. As Dusollier rightfully points out, ‘the issue of compatibility also proves that the approach might be very fragmented--not as global as a public ordering process might be. Therefore, there might be no legal certainty as to the limits of entitlements and freedoms granted by the license, which also reduces the effectiveness of the open-access norm’.

4.1. Contract formation

Creative Commons licenses are expressed in three different formats: the Commons Deed (human-readable code), the Legal Code (lawyer-readable code); and the metadata (machine-readable code). The Commons Deed, which is the first document visible to the user, is a summary of the key terms of the actual license, which basically states what users can and cannot do with the work. This Deed itself has no legal value, and its contents do not appear in the actual license. The Legal Code is the actual license, designed to be enforced in a court of law, which the user will read only if he takes deliberate action to access it. The metadata contains the key license elements that apply to a work in order to enable discovery through search engines.

Whereas the Commons Deed and Digital Code remain the same, a discrepancy between the Commons Deed and the Legal Code attached to a single work may give rise to problematic situations. For example, Japanese-speaking users of a work released in The Netherlands automatically view a full translation of the Commons Deed in their own language, as the site detects the users' web browser settings, but the Legal Code remains in Dutch. The true license terms are therefore not understandable to the Japanese user.

To what extent is the Creative Commons licence binding on parties of different jurisdictions? Under European and Japanese law, is the consent of the parties based on the summary provided by the Commons Deed sufficient to consider the license binding or must consent be exchanged on the basis of the Legal Code? Does the fact that the local porting process is at different stages among jurisdictions affect the consent given by users of different jurisdictions?

A research on the binding nature of licenses concluded between parties of different jurisdictions is not only interesting in the context of the Creative Commons project. More importantly, the findings of this study may guide the future development of other global, standardized, and automated licensing infrastructures with respect to the online distribution of copyright protected material. Only in these circumstances will content providers invest in the distribution of protected content in the digital networked environment.

4.2. Derivative works

One of the main consequences ensuing from a lack of compatibility between licences is that users may not be able to mix, mash and re-use works to the extent that they would want to, due to the uncertainty surrounding the scope of the licences. For example, any derivative work based on an original work released under a CC-Attribution and CC-Attribution-NonCommercial licence must be distributed under a licence that includes the same licence elements as the original (can also include other restrictions). However, licensing the derivative work under broader terms could be used to circumvent the original licence.

The different jurisdiction licenses with the same license elements may be slightly different regarding restrictions imposed on distribution of derivatives. For example, CC-Attribution 2.1 Japan is somehow more restrictive than CC-Attribution 2.0 Unported or 3.0 US at least on one aspect. It also seems that CC-Attribution 3.0 US is more restrictive than CC-Attribution-ShareAlike 3.0 US on the same aspect. The difference has to do with the treatment of license notices and warranty disclaimer notices in the
Work. If derivatives are allowed to be licensed only under the same or more restrictive licenses, derivatives of CC-Attribution US and CC-Attribution Unported licensed works could be licensed under CC-Attribution Japan license, but not vice versa. Or, it may turn out that CC-Attribution Japan is less restrictive in another aspect that has so far remained unnoticed. In that case the two licenses lose interoperability in an important way.\textsuperscript{9}

5. Conclusions

More research needs to be done to determine exactly where the areas of incompatibility between CC-licences are and what the consequences can be of a lack of compatibility. The fact remains, however, that any hint of incompatibility creates uncertainty among authors and users, which in turn increases transaction costs for all parties involved. This is certainly not the intended outcome of a licensing system that is meant to be ‘simple and easy to use’.

\textsuperscript{9} Observations made by Tomoaki Watanabe, Member, CC Japan Research Fellow Center for Global Communications (GLOCOM) International University of Japan.
LiMo FOUNDATION: HOW TO BENEFIT FROM OPENNESS WHILE BEING INCLUSIVE OF ALL LICENSING MODELS IN THE MOBILE WORLD?

Yann Dietrich

This document only expresses personal opinions of the author, and does not represent any views of his past or present employers, and furthermore does not represent any official position of LiMo Foundation or of any of its members.

Abstract
LiMo Foundation is an industry consortium aiming to unifying force in Mobile Linux by leveraging cooperative development and open-source licensing to deliver a consistent Linux-based mobile terminal platform for use by whole industry on superior economic terms. Challenge was then to develop an innovative IPR approach to benefit from openness while being inclusive of all licensing models, to make possible the coexistence of open source and proprietary licensing models, and LiMo developed such approach by articulating an IPR policy recognizing a specific place in its architecture for various licensing models.

LiMo Foundation is an industry consortium dedicated to creating the first truly open, hardware-independent, Linux-based operating system for mobile devices. Backing from major industry leaders puts LiMo at the Heart of the Mobile Industry and makes LiMo the unifying force in Mobile Linux.

LiMo Foundation was launched in January 2007 as a non-profit industry consortium when it had become apparent that the mobile industry was unwilling to broadly adopt the existing commercially licensed industry platform offerings because of concerns about ownership, governance and cost.

LiMo is leveraging cooperative development and open-source licensing to deliver a consistent Linux-based mobile terminal platform for use by whole industry on superior economic terms. The shared aim of the member companies is to accelerate the creation of compelling, differentiated, next-generation mobile consumer experiences of all kinds. LiMo Foundation is open to all vendors and service providers in the mobile communications marketplace, including device manufacturers, operators,

1 Yann Dietrich is General Counsel with LiMo Foundation, an industry consortium dedicated to creating the first truly open, hardware-independent, Linux-based operating system for mobile devices. Yann joined LiMo in 2007 after serving as head of the Legal department of the France Telecom/Orange IP and Licensing division and EMEA Chief IP counsel for Intel. He participated to the work on IPR issues of several international organizations such as ITU-T, OMA and ETSI and was recently representing the EU ICT industry in many discussions with EU authorities as Chair of the IPR group of the European Information and Communications Technology Industry Association (EICTA) over the last two years. Additionally, he teaches IP and licensing in two French universities and in UK as well.
chipset manufacturers, integrators and independent software vendors. Membership today stands at more than 50 companies.

Today the, wireless world, when it comes to patents, is primarily known for the litigiousness of various market leaders in relation to essential patents for the various wireless radio interfaces (e.g. GSM, WCDMA, CDMA 2000 …). In addition, when it comes to handset software platforms, the mobile world was until recently more reliant on closed “in-house” proprietary systems. However the rapidly increasing complexity of functions being performed by handsets and the need on the part of operators to broadly deploy consumers applications and services has made it uneconomic to sustain in-house systems and is driving their replacement with industry platforms. Probably influenced by the Open source movement, companies have realized that where there is limited differentiation, software is merely a cost, and sharing such costs is actually allowing each company to invest more where it matters: offering a better experience to users.

Obviously, developing such software alone does not allow sharing such costs and will not reduce fragmentation, and miss another opportunity to reduce operators’ costs forced to support all software platforms. The challenge was now to adopt the right rules to transform this business opportunity into a reality, and obviously, rules related to intellectual property rights are highly discussed. Perhaps more so in the case of LiMo Foundation (compared to standards organizations), as developing a shared software platform necessitates dealing with both patents and with copyrights as you are not talking only about a standard but also about the implementation of such standard.

The first challenge is obviously to create a safe eco-system - a safe harbor - so companies will be comfortable sharing their technologies. The second challenge is now that you have created such a peaceful environment how to foster the collaborative development of the platform software, and here open source principles are helpful, even in an environment inclusive of all business models.

1. Creating a safe IP harbour while respecting existing eco-systems

In this section, we will discuss about the way LiMo foundation structured its IPR policy to create its specific safe harbour while respecting existing licensing eco-systems. Obviously, we all know that the question of patents when it comes to software is emotional and quite controversial. In a context of an industrial consortium, the main priority is to find practical solution, and in this case, the priorities were to use the concept of patent non-assertion and to tailor it depending on the various usage of the software, but probably more important to scope the commitment related to patents. The underlying principle is that the software which are pure commodity as they do not offer any capacity of differentiation will be the only eligible for the core of the platform, and then for such software, the patent commitment should be broad and consequent, namely that none of the members should be able to charge royalties for copyrights, but as well for patents. Obviously, when such software is not a pure commodity, then, this functionality should be optional and the software may be subject to royalties. Now, specifically about patent, some carve-outs were decided, in the same spirit, to ensure that we focus on what is matter in the context of LiMo foundation and not modify the licensing relationships in other eco-systems.
1.1 A core platform IPR protected being copyright free and protected by a patent non-assert

In this sub-section, we will describe the details of the IPR policy of LiMo foundation about the Common code and the Foundation APIs, both benefiting from the higher level of IPR protection, and then the dynamics with the Non Common Code. Interestingly, we will analyze the criteria used to select Common Code and how in this scenario IPR and compliance aspects are closely linked.

1.1.1 A level of IP protection depending on the degree of commonality of the feature

Establishing a link between the value in terms of differentiation of a software and its costs in terms of intellectual property is not an invention of LiMo Foundation but an important principle of Open source2. When a piece of software is not adding any capacity of differentiation to a group of individuals/companies, it makes more sense for such group to mutualise the costs. Obviously, when another software is more capable of differentiation, the innovator will be interested to keep such innovation for itself or to value it.

In terms of patent protection, the patent non-assert between all Members will then include distribution to non-members (commercial exploitation) when it comes to the Common Code, the core of the platform to be used by all Members in what we called an Approved Implementation. Such strong patent protection is also granted to the Foundation APIs in order to ensure a safe patent harbour to our developers’ community. For Non-Common code, the patent non-assert is limited to the use between members inside the Foundation (R&D license). In terms of copyright, the same logic applies, only copyright royalty free contributions being eligible for the Common code while the Non Common Code being open to all licensing models.

These concepts of Common Code and Non-Common Code are built around the value in terms of differentiation of a module, and articulated architecturally around the concepts of Framework3 and plug-ins. The core, hardware independent and geographic functionalities are put together in a Framework which is expected to become Common-Code while more differentiating technologies will be added to the platform through plug-ins expected to be Non Common. For example, a multimedia framework will integrate all core functionalities about the management of multimedia objects while audio and video codecs will be integrated as Plug-ins.

1.1.2 Fragmentation dynamics in the Mobile industry

The Mobile industry is certainly a very good example of where the concepts of interoperability and fragmentation are fully part of the business equation. For example, having the possibility to send a text message only between Motorola’ phones does not make sense, neither will it make sense to be able to

---

3 “Framework” shall mean Middleware approved by the Foundation for inclusion in the Foundation Platform that is designed to provide certain core, hardware independent and geographic-market independent functionality for a certain type or class of Modules (e.g. “multimedia”), but by itself does not provide a set of functionality that is complete or near complete for applications needing to access functionality within such area. A Framework, together with Plug-Ins, provides all or nearly all of the functionality needed by applications within such area.
send text messages only between Orange’ customers. Today, for most of this very standard features, business can only grow when a sufficient degree of interoperability exists creating a large market.

Now, when it comes to Mobile platforms, the same equation exists and multiplying them creates two difficulties: increasing the costs of the operators and the complexity to provide rich services – splitting the application developers between several environments.

Obviously, it does not mean that all operators and phone makers are offering the same product and services, and today, new innovations appear every day and innovators should be able to be rewarded for their investment.

In the context of LiMo foundation, this requirement to manage fragmentation was integrated in the IPR policy. It means that traditionally compliance programs are organized around a trademark licensing program, meaning that you get a license to implement a standard, and if you want to be in a position to add a special logo indicating to consumers that your product is compliant to the standard, you will have to pass compliance tests, when actually, it is not about a profile of the standard (a selection of options described in the standard). In the context of LiMo, because fragmentation matters more, and also because of the importance of the patent commitments of all members, the license you get from various Members is limited to the concept previously explained of Approved Implementation.

1.2 A IPR protection respectful of neighbouring eco-systems

The ICT world is extremely complex and it requires some efforts when setting up an IPR policy to envisage all potential consequences. For example, how an IPR policy related to a software platform working on a phone will impact radio access technologies of such phone? How it will affect the mp3 technologies used in this phone? Both technologies being heavily patented and known active licensing programs.

Middleware software offers, first, a less active patent environment, but also if properly scoped less important in terms of differentiation. Challenge was then for LiMo Foundation to adopt an IPR policy supporting its business objectives while not “changing the world”, affecting so much neighbouring eco-systems in terms of patents that the IPR policy would have become too burdensome for any patent holders.

The first carve-out, and probably the most efficient is to exclude essential patents for standards. This type of exclusion will then allow the eco-system created around these patents to remain untouched, while at the same time, most of these patents are available through a commitment to license from companies participating to the relevant standardization process at some conditions defined by the standards organization policy, so a right to get a license is already secured. For example, a module implementing some specifications of the W3C, OASIS, ETSI, a very large proportion of these patents are already licensed, or at least subject to a commitment to license under the rules of the respective organizations. Organizing a second source of license for these patents under the LiMo IPR policy will create complexities when not unnecessarily tension by affecting eco-systems already in place. In addition, in most of the cases, some licensing arrangements already exist about these patents and then the conditions at which those patents are known or predictable.
The second carve-out, more complex is the exclusion of the combination, in more details, the contributory infringement of a combination patent where a portion of the combination necessary for the infringement is outside of the Foundation Platform. What does it mean practically is when you have a claim of patent covering a combination of the elements A, B and C, then, in such case, if the element C is outside the scope of the Foundation platform, such patent will not fall under the patent non-assert.

While, it may appear as seriously limited the scope of the patent-non assert those limitations are important, discussions about IPR policy are complex, and especially when the scope does not include specifications but also implementations. This is why when it comes to negotiate an IPR policy, the most important aspect is to understand its scope and its objectives. It was not the point here to address all patent issues or matters around any technology, but to specifically imagine an innovative IPR policy for the building of middleware platform based on Linux for communicating devices. Not having these carve-outs would have created unnecessarily tensions irrelevant to the objectives of LiMo Foundation.

2. Foster collaborative development based on open source principles while being inclusive of all licensing models

2.1 Being inclusive of all licensing models

2.1.1 Inclusive of proprietary licensing and patent royalty-bearing technologies

As already explained, the first important aspect is to define appropriately the platform to promote innovation on the top and down the platform while still offering meaningful software. In the figure below, we can clearly notice the scope of the platform obviously does not include: Applications where operators and handset makers will develop innovative applications for their clients, but also does not include UI (user interface) for the same reason – OS: the platform does not include the kernel itself, we specify some minimum requirements for a Linux Kernel and then each implementer is free to select their own Linux distribution / Hardware: our objective is to define a hardware neutral platform.
In order to implement such a feature in LiMo Foundation IPR policy, the fundamental point is to define and understand each components of the platform, their respective role, the value they potential add in terms of differentiation, and then define what will be the core of the platform and then the additional functionalities which can be add. Important is also to distinguish between the software itself and the APIs, the interface.

So, a contributor will have the choice between 4 licensing models for its contribution: Open source, Foundation Public License Common Capable (patent and copyright free), FPL Non Common Capable (copyright but possibility to charge royalties for patents), or Proprietary. Depending on its choice and depending on the usage of its contribution, then our technical body will decide whether the contribution will become Common Code or not, Common Code meaning the core of the platform, the part of the platform required for compliance as well as benefiting for the strong patent non-assert.

In our picture above normally the framework are expected to be part of the Common Code, Plug-in being normally optional features which can be plugged to a framework. Obviously, only Open source and FPL Common capable contributions are eligible for the core of the platform.

While the contributor is free to adopt the licensing models of his choice, only contributions under a patent and copyright royalty free license which is compatible with other licenses will be eligible for frameworks. To summarize, the LiMo platform has been built around these concepts of Framework and Plug-ins to ensure that innovation under proprietary license and/or patent royalty bearing technologies will be eligible as Plug-ins.

2.1.2 Inclusive of Open source software

At least equally important for LiMo foundation is the ability to work with the most relevant open source software in the mobile field. To achieve it, based on the experience of our members and other sources, LiMo Foundation is working constantly to ensure the coexistence between all types of licenses, incl. open source license which is achievable but requires diligence and realism. Certain open source licenses are sometimes referred as viral, term non-appropriate as open source is a license model amongst other and should be respected as such. Important here is that, similarly to other types of licenses, certain open source licenses have an effect which goes beyond the software distributed under
these licenses, what is called “copyleft”. Depending on the type of software, on the way you combine the open source software and another type of software, on the exact terms of the license, the combined code will or not have to be made available and distributed under the terms of the open source license. This may be critical and generally painted as creating difficulty to combine open source and proprietary.

In reality, it requires a lot of attention to ensure that you are combining software in the right manner. In LiMo, to manage these difficulties, we develop a list of open source licenses, actually two lists, to distinguish between the kernel space (patches to the Linux kernel) and the user space (middleware). Interactions and rules are actually different when you consider each of these spaces separately. Contributions to the kernel will be acceptable under GPL v2.0, while for the moment GPL v2.0 is not an usable open source license for the user space.

We are also currently implementing code scanning tools in order to allow us to manage this coexistence as efficiently as possible and generally to ensure that our members are able to contribute all relevant open source software to become part of the platform.

Finally, this is not only a legal matter, but it is also vital to ensure that you understand the views of the open source community. Certain things may be legal but not admissible for the community, and it is extremely wise to understand those specific requirements and to take them into account.

### 2.2 Foster collaborative development using open source principles

LiMo Foundation decided to a collaborative based approach based on open source principles rather than a “pure” open source approach. Reason is not some “proprietary reflex” but more that disclosing our source code to the public will give opportunity to patent holders to identify very conveniently any possible patent infringements of our code, and then it was decided to give such access only to those who accepts to be bound by the terms of our IP safe harbour, patent non assert.

First, LiMo Foundation decided to create their own collaborative based license: the Foundation Public License (FPL) which is a very similar license to copylefted open source license (modifications should be contributed back in our case), but which is a license limited to the Foundation, under which the source code will circulate within the Foundation while the object will be distributed only under certain conditions to non-members. The copyleft in our FPL is actually stronger than the GPL v2.0 for example: in the latter license, your obligation to give access to your modifications is only when you distribute the software and only to the persons to who you distribute such software vs. in LiMo, it is actually a positive obligation to contribute them back to the Foundation.

This is why interestingly, LiMo Foundation is, to a certain extent, more open source than other initiatives stamped as “open source” but using permissive license, which does not mandate to contribute back its modifications under the same license.

Secondly, our IPR policy is built around this concept that non-differentiating software should be royalty-free from an IPR perspective, and LiMo articulated these principles through its architecture and its IPR policy.
Finally, our platform is composed by many open source components, such as the Linux kernel, gtk, gStreamer ... and we are working now to build strong relationships with these communities and then a mutually beneficial flow of innovation with them. A very usual pitfall when you engage with open source is to fork, to pick an open source software and to modify it without actively ensuring consistency between your own version and the one of the community which evolves. Result is disastrous: negatively perceived by the community as you do not contribute – maintenance as you need to maintain your own version – innovation as you loose the benefits of new enhancements adopted by the community as your code is not compatible anymore with the version developed by the community. This is why it is important to engage really with the relevant community and to discuss with them the modifications you will need, to contribute them to the community and hopefully to have them adopted.

3. Conclusion

LiMo foundation is working in a more complex environment than traditional standards organizations, dealing with the specifications but also the implementation, but the keys for success remain the same: a clear scope and a simple business objective. Once these elements defined, the challenge is to define the IPR policy to achieve such business objective within the scope defined, and while it is quite complex when you enter into the implementation’ field, LiMo Foundation IPR policy is an example of such creativity combining all licensing models in a meaningful way.
EUROPEAN UNION PUBLIC LICENSE - KEY PROBLEMS AND CHALLENGES FOR THE FUTURE

Maciej Barczewski

Abstract

On 9 January 2007 the European Commission has approved the text of the European Union Public License (EUPL v.1.0). It has been approved as a licence to be used for the distribution of software developed in the framework of the IDABC programme. The paper discusses some of the controversial clauses of the License.

1. Introduction

At the close of the last millennium the European Commission became aware of numerous benefits of using Free/Open Source Software (FOSS) for the development of the Information Society. It was argued that open source allows to avoid vendor lock-in and is the key element in implementing interoperability and open standards. Moreover, development methods and the legal framework of FOSS licenses fit well with the requirements of cross-border collaboration and increase the quality of the software while lowering the costs of its development. It was also noticed that European administrations produce many customised applications, that are similar and can be reused in localised versions.

Consequently, in 2004 studies on available FOSS licences that would be adequate for the use by the European Commission were initiated. However, it soon became clear that the previously existing open source solutions did not meet the expectations of EU legal services. Firstly, because of the fact that most of hitherto licences are drafted with American law in mind, especially with reference to used terminology and licensing style, but also to applicable law and jurisdiction. Secondly, above mentioned licences were not thoroughly compatible and the range of their application to derivative software raised doubts. The lack of freedom to possible modification of its content and adapting it for the need of creating official versions of the licence in all official languages of the European Union was a significant obstacle for the Commission to accept any of the existing licences.

For the reasons quoted above the European Commission decided that creating a new licence tailored to EU needs and requirements was necessary. Its draft was worked out within the IDABC programme, in cooperation with the European Commission’s Directorate-General for Informatics and Directorate-General for Information Society and Media. As a result, on 09 January 2007 the

1 Dr. iur., adiunkt at the Faculty of Law and Administration at the University of Gdańsk, Poland. Adjunct Professor at Chicago-Kent College of Law, USA. Attorney-at-law.
2 For example the American notion of “distribution” encompasses the diffusion of copies through the web, whereas the European distribution right concerns only the distribution of tangible copies of the program – see [1].
3 IDABC (Interoperable Delivery of pan-European eGovernment Services to Public Administrations, Businesses and Citizens) is a programme of the European Commission aiming inter alia to create awareness and promote knowledge on Open Source Software in public administrations. Earlier these aims were carried out in the framework of IDA (Interchange of data between Administrations) programme.
European Commission approved the text of the new FOSS licence – the European Union Public License (EUPL v.1.0) – whose aim is to allow the distribution of computer software created by EU institutions and administration organs of member states. Originally the text of the Licence was approved in three equivalent language versions – English, German and French. Exactly a year later, in decision of 9 January 2008, the European Commission approved the text of the licence in the remaining nineteen official languages of EU, trying to take into account specificity of legal regulations in each member state in individual versions.

The EUPL has been drafted taking into consideration European copyright law concepts, as well as the international copyright framework - the rights covered by the license include rights phrased not only in EU terminology, but refer broadly to the right to reproduce, communicate, and distribute, as defined by the WIPO treaties. Moreover, it ensures to the licensee the rights to use the software in any circumstance and for all usage, modify the original software, and/or make derivative works out of it, lend and rent the software or copies thereof, sub-licence rights in the software or copies thereof and, last but not least, obtain the source code of the software from a free access repository.

2. Key problems

It should be noted that during working on the draft of the Licence some regulations included in it raised controversy and doubts among both promoters of the idea of free software, practising lawyers and law doctrine representatives from individual EU member states. They concerned, among other things, duties of licensee resulting from so called copyleft clause and closely connected with it compatibility clause included in point 5 of the Licence.

The EUPL is a “copyleft” licence and, as such, allows the use, modification and distribution of software on the condition that its modifications are distributed under the same terms and conditions. In this way it allows to avoid appropriation of the licensed work by a third party who could sell it as a proprietary work, avoiding at the same time the situation where the European Commission would have to purchase under the terms of a proprietary licence a new version of software originally released under the EUPL licence.

The main weakness of “copyleft” licenses however, is that they are generally not mutually compatible - the more copyleft licences exist, the more compatibility problems are likely to occur. The EUPL intends to deal with this issue by way of a compatibility clause allowing, in certain circumstances, the redistribution of derived works under other licences that are chosen and gathered in an exhaustive list attached to the EUPL.

It must noted that the term “compatibility” in this context means the possibility either to create software on basis of a combination of software distributed under different licences, or, when open source code is used in software, to distribute this latter under another licence. Yet, one must pay attention to the fact that this notion does not encompass reciprocity - merging some code with copyleft licensed code usually means that the “compatible licence” steps aside for the copyleft licence.

The compatibility issue has to be addressed from two points of views: the upstream, and the downstream perspectives. Upstream compatibility depends almost exclusively on the terms and

---

4 General wording of the EUPL allows to use it for the software created also by other entities.
5 Except Irish.
conditions of the upstream licence, and could not be solved in the drafting of the EUPL. Moreover, according to the prevailing view, given the actual drafting of the EUPL, its background and the aims it has to fulfill, it is unlikely that the EUPL will ever benefit from this kind of “upstream compatibility”.[6]

As it was mentioned before, the issue of “downstream compatibility”, has been addressed by the compatibility clause, which contains the listing of licences which the EUPL is compatible to, thus enabling modification and distribution of code licensed under the EUPL under the following FOSS licences:

- General Public License (GPL) v. 2,
- Open Software License (OSL) v. 2.1, v. 3.0,
- Common Public License v. 1.0,
- Eclipse Public License v. 1.0,
- Cecill v. 2.0.6

Fabian Bastin and Philippe Laurent remark, that conflicting situations may arise when a person - who remains licensee under the EUPL and becomes, at the same time, licensor under a compatible licence - will be restricted by the fact he should respect the application of both licences on a particular point. Moreover, one could imagine a situation when the obligations of a licensee under EUPL conflicts with his obligation as licensor under the compatible license, even after the compatibility clause has been applied. In order to prevent those situations the compatibility clause has been complemented, with a clear indication, that in a case when the licensee’s obligations under the compatible licence conflict with his obligations under the EUPL, the obligations of the compatible licence shall prevail.

According to Lucie Guibault and Ashwin van Rooijen, the compatibility clause, although arguably necessary, may considerably diminish the EUPL’s success. Since the compatibility clause only requires a situation of two simultaneous, conflicting obligations to make the compatible licence prevail, even a tiny portion of code licensed under a compatible license will change the licensing obligations for the project. Nonetheless, Rishab Aiyer Ghosh explains that this is unavoidable and although it may indeed limit the extent of software that is available under the EUPL, it will ensure that software initially released under the EUPL is developed and reused further.[8]

In future revisions of the EUPL it will be possible to update the list of compatible licenses. It is advised that the possible extension would concern only strong copyleft licenses used and approved by creators of free software and would cover only licenses used by a public administration of a Member State of the European Community or developers partially or totally funded by the European Community or one of its Member States.[9] It may be expected that third version of General Public License (GLP) would appear in the nearest extension of the list of compatible licenses.

According to Art. 13 the European Commission may put into force binding new versions of the License, so far this is required and reasonable. Such clause raised concerns as regards the

---

6 Criteria of the choice of the five licenses in the clause were as follows: firstly, only licences that were popular and widely used were taken into consideration, secondly non-copyleft licences were discarded of (eg. Apache License, BSD License), and finally “weak copyleft” licences or licences with a copyleft effect which does not extend to linkage were disposed of (eg. Mozilla Public License 1.1) – see [7].
Free/Open Source nature of the license, however, in the statement issued later the significance of the criterion of being “required and reasonable” was stressed:

- "required" means that the European Commission may update the licence to address new legal or technological issues that would otherwise keep the licence from functioning as intended,
- "reasonable" means that a new version will not change the fundamental characteristics of the licence, such as the freedoms it grants, the liability exemption, or its reciprocal (or “copyleft”) character, meaning that the exclusive appropriation of the licensed work will not be authorised.7

The application of the above mentioned criteria reduces doubt concerning the possibility of unilateral imposing of new version of the license by the Commission. It must be noted here however, that multiple translators of the EUPL questioned the validity of such unilateral modifications of contractual obligations, facing their national law. Moreover, adding last EUPL version in the compatible license list would be recommended.

The problem of conformity of the regulations in the License with a national law also appears with regard to widely defined disclaimers of warranty and liability included in art. 7 and 8, and also expressed in art. 2 possibility of waiving of moral rights8 and exercising rights granted by the EUPL on any media, supports and formats, whether now known or later invented.9 However, it is assumed that the regulations mentioned above would be enforceable only to the extend allowed by a national law.

3. Challenges for the future

The problems discussed above do not cover all spectrum of doubts connected with application of the first version of the European Union Public License – the scope of the license’s application with reference to the Application Service Provider (ASP) model of software distribution is not clear, it does not refer to the problem of use of Digital Rights Management systems, doubts concern also interpretation of some definitions used there. Yet, the fact that for the first time a public administration body of the size of the European Commission by an official decision published an open source license to use it in order to distribute some of its own software cannot be overestimated. Such activity is a precedental political signal and, without generating any obligation, will be an exemplar for other European administrations and organizations to use open source software. For this reason approval of EUPL should not be treated as an aim itself but as significant means to reach guidelines contained in eGovernment Action Plan i2010.

The next essential step will be approval of the EUPL by the open source community. Only when the license is widely used will the aim to reinforce legal interoperability by adopting a common

---

8 One could consider encompassing the moral right to remain anonymous (not revealing authorship) in future versions of the EUPL. However, it should be evaluated whether an exercise of such a right would not collide with other principles of the distribution of an EUPL-licensed software.
9 For example, according to art. 41 of the Polish Copyright and Neighbouring Rights Act of 1994, economic rights can be transferred (licensed) only with reference to modes of exploitation of works mentioned explicitly in the contract (license) and known at the time of conclusion of the contract (licence). Since future versions of the EUPL may introduce different modes of exploitation and since they will be automatically binding to the Licensee, this provision of Polish law will conflict with the EUPL. One of the possible solutions to this conflict would be to allow the Licensee to choose and indicate which version of the EUPL applies to the provided Work or Software.
framework for pooling public sector software which is contained in the License preamble be reached.

4. References


OPEN SOURCE SOFTWARE POLICY

Benoît Müller¹

Abstract

Software is among the most innovative of industries, and software innovation is largely driven by the private sector. Innovation can occur under a variety of development and business models. Indeed, BSA members develop and deploy open source, proprietary and mixed solutions. BSA favours a diverse software ecosystem that enables users to select the solution that best meets their needs.

Government can help facilitate software innovation through neutral policies that promote competition and choice. Specifically, we believe governments should:

(i) Select software on its merits, not on its method of development. Public entities should procure software based on functionality, performance, security, value and similar neutral criteria.
(ii) Ensure that publicly-funded research is available to all.
(iii) Promote voluntary, industry-led standards and interoperability solutions. Government policy on software standards should not favour any particular development model.
(iv) Maintain strong intellectual property protection consistent with the principles of neutrality. Policy makers should not make specific IP licensing choices a precondition for eligibility for procurement.

¹ Director of Software Policy, BSA, Brussels. E-mail: BenoitM@bsa.org.
IP INFRINGEMENT IN INTERNET - A TORT OR A CRIME?

Michal Koščík1

Abstract
A decade-long fight of IP-rights holders against internet piracy and P2P networks gave rise to plenty of new laws, directives and court decisions all over the world, but did not bring any tangible success in uprooting this piracy. The focus of IP rights holders and their associations was shifting from individual users towards online service providers and P2P software producers, what lead to decline of several major P2P networks and servers. Despite winning legal battles against online service providers such as Napster or Torrent-spy, IP holders are still losing their war against piracy and are turning their focus back on the individual file-sharers and recently, on the providers of internet connection.

However, it seems that the rights holders cannot cope with the problem of internet piracy alone and that the state authorities will have to play a bigger role in copyright protection. This means that a bigger emphasis on criminal liability for internet piracy is a likely trend in the future. This trend will be even more propelled by the International Convention on Cybercrime.

In the current situation the lawmakers and judicial institutions have to find the reasonable and just balance between the responsibilities of parties involved in illegal file transfers, rights of internet users and rights of copyright holders, between the criminal and civil liability of the offenders and to decide about the intensity of intervention of state authorities.

This paper should give brief description of current status quo of user’s, ISP’s and OSP’s liability in light of EC legislation and ECJ case-law and in several cases and compare it with the North American approach. However, the main focus and contribution of this paper is to analyze upcoming trends in battling internet piracy and their impact on legal sanctions for conducting or assisting breach of IP-rights in cyberspace.

1. Civil or criminal liability? - Criminal sanction as an “ultima ratio”

Criminal law is an integral part of every legal system which serves as a deterrent factor for anybody who would be tempted to breach most important rules of the system and thus threaten the most significant values of the society. The practical problem lies in the task to define which rules and values are so important to be protected by the criminal law. The theory of criminal law honors the principle of “ultima ratio” – the principle of last resort. In other words, this principle sets forth that the criminal law should be applied only where the other means of protection were not sufficient. The same principle applies once again when deciding about the severity of punishment for misconduct when the heavier punishment should be imposed only if a lighter punishment doesn’t meet its purpose.

When talking about the suitability of criminal sanctions for copyright infringement, we have to identify whether such infringement violates or endangers values which deserve to be protected by criminal law and, with respect to the “ultima ratio rule”, whether these values cannot be protected effectively by other legal means.

1 Masaryk University, Brno, CZ.
2. Copyright as a part of private law

2.1. Measures of civil law

Modern consider the private property to be one of the basic elements of the market system and thus one of the basic prerequisite of smooth functioning of the society itself. The private property is therefore considered to be worth protection by state, its authorities and legal regulations. The intellectual property recognized as a “sui generis” branch of private property is traditionally protected by regulations of both private and public law.

Since the copyright is traditionally considered as a part of private branch of law closely interconnected with the civil law, it seems strictly logical that the owner of a copyright right would try to enforce his rights by means of civil procedure. When we look closely at the legal instruments that copyright holders can use to protect their rights, we’ll find out, that they usually have wide range of options. In most jurisdictions, it would be common that the owner of copyright would have an option to apply for an injunction aimed at prohibiting the continuation of the infringement, against the violating party or seek damages. The public apology of offender, publication of a decision, allocation of legal costs, compensations and remedies are other legal tools that copyright users may use under most of world’s jurisdictions. A duty to require information such as the duty of infringer to inform of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution which is applicable e.g. in WTO countries or members of European Union or measures for preserving evidence stated in article of TRIPS agreement or article 7 of 2004/48/EC are undoubtedly other legal institutes which are strongly in favour of copyright holders’ interests and which improve his position in enforcement of his rights. Moreover many jurisdictions provide protection also for the means of digital rights management by prohibiting circumvention of DRM or disseminating tools for DRM circumvention.

When we look at the plenty of options that copyright holders have to protect their legal interests, we can ask ourselves a question whether it is really necessary to have more protection of intellectual property rights by the means of criminal law, which should be applied only when the other norms fail to give enough protection. To answer this question we have to analyze how efficient these tools are in real life, in other words, we must ask whether copyright holders really manage to protect their rights via civil cases.

2.2. Efficiency of civil measures

Legal tools described in the previous chapters can be undoubtedly useful and efficient in most of copyright infringement cases, however the practical experience showed, that they lack any efficiency when protecting copyright against so called “internet piracy”.

The phenomenon of copyright piracy existed long before the speed of internet lines and progress in compression of audio and video formats enabled users to download songs, movies and computer

---

2 E.g. Rei-vindicatio – action establihed in roman law
3 E.g. theft.
4 E.g. Article 46 of TRIPS
5 Due to article 47 of TRIPS
6 As a result of implementation of article 8 of the Directive 2004/48/EC
7 e.g. the article 6 of EU directive no 2001/29/EC binds member states to „provide adequate legal protection against the circumvention of any effective technological measures ...” and to provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which are promoted, advertised or marketed for the purpose of circumvention of, or have only a limited commercially significant purpose or use other than to circumvent, or are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.
programs, however these advances in technology made the problem of piracy so obvious that it required immediate response from the stakeholders of so called “creative industry”. Their response was not primarily aimed at the individual “pirates” but at the providers of services and authors of computer programs that enabled users to share and download media files. This strategy seemed to be successful when representatives of copyright holders forced major providers of P2P services to restrict their activities to distribution of purely legal content, until it has came out that P2P networks are like mythological hydra, a creature with several heads that cannot be beaten because if one of its heads is severed another (or two of them) would grow in its place. The community of users of 2P2 networks has proven to be independent to individual servers, programs or services because the users could quickly find an alternative source of illegal downloads if any of the sources declined.

Even though the civil procedures against providers of services related to P2P led to adjudication of high damages or to the restriction of activities of individual providers it didn’t in fact deter other subjects from establishing new file-sharing servers or develop new P2P clients. The users of these services weren’t distracted either, since a closing down of an individual service was for them rather a nuisance than as a serious obstacle in accessing illegally shared content. A conclusion can be made that even though civil measures proved to be very successful when enforcing rights against individual infringer they failed distract other infringers and thus failed to protect rights copyright holders. Is is obvious that current copyright schemes and regulations alone cannot uproot the problem of computer piracy so the changes in copyright regulations seem to be unavoidable. These changes can take place either by amending current copyright regulations or by emphasizing criminal liability of infringer.

3. Internet piracy in light of criminal law

3.1. General overview

Despite the fact that the criminal prosecution of internet piracy is becoming more usual in the positive law this area is still far from settled. Whereas WTO members implemented a criminal prosecution of copyright infringement on a commercial scales the European parliament warned that criminalising consumers who are not seeking to make a profit is not the right solution to combat digital piracy. It seems that there exists a major opinion that only the “dangerous” pirates should be prosecuted instead of “harmless individuals”. The stance of European parliament is in consonance with the stance of United States Department of Justice which concludes that Criminal copyright penalties have always been the exception rather than the rule. Although criminal copyright law has greatly expanded the scope of the conduct it penalizes over the past century, criminal sanctions continue to apply only to certain types of infringement—generally when the infringement is particularly serious, the infringer knows the infringement is wrong, or the type of case renders civil enforcement by individual copyright owners especially difficult. This generosity to individual users who share files in small amounts is apparent from both international conventions and national regulations. However national regulations differ when it comes to setting a border between minor and major copyright piracy. The border between criminal and non-criminal

---

8 http://www.pantheon.org/articles/h/hydra.html
9 bit commet
12 TRIPS and Convention on cybercrime relate only to copyright infringement on a commercial basis
act is usually formed by a financial threshold, extent or duration of copyright infringement\(^{13}\), or the motive of infringer (i.e. whether infringer infringed copyright for a commercial gain) or combination of these three elements.

**3.2. Internet piracy in light of the Convention on Cybercrime**

The Convention on Cybercrime, which was adopted in September 2001, put copyright piracy on a list of “cybercrimes” which its signatories bound themselves to combat among other crimes such as frauds, forgery and child pornography. The signatory countries bound themselves to establish criminal offence of violation of copyright [article 10 (1)] and copyright related rights. [article 10 (2)]. Many signatory states had however already enacted criminal prosecution of copyright infringement before signing the convention. The article 61 of TRIPS agreement has bound all WTO members to *provide for criminal procedures and penalties to be applied at least in cases of willful trademark counterfeiting or copyright piracy on a commercial scale*. There is virtually no difference between the provisions of the Convention on Cybercrime and the TRIPS agreement since the Convention on Cybercrime restricts itself to acts that are committed *willfully, on a commercial scale and by means of a computer system*. The restriction of a duty to criminalize only those acts that were committed by means of a computer system seems logical however it has a sense only for signatories which are not members of WTO\(^{14}\). This fact is also admitted by explanatory report on the Convention on Cybercrime which states that its provisions are *in line with Article 61 of the TRIPS Agreement which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale"*. Moreover, signatories of both documents are not limited to restrict criminal liability only to the piracy on a commercial scale. It is apparent that the substantive provisions of the Convention on Cybercrime did not bring any new element to the international protection of copyright, however the provisions of the Cybercrime Convention about copyright infringement could be efficient in case it is signed by a non-WTO member such as Russia\(^{15}\). It is also possible that the signatory states would reevaluate their current provisions on copyright protection when implementing the Convention despite the fact that they had already met the convention’s minimum standards by implementing TRIPS.

It seems that the procedural provisions of the Convention on Cybercrime will have much bigger influence in the development of intellectual property rights than its substantial norms since it establishes a rather complex framework of international cooperation in the field of cybercrime. In article 23 the signatory states agree to cooperate “*to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*” and this commitment is only boosted by commitment of mutual assistance in investigation and collection of evidence in the article 25. It might be possible that the copyright holders will take advantage and try to initiate criminal procedures to deter achieve some exemplary punishments and take advantage of deterring function of criminal prosecution.

\(^{13}\) for example, the US Code considers as a criminal offence “the reproduction or distribution, including by electronic means, during any 180–day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000”, or an infringement ) for purposes of commercial advantage or private financial gain – see USC §506.

\(^{14}\) however all the states which have ratified the convention are WTO members.

\(^{15}\) However, Russia has not signed the Convention yet
3.3. Civil or criminal liability – conclusion

It seems that the upcoming period will bring bigger emphasis on criminal prosecution of computer piracy in the positive laws of individual states, since copyright owners failed to protect their rights in civil procedures. Only the future will show whether this approach will bring better results, however it could be doubted because strong criminal prosecution of piracy doesn’t have full support of neither political elites, nor members of society. It can be assumed that in case of eventual failure of this approach could lead to further reevaluation and improvement of owners’ position in civil procedure or to the revaluation of fundamental principles of copyright law.

4. Current trends in liability of computer piracy participants

4.1. Current trends in liability of internet users

Despite the fact that the vast majority of “ordinary” users of P2P (or other) services who breach the copyright are under most jurisdictions subject to both civil and criminal liability, they have not been in the focus of copyright holders’ enforcement and their acts were still rather pardoned by state authorities. Copyright holders have focused mainly on the providers of internet services due to the disparity between difficulties in proving an infringement of individual users and perspective financial compensation.

However it is likely that an increase of amount of suits against individuals will become a trend in the upcoming period as it can nowadays be seen in USA where it is possible to claim statutory damages between $750 to 150 000$ without trying to prove actual damages\textsuperscript{16}. These damages can reach multiplies of actual damages and their height is capable to discourage individuals from file-sharing and encourage owners to enforce their rights. With such high statutory damages it remains questionable, whether more protection from the criminal branch of law is still needed.

This trend is likely emerge in the EU member countries as well, and can be supported by implementation of the directive 2004/48/EC which presumes the possibility of statutory damages\textsuperscript{17} and improves the copyright owners’ position in civil procedures by setting forth the rules on obtaining information and evidence. Both 2004/48/EC directive and regulation of US Code presume a mitigation of damages for so called “innocent infringers” who have infringed copyright without actual knowledge of infringement eg. by using P2P software without being aware of the fact that it simultaneously shares downloaded content.

The Convention on Cybercrime, which is only applicable to copyright privacy on a commercial scale, can paradoxically cause some changes in the criminal provisions regarding individual infringers because the signatory states may decide to reevaluate their copyright policies in the process of ratification of the convention.

4.2. Trends in responsibility and liability of internet service providers (ISPs)

The internet service providers have been in constant legal war with copyright holder’s representatives for more than a decade. Whereas there had been no doubts in cases of direct

\textsuperscript{16} see 17 U.S.C. § 506(a)
\textsuperscript{17} see Article 13 - 2004/48/EC as an alternative to (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question.
copyright infringement of ISPs, the indirect infringement of ISPs still remains unsettled despite several milestone decisions like rulings in Napster, Gorkster and Amister cases. The procedures against producers of P2P networks and programmers of P2P clients have led only to a better legal awareness of computer pirates who have quickly learned how to develop software which could get easily out of its creators control to be “abused” by certain users. These creators could be held liable only when they are convicted to create such software with pure intention to infringe or aid with infringement of intellectual property which is almost impossible since almost every such application can be used for legal purposes.

The attention of both copyright holders, state authorities and academics is focused on the liability of providers of online services which enable users to exchange information and upload user content such as torrent servers or video-streaming sites. These servers give enormous challenge to both criminal and civil lawyers.

From the criminal law point of view, these servers operate on a commercial basis and it is apparent that individual users would not be able to seriously infringe any intellectual property if these services didn’t exist. It is however difficult to prove that providers willfully aid its users to infringe intellectual property especially when they cooperate with copyright holders and erase illegal content upon request. On the other hand it is hard to believe that these providers are not aware about the huge amounts of illegal content on their servers and it will be always questionable whether they are really doing all what is necessary since they can generate profits from infringing\textsuperscript{18} content as well.

From the point of view of civil law, the question is, how should copyright holders be reimbursed for losses they gain from the functioning of a service which follows the applicable laws or utilizes safe harbor regimes. I dare to say that key to this answer is to improve enforcement of damages on individual users who are primarily responsible for uploaded content and to put more emphasis on criminal prosecution of copyright infringers on a commercial basis.

\textsuperscript{18} I dare to say that infringing content is the major source of income of some services
RESOLVING IP DISPUTES ON THE INTERNET –
IS A COURT LITIGATION THE ONLY OPTION?

Justyna Ożegalska-Trybalska

Abstract
ADR for domain names take into consideration circumstances specific for the Internet alternative
dispute resolution proceedings are characterised by the relatively low costs and short time needed
for issuing a decision on a dispute. ADR offers high expertise of arbitrators who are specialists in
IP and Internet law and combines academic knowledge and practical experience relevant to subject
to the dispute. Alternative systems for resolving domain name disputes create an attractive platform
for resolving cross-border domain-name disputes, involving parties from different countries. In this
regard, significant problems with determination of jurisdiction and choice of law in disputes
involving infringement of rights on the Internet are effectively eliminated.

1. Introduction

The rapid development of Internet technologies over the last decade has had a significant impact on
national intellectual property (IP) protection systems. A virtual world provides new means and new
territories for infringement of IP rights. Next to copyright, trademarks and other distinctive signs are
most often targeted on the Internet through unauthorized use by third parties and are the subject of
unfair on-line commercial practices.

Usually, when somebody’s rights are being infringed, national court litigation is considered to be
the only way of resolving it. Territorially based juridical systems are, however, not always the most
effective option for resolving disputes occurring on the Internet, since they usually extend beyond
local borders and - due to the technological context – present specific features not relevant from the
point of view of traditional IP regulations. In that context, the following question arises: is litigation
before a relevant national court always the only and best option for resolving conflict taking place
in virtual world? If not - what are the alternatives?

This paper will investigate these issues by presenting co-called Alternative Dispute Resolution
(ADR) systems as an effective way of enforcing IP rights on the Internet without the need for going
to court, as well as answering some questions: why opt for ADR in IP disputes rather then use
ordinary judicial systems; what is the legal framework for ADR policies related to Internet disputes;
and what are the advantages of using them? This will be achieved through reference to ADRs for
resolving disputes between owners of distinctive signs and domain name registrants, which are
often mentioned as a good example of a successful mechanism for resolving on-line disputes.

1 Intellectual Property Law Institute, Jagiellonian University, Krakow.
2. Infringement of IP rights on the Internet

The Internet has become a cheap, easy accessible platform for promotion and advertising activities, which necessary involve use of trademarks and other distinctive signs (trade names, company names, abbreviations). Modern on-line technologies create a rapidly growing market for new forms of infringement of rights to protected commercial designations, which result in a distinct increase in the number of internet-related disputes.

The most common way of targeting trademark rights on the Internet is through unauthorised exploitation of somebody’s trademark as domain name. Domain names are user-friendly forms of Internet addresses which, in order to be easily remembered by Internet users, usually correspond to characteristic commercial designations. As practice shows, such disputes are not always susceptible to effective resolution under national regulations before common courts, for a number of reasons. First of all, trademarks enjoy territorial protection, while trademark infringement on the Internet lacks any territorial barriers. This creates difficulty for legitimate rights-holders of having legal grounds for initiating court proceedings in all countries of potential infringement, as well as creating the problem of avoiding high costs of enforcing trademark rights in a number of jurisdictions.

Moreover, the forms of unauthorised use of trademarks in domain names differ from these being prohibited by traditional trademark regulations. As a result, some unfair practices related to abusive use of trademarks on-line, such for example co-called ‘cybersquatting’, cannot be successfully targeted before national courts.

Finally, as in the case of any infringement that occurs on international level, it is always difficult to determine applicable law and jurisdiction.

As a result of the growing number of conflicts between domain name holders and owners of IP rights from the one side, and limitations in using juridical systems and ordinary IP regulations from the other side, alternative resolution systems have been established for resolving disputes over generic and country domain names. Practice has shown that, in many cases, private dispute resolution mechanisms for domain names allow the effective protection of trademarks and other protected signs on the Internet.

3. Alternative Dispute Resolution over IP on the Internet – why to opt for it?

Alternative Dispute Resolution (ADR) mechanisms, successfully used in international and commercial disputes as an alternative to court litigation, are now considered as a very effective way of resolving disputes over infringement IP right on the Internet, in particular disputes over the unauthorised exploitation of trademarks in domain names. All ADR procedures such as negotiation, mediation, and arbitration are eligible for use in the mentioned disputes.

A mediation is a voluntary dispute resolution procedure in which a mediator, at the request of parties to the dispute, assists them in reaching common satisfactory settlement of the dispute. By choosing mediation, the parties do not lose control over the resolution process and have influence

---

2 For more information on dispute resolution for domain names see Guide to WIPO Domain Name Dispute Resolution, WIPO Arbitration and Mediation center, available at: http://arbiter.wipo.int.

3 Alternative Dispute Resolution is the term for the ways used by the parties to solve conflicts without traditional Court litigation, but with the help of an independent third party.
on it, until signing a final settlement. Parties can together agree settlement which ensures their interests.

Arbitration, which is especially widely used in domain-names disputes, is more formal and can be initiated only on the ground of a signed agreement between parties, under which a dispute is submitted to an independent arbitrator (or panel of arbitrators). Even though parties have influence in choosing an arbitrator, they have no influence on the final award, which is binding for them.

Even though ADR systems for domain-names disputes differ from each other, they have many common features, making them a very attractive alternative way of resolving conflicts involving IP rights.

As opposed to very formal court litigation proceedings, the discussed ADRs involve minimum formal requirements. An ADR procedure is usually conducted on-line with the help of various on-line tools (on-line samples of Complaint, Response), without any need to visit a courtroom. The other advantage of decisions issued by arbitrators is that they are based not only on formal grounds, but all facts and circumstances of the case, including those typical of and crucial for infringement of IP on the Internet. Moreover, in the case of alternative mechanisms, court litigation involving many procedures in different jurisdictions is replaced by one simple ADR procedure.

The effectiveness of the ADR systems is guaranteed by a mandatory character of the procedure on the part of the domain name registrant derived from a registration agreement and easy enforceability of the decision by the registrar. The registrar also guarantees that after he/she is formally notified of a dispute, it blocks transfers of disputed domain name, which makes the alleged infringer unable to transfer the domain name to any third party.

Comparing to traditional court litigation, ADR systems are very attractive in terms of both length of proceeding and the costs involved in resolving a given dispute. Final decisions are usually issued after between one and two months, and cost are costs substantially less than the costs of litigation before the courts.

Finally, which is particularly important for IP right holders, remedies available under ADR policies usually involve the transfer of the disputed domain name registration to the complainant.

4. Uniform Dispute Resolution Policy and other ADRs system for domain names

At the moment a great number of ADR systems for domain names are in operation all around the world. Next to “international” ADR systems applicable to most generic top Level Domain Names (com, .org etc) which are governed by the Uniform Domain Name Resolution Policy, national registrars have implemented different models for resolving disputes over country code domain names (.de, .eu, etc). Some internal arbitration is conducted by a registry of country domain names (e.g. ADR of Nominet UK for disputes in the UK), others by an independent dispute resolution provider (e.g. ADR for .eu provided by the Czech Arbitration Court). There are also countries, like Germany, where there is no alternative to court litigation in disputes over domains ending with .de.

---

6 Detailed information on UDRP and national ADR systems can be found in: BETTINGER. T: Handbuch des Domainrechts. Nationale Schutzsysteme und internationale Streitbeilegung, München 2008.
4.1. Uniform Domain Name Dispute Resolution – UDRP

The most popular ADR system for resolving domain name disputes operates under the Uniform Domain Name Dispute Resolution Policy (UDRP) adopted by Internet Corporation for Domain Names and Numbers (ICANN) at the end of 1999. UDRP is an expedited administrative proceeding for the resolution of disputes arising from abusive registration and use by third parties of domain names corresponding to their protected trade marks. UDRP is mandatory for disputes over most Top Level domain names, such as: .aero, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel. It is also used voluntarily for certain country codes Top Level Domain Names.

UDRP has been designed mainly to disputes involving already mentioned cybersquatting, which is a term for bad-faith registration of domain names corresponding to trademarks (or other distinctive signs) by third parties not having rights to them, with the sole purpose of profiting from the sale of such domains.

The main problem that courts all around the world have faced while fighting with cybersquatters were difficulties in applying national trademark regulations to this unfair practice. Traditionally, a right to a trademark is infringed when an allegedly infringing sign is used in the course of trade for identification of goods or services, which causes the likelihood of confusion among customers. Meantime, typical cybersquatters only register domain names identical or similar to protected trademarks, without using them for active, commercial web sites and for identification of any goods and services. Moreover the bad-faith characteristic for the activities of domain name pirates is not recognised as an independent ground for determining trademark infringement.

The purpose of implementing UDRP was aimed at removing this gap and provides trademark owners with an effective, not costly and fast way of resolving disputes involving their trademarks. According to UDRP, the holder is required to submit to an administrative mandatory proceeding under the UDRP if a third party (complainant) asserts that:

1) A domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and 2) the holder of said domain name has no rights or legitimate interests in respect of it; and 3) the domain name has been registered and is being used in bad faith.

From the very beginning of its establishment, UDRP is probably the most frequently-used mechanism for resolution of domain-name disputes. Since the beginning of 2000, when the UDRP system was launched, approximately 12,000 cases have been filed under UDRP only in WIPO Mediation and Arbitration Centre which, next to the Asian Domain Name Resolution centre and the National Arbitration Forum, is an authorized provider of UDRP resolution services.

Conducting a UDRP proceeding is not cheap, but neither is it as costly as court litigation. The fee charged by WIPO for a proceeding involving up to five domain names is $1500.

Despite the popularity of UDRP as a way of resolving conflict over domain names, and not questioning the advantages of this system compared to traditional court litigation, there are a number of issues that can be considered as ‘disadvantages’ of this resolution policy in comparison with traditional court litigation.

Firstly, decisions issued under this policy are not binding on national courts, which may resolve dispute in a different way. Decisions issued under UDRP are binding only to domain name
registrars and do not stop parties from resolving a dispute before the traditional courts. This creates legal uncertainty in regard to final decision. Secondly, no damages are available. Thirdly, a panellist has no power to issue emergency injunctions, which in some situations might be considered an important disadvantage of UDRP.

4.2 ADR for .eu

Relatively speaking, the newest ADR system has been introduced on the European level for disputes arising with the registration and use of the .eu country code domain name for the European Union. It operates under ADR Rules and ADR Supplemental Rules established in line with the Public Policy Rules for .eu of the European Commission (EC Regulation 874/2004). They apply to disputes over signs, in respect of which a right is recognised or established by the national law of a Member State or/and Community law. The conditions under which conflicts between trademark owners and holders of an .eu domain name are disputed are very similar to those implemented by UDRP: 1) the disputed domain name is identical or confusingly similar to the name in respect of which a right is recognised or established by the national law of the Member State or/and Community law, and either 2) the disputed domain name has been registered without rights or legitimate interests, or 3) the disputed domain name has been registered or is being used in bad faith.

The dispute resolution provider for disputes over .eu is the Czech Arbitration Court. Decisions issued by the Arbitration Court are final, not subject to appeal and compulsory to the parties. Parties can initiate a court proceeding which will have consequences to the implementation of the decision. In any case, proceedings are terminated if, before their end, a dispute is finally decided by the court of a competent jurisdiction or other ADR body. The available remedies are: annulment, transfer, revocation, attribution of .eu domain name.

On the one hand, ADR procedure for .eu is more formalised than UDRP, which can be considered by parties as a disadvantage. On the other hand it is fully conducted via an on-line arbitration platform, which is a convenient way for ‘participating’ in resolution proceedings. Parties have the freedom to choose the language of the proceedings, which is an attractive aspect of this resolution process not available in national court litigations. The ADR proceeding for .eu is conducted for reasonable fees which, for a dispute involving up to 2 domain names carried out by one panellist, is 1850 euro.

4.3. ADR for .pl

An interesting ADR framework for domain names disputes has been established for .pl domain names. In Poland, there are three independent ADR systems for resolving disputes over .pl domain names. Most disputes over IP rights infringed by the registration and use of domain names with .pl endings have been resolved by the Arbitration Court for Domain Names at the Polish Chamber for Information Technology and Telecommunications.

Unlike the UDRP, the scope of application of which only covers domain registration in bad faith, the Polish alternative dispute settlement proceedings apply to all disputes resulting from the infringement of third-party rights by the registration and use of domain names (including infringements of right of protection for a trademark, unfair competition law, personality rights and firm name rights).
Disputes are subject not to a special regulation on domain names but to substantive Polish law, procedural rules of arbitration court and procedural provisions concerning arbitration system of civil procedural code. Both mediation and arbitration stages are available. The parties to the dispute are free to conclude a settlement before the arbitrator at any stage of the arbitration proceeding. The arbitration decision is binding to the parties and has the same legal effect as a court decision. There is no right to appeal against the decision, which is definitely a disadvantage compared to court litigation which provides stages of appeal.

Remedies available before the Polish arbitration court for domain names are limited compared to other ADR system for resolving domain-name disputes. The only remedy is a court statement that registration and use of a disputed domain name has infringed the claimant’s rights, which is a basis for terminating the registration agreement with the domain name holder. Such a model definitely lacks the attractive consequence of opting for ADR: the transfer of an infringing domain name to a legitimate right holder.

The arbitration fee of approximately 500 euro for one domain name is easily affordable, and is definitely much lower than costs of conducting litigation before a court.

5. Conclusions

As shown above, ADR systems designed for resolving disputes over infringement of trademark on the Internet surely provide trademark owners with an effective tool for enforcing their rights on the Internet and, in many cases, are more attractive in terms of time, costs, and remedies available, than traditional court litigation. There are a number of reasons why a party, whose intellectual property is being targeted in the virtual world, should consider using relevant ADR policy rather than going to court.

Firstly, bearing in mind that ADR for domain names take into consideration circumstances specific for the Internet that have no decisive significance from the point of view of substantive law, they often ensure more adequate protection of IP rights (mainly trademarks) than traditional provisions of trademark and unfair competition law.

Secondly, in opposition to formal, expensive and durable proceedings before common courts, alternative dispute resolution proceedings are characterised by the relatively low costs and short time needed for issuing a decision on a dispute. This is of special importance considering that consequences of trademark infringement, defamation, misleading of Internet users by “false” domain name may be particularly acute on the Internet.

Thirdly, ADR offers high expertise of arbitrators who are specialists in IP and Internet law and combines academic knowledge and practical experience relevant to subject to the dispute.

Fourthly, most domain-name ADR policies provide claims either to cancel registration of an infringing domain name or to transfer it to the holder of the IP right which has been infringed from the registration and use of domain name. It is important to mention that the accomplishment of such claims is not always possible within the limits of traditional IP regulations and common court proceedings.

Finally, alternative systems for resolving domain name disputes create an attractive platform for resolving cross-border domain-name disputes, involving parties from different countries. In this regard, significant problems with determination of jurisdiction and choice of law in disputes involving infringement of rights on the Internet are effectively eliminated. In the case of a domain-
name dispute which is subject to ADR proceeding, a ‘court’ competent for resolving the dispute is the relevant dispute resolution provider.

6. References


ON THE GRAMMAR OF PATENT CLAIMS

Georg Jakob and Hartmut Pilch*

Abstract
At the heart of the patent system lies something both patent law and international treaties give less attention than it actually might deserve: Patent claims are the very essence of every patent, defining the exact scope of the exclusive rights the patent holder is granted. Generally outlined at best by legislation and often neglected by the courts, patent offices and patent lawyers have developed their own grammar, syntax and logic of how these exclusive rights are to be formulated. This paper suggest that some aspects of the patent system currently perceived as problematic - from patents on software to patents on life, from Amazon’s gift-ordering to Monsanto biotec patents - have their root in some peculiar features of the language used in patent claims and its use established by patent offices and patent attorneys.

1. The Patent System in Crisis?

There are at least two issues on which the patent system has become subject to criticism from experts and also suffered severe backlashes in public opinion: So called biotechnical patents and patents on software. Both have been granted by the European Patent Office (EPO) since the 80ies and early 90ies, both have been heavily criticised on ethical as well as legal grounds, among the main arguments being their violation of Article 52 respectively 53 of the European Patent Convention (EPC). A legislative approach of ex-post justification was perceived to be enough to resolve this dilemma. And so, after being rejected in 1995 by the European Parliament (EP), the directive 98/44/EC on the legal protection of biotechnological inventions was finally adopted in 1998 in its second reading despite continuing concern across Europe. However, the second attempt to legalise a questionable EPO practise, the directive proposal COM (2002) 92 on the patentability of computer-implemented inventions, trying de facto to abolish the provision of Art 52 (2) (c), which excludes programs for computers as such from patentability, was finally rejected by the EP in its second reading on 6 July 2005 with a large majority of 648 votes. Efforts of rewriting that decision by various procedural backdoors like the Community Patent or the European Patent Litigation Agreement have been put forward ever since, while, as we will see on the following pages, the EPO simply continues its practise without significant change.

Some might see one issue as being more important than the other, but both are closely related. While one is about patents on life, the other is about patents on mathematical instructions, therefore on human thought processes [14], p 32. Although sometimes a major problem is identified in such patents as generally being too broad, with no clearly defined boundaries [1], p 46 ff, this is not necessarily

*Hartmut Pilch is the Founder of the Foundation for a Free Information Infrastructure e.V., Blutenburgstr. 17, 80636 Munich, and was its president from 1999-2005. Both he and Georg Jakob are current board members of the FFII. email: gjakob@ffii.org, phm@ffii.org
always the case. As we will see, some of the claims in question are quite specific indeed. The problem is rather that these claims contain subject matter excluded from patentability and no novel inventive teaching.

2. Some Patent Basics

2.1. Description, Claims and Infringement

Before we start our analysis, it is important to recall the basic architecture of a patent once more. Every patent consists of a detailed description, often some drawings and one or more claims. While the technical description and the drawings help to understand the details of an invention, these claims are the really interesting part, since they are exactly defining the monopoly of the patent holder who is entitled to ban (or collect license fees from) everybody else from using anything that is mentioned in the claims.

![Figure 1. Patent claims](image)

Some national legislations treat patent claims in more or less detail than others (the most detailed perhaps being § 9 of the German Patentverordnung, but cf also Rule 43 of the Implementing Regulations to the Convention on the Grant of European Patents), but a common requirement is that they should be clear and concise as well as supported by the description (cf Art 84 EPC). Usually, they briefly summarise the state of the art regarding a particular invention and then, introduced by "characterised by" or "comprising" contain those elements that the applicant deems his essential invention [10], p 148. A typical patent claim looks like this:

- A process and/or apparatus (of patentable subject matter) consisting of (state of the art), comprising...
- ...an inventive step (that is being disclosed, i.e. a novel teaching) of industrial application.

There are independent and dependent claims, the latter of which refer to other claims. It is important to keep in mind though, that a patent can already be infringed by violating only one single claim. If the defendant does not use the claim features identically or does not use all claim features, infringement might still lie in what is called equivalent use (BGH 28 IIC 795, 1987 - Formstein). Some arguments developed in this context are considered "obscure teachings" by individual scholars [8], [10], p 182...
and a more detailed analysis of this discussion would likely exceed the purpose of this article; suffice to say, in a worst case scenario, any single patent claim can have the effect of the whole patent. Therefore, every patent with only one claim on a computer program as such is in essence a patent on a computer program as such. In other words, any patent containing even one program claim has to be considered a software patent in violation of Art 52 (2) EPC. Likewise, any patent containing just one claim on natural properties of an organism can be seen as a patent on life.

In the US, patent applications have been filed containing more than 1.000 claims. At the EPO, such applications are usually rejected or split into up to 26 separated applications [11], p 12.


A patent attorney in many cases is not, for lack of a better word, a lawyer as such. According e.g. to § 6 of the German Patentanwaltsordnung or the §§ 3 ff of the Austrian Patentanwaltsgesetz, the most important prerequisite is not a degree in law, but in either natural science or engineering. Such a degree qualifies for the patent attorney training, which usually includes an apprenticeship of practical work at a patent attorney firm and/or the patent office, some additional studies of law and a final exam at the patent office. It is not unusual that a patent attorney becomes a patent examiner or vice-versa. The patent community therefore is a highly specialised group of experts and it would hardly be surprising to observe them constructing a language of their own.

3. Patent Claim Language

Although there is a vast literature dealing with the construction and interpretation of patent claims, e.g. [4], [2], [3], [6], [12], [17], [18], little attempts have been made at linguistically analysing the construction of claims, c.f. [20]. What follows is the first attempt to document a grammatical peculiarity common to many patents which are being perceived as problematic by experts, unwanted by the general public and often revoked by the patent office itself in the end, years after they have been granted.

3.1. The Monsanto Patent EP301749

In 1989, an application for an European patent by Monsanto Inc. on particle-mediated transformation of soybean plants and lines was published. This patent, EP301749 was granted in 1994 and opposition was filed immediately. From its frist publication on, the patent had been under heavy criticism because of claims monopolising vast areas of genetic research regarding soy (such as claim 5 on the genes being present in the meristematic tissue of a soy plant). After legal battles which lasted over a decade, the patent was finally revoked in 2007. Since protection is granted from the moment of application, the patent was in force - and enforceable - for a total of 18 years - only two years less than the maximum lifespan of a patent. According to Art 63 EPC, the duration of an European patent is 20 years (which can be extended only under special circumstances). Although Art 68 EPC specifies that a patent after its revocation shall be deemed not to have had its effect, it still endows its holder with a very strong market position as long as it is not revoked, enabling him to bully competitors, achieve out-of court settlements and close valuable cross-licensing deals, all of which hardly provide practicable means of revision after the revocation of the patent they were based on.

1 According to a conversation with the president of the German Patent and Trademark Office held on 15. July 2008, a degree in Computer science is not sufficient, although this subject is taught at technical universities.
But monopolisation of such basic research rights was not the only problem with this patent. Some of the procedures of identifying the presence of modified genes in soy plants even have a practical application which one might sarcastically call "Digital Rights Management on living creatures". Claim 24 of EP301749 reads:

A seed produced by a plant as claimed in either claim 22 or claim 23.

The claims 22 and 23 are on marking a modified genome by an enzyme and detecting such a mark by luminescent or colorimetric assay. Together with claim 24 that also means that e.g. a farmer whose crop has been contaminated by genetically modified seeds even without his knowledge, could be considered as infringing EP301749: Not only a seed produced in a laboratory is protected, but any seed by any plant in which that genome can be detected by the described method. This is not a hypothetical issue, as the case of the canadian farmer Percy Schmeiser demonstrates. Schmeiser was forced by court order in 2001 (2001 FCT 256) to hand over his saved seed from 1997 on to Monsanto, because it had been contaminated by a patented Monsanto seed. The following decision by the Canadian Supreme Court (2004 SCC 34) confirmed the patent infringement, but ruled that Schmeiser was not liable to also pay further damages to Monsanto.[13]

Of course, one could argue that the checks and balances in at the EPO work quite well. After all, a widely criticised patent has been revoked. However one should not forget that this patent has been in force for 18 years. In the meantime, Monsanto has gathered a collection of 152 more patents or published patent applications at the EPO, so the investment in keeping a protected monopoly on basic research techniques looks to have paid of quite well in this case - at least for the patent holder.

But increasingly, patents are not only granted on genetically modified plants, but also on substances derived from plants which have been known and used for a long time (sometimes centuries) only because they are chemically isolated or synthesised. By proper claim construction, a patent can be obtained not only on the process of isolation or synthesising, but on all products containing the substance, no matter if of natural origin, isolated or synthesised. See e.g. [19] and for a vast array of further examples [7].

3.2. The Amazon Patent EP0927945

In 1999, a patent application from Amazon.com Inc. on a method and system for placing a purchase order via a communications network was published by the EPO. Although supporters of the directive proposal COM (2002) 92 claimed that patents like the infamous Amazon one-click patent in the US would be highly unlikely or even impossible under the current EPO doctrine, the patent was granted in 2003. Passages like

An embodiment of the present invention provides a method and system for ordering an item from a client system. The client system is provided with an identifier that identifies a customer. The client system displays information that identifies the item and displays an indication of an action (e.g., a single action such as clicking a mouse button) that a purchaser is to perform to order the identified item.

in the summary reveal this patent as a direct descendant, if not a twin brother to its american relative. The first claim immediately demonstrates what this is all about:
A method in a computer system for co-ordinating delivery of a gift from a gift giver to a recipient, the gift and recipient being specified in a gift order, the method comprising: determining whether the gift order includes sufficient information so that the gift can be delivered to the recipient; when sufficient information is not provided in the gift order, obtaining delivery information from one or more information sources; and when sufficient delivery information can be obtained from the additional information sources so that the gift can be delivered to the recipient, directing the gift to be sent to the recipient as indicated by the deliver information.

Ordering a gift for somebody else was hardly anything new in 1999, neither is any of the instructions on handling contact data. The only distinctive thing here might be that these instructions are supposed to be carried out by a computer - also nothing earth-shakingly new in 1999. A set of instructions running on a computer is simply a computer program, nothing more. The linguistic game that is being played here is quite trivial. Instead of claiming a computer program in a completely obvious manner like

1. A computer program, comprising...
2. (whatever the computer program does)

the grammatical logic is modified by explicitly stating the obvious, i.e. mentioning the general purpose computer (on which any program needs to run to have any use at all) as if it was a patentable machine and defining a computer program (as such) as a core invention:

1. A computer system, comprising...
2. a computer program

Every single other claim of the gift ordering patent confirms this: receiving the gift order via email (claim 2), determining if the order contains contact data of the recipient (claim 3), contacting the recipient via email or phone (claims 4 and 5), reading the contact information from various kinds of databases (claim 6) as well as a logistics program containing more of the same (claims 7-11). All claims are on pure instructions for reading, processing and writing data, in other words: on mere software as such. The only exception might be seen in claim 5: If you can’t find the contact data in any of the databases and if you get no response via email either, pick up the phone and make a call. Not that new either.

Accordingly, that patent was revoked by the EPO board of appeals after an opposition filed by FFII e.V. et al. When Amazon’s representative stated during the oral proceedings that the method to be patented comprised a computer, and therefore represented patentable new technology, one of the patent examiners responded: "The machine was always able to do that. You just programmed it to do it!" Although this is the case for all patents on software as such, the EPO could not yet bring itself to a rejection based on unpatentable subject matter based upon Art 52 EPC. This lead to a mental balancing act, of having to re-examine the whole patent in detail and rejecting the claims due to the lack of an inventive step, which entitled Amazon to immediately formulate new patent claims. Since all of the newly filed claims were found to be in violation of the (rather formal) prescriptions of Art
123 EPC, the patent was then revoked in its entirety. Nevertheless, that patent enjoyed theoretical enforcability for a total of 8 years before its revocation. If you look at the progress computers and computer programs made since 1999, this looks like an eternity.

3.3. Further Examples

So far we have analysed patents which have been revoked. Despite these decisions as well as the rejection of the directive proposal COM (2002) 92 in 2005, many such patents are still in force or even newly granted. One example is EP0287578, one in a series of patents on the famous MP3 music compression format by the Fraunhofer Institute, which by some is even considered to be a digital example of the famous German art of engineering as well as a justified protection of years of investment in research. Although there really has been conducted some valuable research on the human perception of music during the development of the file format, the only claim actually referring to the results of such research is claim 11. The main claim is quite different, though:

Digital coding process for transmitting and/or storing acoustic signals, specifically music signals, comprising the following steps: N samples of the acoustic signal are converted into M spectral coefficients; said M spectral coefficients are subjected to quantisation at a first level; after coding by means of an entropic encoder the number of bits required to represent all the quantized spectral coefficients is checked; when the required number of bits does not correspond to a specified number of bits quantization and coding are repeated in subsequent steps, each at a modified quantization level, until the number of bits required for representation reaches the specified number of bits, and additionally to the data bits the required quantization level is transmitted and/or stored.

This sounds rather complicated, but is actually a quite simple procedure:

- First, it is decided how much disk space shall be assigned to a file yet to be created.
- The music is then compressed by already known methods (spectral coefficients, entropic encoding) with a certain trade-off in quality, since parts of the information are simply left out.
- The resulting file is checked if it uses the desired disk space. If it does not, the process is repeated until it does.

It is somewhat misleading to refer to something like this as a "broad claim". Rather, it is a quite specific monopoly on methods that are already known in an application (music) and which are not that difficult to come up with. The MP3-patent has been applied for in 1987, therefore the European patent has expired in 2007, because the maximum patent lifetime was reached. Although most of its claims are similar in nature to those of the Amazon patent, none of them have been revoked or at least limited by the EPO. And that patent is only one of a series of at least 18 other international patents covering the MP3 format, some of which will be in force up until 2017. After holding still until MP3 had become a widely accepted format on the market towards the end of 1998, the patent holders are enforcing their patents ever since against and collecting license fees from most known developers of audio encoding software.
This is neither a singular lapse of judgement, nor a past practice of the EPO. In fact such patents are still being granted. FFII research has shown that many of the most basic elements of a simple on-line webshop continue to be protected by patents. The examples in Figure 2 contain such claims as

- A network-based sales system, comprising: a merchant database comprising a plurality of digital advertisements and a plurality of respective product fulfillment items [...] (EP0803105, claim 1)

- A method according to claim 1 or 2, characterized in that the specification of the service request in step b) takes place in a dialogue with the central data base device, the service request being specified, amongst other things, on the basis of one or more parameters for time, place, price and quality respectively. (EP0738446, claim 3)

- An apparatus according to any one of the preceding claims, wherein said central server further comprises third storage means for storing an array of data representing the current exchange rate between each resource and at least one other resource, and wherein said processing means is further for retrieving exchange rate data from said third storage means. (EP1016014, claim 6)

- The method of claim 1 wherein the established area is movable to various desirable locations around the screen (EP0689133, claim 2)

- The method as claimed in claim 1, including the step of: closing said preview window whenever said button is released. (EP0537100, claim 2)

These examples are quite random and the list could be continued at will based on any of the patents shown in Figure 2.

4. Conclusion: Towards a more consistent Grammar of Claims

Apart from the two topics mentioned in the introduction and analysed in this paper so far, there is one more reason why the patent system is under fire - this time from within: Patent offices suffer from an overload of applications they have to deal with. Among the main reasons why EPO employees went on strike in 2006 was that they were "having to assess an increasing number of patent applications, with the backlog of applications piling up".[16]

Understanding the true effect of patent claims and the language used in them might also help in developing a deeper understanding of the correct interpretation of the exclusion of programs for computers as such in Art 52 EPC which in turn could provide effective means to significantly reduce that overload by avoiding the granting of most of the above mentioned patent claims in the first place in a simple, transparent and reliable way. Before entering a thorough examination of the patent and its technical description, an examiner should ask himself if a program for computers as such can be found in any of the claims. Any such claim could then be rejected without further examination by applying two rather simple rules which were (re-)proposed by the FFII in 2005[5]:

---

2 According to the EPO database, only two patents mentioned there have lapsed in the meantime due to non-payment of fees by the patent holder (EP0807891 lapsed 9 years after publication, EP1072143 after 5 years). All others still remain enforceable, some of them for up to 15 years more.
Ladybugs are very useful insects. They dispose of parasites. However, software patent litigators are far too large for them in general.

<table>
<thead>
<tr>
<th>Webshop</th>
<th>Selling things over a network using a server, client and payment processor, or using a client and a server – EP803105, EP738446 and EP1016014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order by cell phone</td>
<td>Selling over a mobile phone network – EP1090494</td>
</tr>
<tr>
<td>Shopping cart</td>
<td>Electronic shopping cart – EP807891</td>
</tr>
<tr>
<td>[CDs] [Films] [Books]</td>
<td>Tabbed palettes and restrict search – EP689133 and EP1131752</td>
</tr>
<tr>
<td>Picture link</td>
<td>Preview window – EP537100</td>
</tr>
<tr>
<td>Get key via sms</td>
<td>Sending key to decrypt bought data via mobile phone network – EP1374189</td>
</tr>
<tr>
<td>View film</td>
<td>Video streaming (&quot;segmented video on-demand&quot;) – EP633694</td>
</tr>
<tr>
<td>Copy protection</td>
<td>Encrypt file so it can only be played on authorised devices – EP1072143</td>
</tr>
<tr>
<td>Credit card</td>
<td>Pay with credit card on the Internet – EP779587</td>
</tr>
<tr>
<td>Adapt pages</td>
<td>Generate different web page depending on detected device – EP1320972</td>
</tr>
<tr>
<td>Request loan</td>
<td>Automated loan application – EP715740</td>
</tr>
<tr>
<td>Secure card payment</td>
<td>Secure online credit/debit card payment with PIN code – EP1218865</td>
</tr>
<tr>
<td>Send offers</td>
<td>Send offers in response to request – EP986016</td>
</tr>
<tr>
<td>Delivery</td>
<td>Ship items to the correct pick-up point of the used delivery service – EP1181655</td>
</tr>
<tr>
<td>Support system</td>
<td>Support system based on answers to questions – EP915422</td>
</tr>
<tr>
<td>Preview chapters</td>
<td>Use of TV as metaphor for selecting different video fragments – EP670652</td>
</tr>
<tr>
<td>Image</td>
<td>Reduce page loading time by automatically reducing image quality – EP992922</td>
</tr>
<tr>
<td>Related results</td>
<td>Show related results if customer likes the current ones – EP628919</td>
</tr>
<tr>
<td>Rebate code</td>
<td>Allow rebate codes to be entered by customers – EP929874</td>
</tr>
<tr>
<td>Web-to-Print</td>
<td>Generation of prepress formats or printouts from low resolution templates via the Internet – EP852359 and EP1169848</td>
</tr>
</tbody>
</table>


Figure 2. The patented webshop
1. A claimed object that consists only of instructions for use of generic data processing hardware (universal computer), also called "program for computers" or "computer-implemented solution", is not an invention in the sense of patent law, regardless of the form in which it is claimed.

2. A claimed object can be an invention in the sense of patent law only if it contributes knowledge to the state of the art in a field of applied natural science.

The first of these two rules is not only contained in Article 52 of the European Patent Convention, but also explained in the European Patent Office’s Examination Guidelines of 1978. It is one of the simplest rules that patent courts have ever applied and theoretically would allow even a robot to sort out the most common software patent claims. The second is a simplification of more elaborate versions that were developed by German courts (see e.g. BGH 28 X ZB 23/74, 1976 - Dispositionsprogramm; for details and an earlier version of the two rules [15]). It is an auxiliary rule, needed for cases that do not fit clearly into the list of unpatentable items of Art 52 (2) EPC. According to its strictest interpretation, an invention must impart knowledge about effects of the use of forces of nature, i.e. knowledge that was gained by experimentation rather than by deduction. The EPO has never sought to formulate this rule as clearly as the German courts, and yet they have, in a series of decisions starting with Vicom in 1986, heavily relied on it and stretched it beyond bearing, so that it became increasingly difficult for them to argue that their practice was still in line with rule 1, respectively Art 52 EPC.

The first rule could also easily be adapted to avoid those cases that might be considered "patents on life" by a simple reformulation like "consist only of properties found in non-genetically-modified (naturally bred) life-forms" instead of "consists only of instructions for use of generic data processing hardware (universal computer), also called[...]") Such a rule would have helped to reject at least some of the claims in EP0927945 already upon application and would exclude many of the examples in [7] as well.

These proposed rules need not lead to the complete rejection of the complete patent application in each and every case. Quite to the contrary, they would only serve to cut out those claims that are not compliant. But instead of further burdening the patent offices by forcing them to thoroughly examine lengthy rhetoric explaining why a certain software (or organism) should be, according to the applicant, considered an invention despite of Art 52 EPC (or Art 53 EPC), and then re-examining it all over again during an opposition procedure, it would encourage the applicant to formulate his claims in a proper - and more understandable - manner in the first place.

References


UNFAIR COMPETITION CAUSED BY BAD FAITH
UTILITY MODEL REGISTRATION

Knut K. Wimberger¹

Abstract
A rising amount of domestic utility models prevent and/or obstruct foreign businesses from competing on the Chinese market under fair conditions. If justice is sought before the patent reexamination board or civil courts, especially for SME, the costs for legal representation are unaffordable high; proceedings consume much time and human resources that are not available. Market access is effectively inhibited.

1. Domestic and Foreign Utility Models
There have been 181,324 utility model applications in 2007, 99.3% of domestic, 0.7% of foreign origin. 150,023 utility models have been granted in 2007, 98.9% to domestic, 1.1% to foreign applicants. In comparison, there have been 245,161 invention patent applications in 2007, only 62.4% were of domestic, but 37.6% were of foreign origin (see tables below).

The reason for the stark difference in foreign and domestic applications of the three Chinese patents might be alternatively or complementarily (different sources):

- Chinese inventors still lack the kind of technology that can be applied for invention patents
- Chinese inventors lack the financial funds to apply for invention patents and therefore confine themselves to cheaper utility models or design patents (similar statistics like utility model).
- Chinese applicants register in good or bad faith utility models for technology have already been patented in other jurisdictions.

2. A Fast and Easy Track to IPR Registration
The current Chinese Patent Law contains following provisions for acquiring patent protection.²

Article 34 CPL: Examination and Publication

¹ Mag. Knut K. Wimberger, Bakk., Höhnegasse 18/21, 1180 Wien, Austria; k.wimberger@awsg.at
The state council patent administration publishes the application of an invention patent within 18 months from the application date if it deems upon preliminary examination that the invention patent application complies with the demands of this law.

**Article 35 CPL: Substantive Examination**
The state council patent administration shall carry out a substantive examination at any time within three years from the date of the invention patent application upon the request of the applicant. […]

**Article 40 CPL: Utility model and design patent applications that have not been rejected upon preliminary examination shall receive a decision from the patent administration of utility model or design patent grant. The corresponding patent grant certificate shall be issued by the state council patent administration and simultaneously registered and published. Utility models and design patent are in force from the date of granting publication.**

Worldwide there exist several national patent systems that offer next to invention patents also the registration of utility models; China and Austria are both such countries. Most of those national patent systems have in common that invention patents have to undergo a preliminary examination in which the formal requirements are checked, in order to proceed to a substantive examination in which the material requirements for registration based on international and national regulations are examined (see chart below).

Utility models on the contrary do not require a substantive examination in most jurisdictions, because the patent systems deem the efforts of substantive examinations too much for technical products of minor inventive steps. Novelty too is required, but not subject to examination. The application and registration procedure therefore lasts only a fraction of the procedure for invention patents (see chart below).

In most national patent system utility models that are void of novelty and/or inventiveness can be detected easily by competitors and will be invalidated as a consequence. Moreover disputes
about the level of inventiveness can arise easily. For these reason, IPR applicants in developed nations with evolved patent systems have lost most their interest in registering utility models. Utility models have become a neglected child within the IPR family, because they are fragile, attackable and provide in consequence no legal security.

In some developing nations utility models have quite on the contrary become a popular form of IPR amongst private inventors and SME. Utility models are easy to register and dirt cheap, for which reasons many developing governments use utility models (as well as designs) to ignite IPR awareness and possession among the domestic business community. The above statistics show that in particular the Chinese government consciously supports the registration of utility models, whereas foreign entities do not register according to established patenting practices.

3. Scope of Legal Protection and its Effects

Article 11 CPL: Exclusion Regulations

Upon the grant of an invention patent or utility model patent it is, unless otherwise stated in this law, not permitted without the licensor’s permission to any entity or individual person to make use of the patent for the purpose of commercial production, usage, promised sales, sales, import of any such patented products, or make use of the patents usage method, promised sales, sales, import of products that make use of patent’s method.3

The owner of a utility model is awarded by the national government the exclusive right for the registered technology for maximum 10 years duration. The scope of legal protection for utility models is identical to invention patents. The owner possesses the exclusive right to produce, sell, trade, license, etc. the patented technology. He can therefore also legally exclude, i.e. inhibit, other entities in performing these actions without his permission by means of filing with civil courts a preliminary injunction or action for permanent injunction.

Preliminary injunctions are designed to prevent imminent damage, e.g. the sale of counterfeited and pirated products at trade fairs. The permanent injunction is designed as a remedy against recurring counterfeiting and piracy activities, e.g. the production and sale of a product that contains technology of the lawful IPR owner. A successful permanent injunction may not only prevent competitors from production and sale of the respective product and therefore inhibit market presence, but also oblige the defendant to pay damage rewards to the plaintiff for profits made from back to the date of application up to verdict.

In effect this means that utility models provide a comprehensive legal protection for technology that has not been examined by the national IP authorities. The national system can therefore be easily abused by applicants, and it can be used to implement national competitiveness policies, that distort international trade and limit market access to China. Utility models that are registered in bad faith, i.e. entrepreneurs apply for IP protection, although they exactly know that the respective technology is neither their creation nor novel nor inventive, enable the IPR owner to permanently inhibit the rightful inventor as well as rightful competitors in doing business, and

might moreover oblige them to pay damage awards to the lawful, but bad faith owner of a utility model.

4. **Costs of UM Application vs. Costs of Invalidation**

China does of course fully comply with international regulations and treaties in terms of its IPR laws. Moreover, a patent examiner asked about the elaborated problem will answer that the true inventor of a product as well as competitors that have used the technology prior to the application date can request invalidation with the patent reexamination board at SIPO. This is correct, but the legal reality shows that the IP system as it works now fails to function. An IPR once granted is not that easy removed again.

A utility model can be registered in China for less than EUR 200.-.\(^4\) Public fees are small, patent attorneys charge much less than for an invention patent and several Chinese authorities on local, provincial and national level provide substantial subsidy for domestic and international IPR application. To request invalidation though is a burdensome and sometimes futile undertaking. It can last several years to remove an IPR from the legal realm. Meanwhile there is insecurity about market access or in the worst case the bad-faith-IPR-owner directs executive organs who rightly do as the law says, against other parties to remove them from trade fairs, to close down their production units or destroy the respective products.

Especially for foreign companies, but equally for Chinese firms, it is important to have in such a case capable lawyers who can succeed with the invalidation in minimum time. This means burdensome evidence gathering, draft of invalidation pleading, ongoing communication with the Patent Reexamination Board, etc. Chinese lawyers that can handle such cases efficiently are rare and may ask fees of EUR 20.000.- and more; costs that might cause a foreign SME to drop the case and retreat from the Chinese market at all.

5. **Example Case ZL01242873.6**

Currently an invalidation case is processed for the second time before the Patent Reexamination Board (PRB) that is based on the above described situation. A Chinese competitor has copied the product of an Austrian company and registered a utility model for a part of the product that had not been patented before. Since the Chinese competitor produces slave copies of the Austrian original product it has to be emphasized that the utility model application was carried out in bad faith and had the sole objective of preventing/limiting the sale of the original product on the Chinese market.

Involved Parties:
- A. The Cool Tool GmbH, Austrian SME
- B. Creative Power Ltd. - 崇宝欧美科贸有限公司, Chinese Partner of A
- C. 佛山市禅城区优耐美模型工具纠纳有限公司, Guangdong dealer of B

\(^4\) Interviews conducted by the author with several Chinese Patent Attorneys during a fact finding mission for Austria Wirtschaftsservice | Innovation Protection Programme in China from 26.2. until 23.3.2007.
D. Guangdong Foshan Shunde Xendoll Ltd. - 广东佛山市顺德区桂容协邦实业有限公司, owner of utility model.

Case Summary:

- Application for utility model titled “微型组合机床” on 2001-07-27. ZL01242873.6 is registered on 2002-04-03 for D. The claims of the utility model describe a small connection piece of a machine tool kit that was originally invented in Austria.
- The patented part has already been produced by A since 1994 and sold in the PRC before 2000. Several witnesses (customers of the exclusive mainland Chinese partner B) testify this fact, most prominently a Chinese official who conducted safety tests on the machine. Several printed publications like product manuals and articles in industry related magazines as well as production evidence for the connection piece prove that there is no novelty to the utility model ZL01242873.6. The connection piece had neither been patented in China nor in other countries, because the minor step of inventiveness was not deemed protruding enough for registration.
- 2003-12-08: PRB rejects a full invalidation, but concedes partial invalidation: the utility model and the provided evidence differ in scope; the utility model possesses novelty and remains in force.
- 2004-05-10: civil action at Beijing No 1. High Court against the PRB for rejecting the request for invalidation.
- 2004-12-20: civil action fails. 1st request for invalidation closed. All possible instances taken.
- 2005-11: D “observes the import of infringing products” by B and distribution and sale by C. D sues B and C at the Foshan Civil Court for ZL01242873.6 infringing import, distribution, sales, reduction of own sales, market price deterioration and overall economic damage.
- 2007-03-02: D “detects the infringing offering of protected technology” on the website of B.
- 2007-4: Foshan Middle Court rules against B and C, and confirms the request of D.
- 2007-4: B and C appeal against the Foshan Middle Court Ruling at the Guangzhou High Court – Decision is still pending because of invalidation request.

Up till now more than EUR 30,000.- and much more in time and efforts have been spent by the A and B to invalidate the utility model and regain free and lawful market access. No results were achieved although the evidence is unmistakably clear and strong. A owns several other utility models, designs, trademarks and copyrights in China; some are in the process of registration.

6. Conclusions and Recommendations

It is a fact that bad-faith-IPR-registrations do occur in China. Not only foreign companies, but also domestic competitors pay high tolls for a currently in parts insufficient and ineffective IPR-
system. China has become the third largest patent filing country worldwide and as a matter of fact its business community develops much faster than in any other developing nation. China in fact has in some regards already left the status of a developing nation and has become a developed nation. But due to the fast changes that take place in China within only a few years other measures are required than in “old developed nations”, where a patent system on the public side and a patenting behavior on the business side had 150 years or more to evolve.

If the comparison may be allowed – China is in particular due to its size, population and enormous amount of FDI that flowed into the country during the past three decades a single case of growth in prosperity that is unrecorded in history. Unique circumstances allow and demand new ideas to resolve the arising problems – the one child policy was widely criticized, but not only China, but the whole world will be grateful for its rigorous implementation that helped to reduce the population growth of an estimated 500 million people up till now. China enacted a law that did what happens naturally in “old developed nations”: the decline in absolute population. It rightly foresaw a development and acted accordingly: a unique human challenge that was tackled by the Chinese government with a unique, new and successful approach.

Although the dimensions of population growth and its impact to our world can not be compared to the impact of a national IP policy on global trade, the effects are economically measurable and can in certain SME cases hurt existentially. It is recommended to find a method to control bad-faith-utility-model-registrations, because unique challenges demand a unique approach. The political competence for IPR coordination, planning and implementation of the national IPR policy has been transferred to SIPO during the restructuring of the Chinese government in early 2008. Still, all trade related aspects of IPR remain with MOFCOM. Therefore both, MOFCOM and SIPO are asked to take the steps that are necessary to enhance the situation of SME like the one mentioned in this memorandum.

Possible mechanisms include:

- Creating awareness among Chinese entrepreneurs that bad-faith-IPR-registration are illegal according to international regulations, without diminishing the general incentives to apply for IPR protection.
- Introducing an administrative penalty for in bad faith applicants
- Introducing regulations to the patent law that demand a global novelty check that has to be signed by the applicant (in combination with a penalty regulation)
- Enabling an obligatory exchange mechanism between IP courts and SIPO that prevents civil cases to be fought over for years, while an IPR might be invalidated at the very end.
- Introduction a damage reward for successful requests for invalidation with the Patent Reexamination Board that comprises the costs of all parties involved in cases fought over a bad faith IPR (only possible in combination with obligatory novelty self check).

Eventually it may be pointed out that it is not only in the interest of foreign entities, but equally if not more in the interest of China to increase the quality of its national IP portfolio. Junk patents, whether invention or utility models, feed on national financial resources and diminish the long term competitiveness of businesses.
Title: Foreign- and Domestic Patent Applications 2007
Source: SIPO

<table>
<thead>
<tr>
<th>国内外三种专利申请受理状况年表</th>
<th>2007年1月 - 2007年12月</th>
</tr>
</thead>
<tbody>
<tr>
<td>分组</td>
<td>申请量</td>
</tr>
<tr>
<td>合计 Total</td>
<td></td>
</tr>
<tr>
<td>申请量</td>
<td>694153</td>
</tr>
<tr>
<td>构成</td>
<td>694153</td>
</tr>
<tr>
<td>国内 Domestic</td>
<td></td>
</tr>
<tr>
<td>申请量</td>
<td>430266</td>
</tr>
<tr>
<td>构成</td>
<td>430266</td>
</tr>
<tr>
<td>国外 Foreign</td>
<td></td>
</tr>
<tr>
<td>申请量</td>
<td>264887</td>
</tr>
<tr>
<td>构成</td>
<td>264887</td>
</tr>
<tr>
<td>合计</td>
<td>694153</td>
</tr>
<tr>
<td>构成</td>
<td>694153</td>
</tr>
</tbody>
</table>

单位：件
<table>
<thead>
<tr>
<th>年份</th>
<th>国内职务</th>
<th>国内非职务</th>
<th>国外</th>
<th>合计</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1月</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12月</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>小计</td>
<td>133814</td>
<td>62974</td>
<td>12051</td>
<td>31945</td>
</tr>
</tbody>
</table>
| 比例 | 44.4%    | 38.2%      | 96.4%| 100.0%

<table>
<thead>
<tr>
<th>年份</th>
<th>国内职务</th>
<th>国内非职务</th>
<th>国外</th>
<th>合计</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1月</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12月</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>小计</td>
<td>301500</td>
<td>1645</td>
<td>1145</td>
<td>313556</td>
</tr>
</tbody>
</table>
| 比例 | 100.0%   | 0.0%       | 0.0% | 100.0%

**单位**: 件

**注释**: 数据来源：SIPO
SOFTWARE PATENTS: SOFTWARE AUTHORS LOST THEIR RIGHTS

Benjamin Henrion

Abstract

Authors receive copyright protection for software in its various forms.

In the recent years, Patent Offices all over the world have been granting patents on software solutions in volume which constitutes an overlap with the domain of authors' rights and a conflict with the freedom of imitation generally endorsed by competition laws. It boils down to the question if an alleged protection gap of copyright for software authors needs to be closed by another legal instrument and how that very instrument suits their needs. Software authors enjoy freedom of speech as any other authors, and software patents undermines the right of software authors to benefit from the fruits of their work.

Conflict of rights between copyright and patents for software may ultimately constitute censorship, similar to censorship of religious speech in the 17th century. The presentation will try to highlight what are the forthcoming dangers for software publishers, and present solutions on how to re-establish full freedom of speech in the writing, publishing and use of computer programs.

1 The Foundation for a Free Information Infrastructure (FFII), Brussels. E-mail: bhenrion@ffii.org.
PATENT POLICY

Richard Schlötter

Abstract

Identifying the “best” IP protection regime is virtually impossible in the abstract: copyrights, trademarks, patents and trade secrets each serve essential, albeit different, roles in the digital economy.

Patent protection has recently become the subject of controversy in some quarters, and thus may merit particular focus. BSA represents many of the world’s most innovative and research-intensive companies – companies that are among the largest owners of patents. Our members share the belief that patents are indispensable to innovation and competitiveness, and also help to promote interoperability among technologies.

Of course, patents will only spur innovation if the patent system is properly functioning. BSA members agree that the European patent system as a general rule works well and consistently produces high-quality patents – both patents for computer implemented inventions and patents on other inventions. To the extent that reforms are needed in Europe, these are unrelated to patent quality or to the substantive rules that apply to patents. Instead, the real need in Europe is for structural improvements at the margins of the patent system – including reforms relating to patent litigation and patent cost – to enable inventors large and small to reap the system’s benefits.

1 Dr. Richard Schlötter, Partner, Reed Smith LLP, Munich, DE; e-mail: rschloetter@reedsmith.com.
Estelle Derclaye*

Abstract
The Database Directive, which created a new database sui generis right and harmonised the copyright provisions for databases, does not exclude “state databases” from protection. The question is whether the state should benefit from such intellectual property protection. De lege ferenda, it has been advocated that neither copyright nor sui generis right should protect such databases for several reasons, a major one being that they are financed by taxpayer’s money. Several solutions exist de lege lata to try and curtail this negative aspect of the Database Directive as applicable to “state databases” (mainly the human right to information and competition law). One solution, specific to the situation of the state, has not been discussed in depth yet. It is provided by the Public Sector Information (PSI) Directive which grants the possibility for anyone to re-use public sector information (and therefore data from state databases) free of charge or at minimal cost, even for commercial purposes. Therefore, even if the state could claim sui generis right on some of its databases, the PSI Directive appears to reduce this right quite substantially. The paper examines in detail whether the PSI Directive does actually do so and analyses some national implementation laws which further highlight its ineffectiveness in curtailing the sui generis right in state databases. It then proposes solutions to remedy this problem.

1. INTRODUCTION
2. THE DATABASE SUI GENERIS RIGHT
3. THE DIRECTIVE ON THE RE-USE OF PUBLIC SECTOR INFORMATION
   3.1. RATIONALE FOR OPEN ACCESS TO PSI AND HISTORY OF THE DIRECTIVE
   3.2. ANALYSIS OF THE PROVISIONS OF THE DIRECTIVE
4. THE NATIONAL EXPERIENCE
   4.1. BELGIUM
      4.1.1. Copyright and database right
      4.1.2. Access to information regimes
      4.1.3. Re-use of PSI
   4.2. UNITED KINGDOM
      4.2.1. Copyright and database right
      4.2.2. Access to information regimes
      4.2.3. Re-use of PSI
5. THE FAILURE OF THE PSI DIRECTIVE: SOLUTIONS BASED ON THE DATABASE DIRECTIVE AND NATIONAL LAWS
   5.1. PRELIMINARY QUESTION: DOES THE STATE REALLY HAVE SUI GENERIS RIGHTS?
   5.2. DOES THE PSI DIRECTIVE TRUMP OR DAMPEN DOWN OBJECTIONABLE STATE SUI GENERIS RIGHTS?
   5.3. SOLUTIONS BASED ON THE DATABASE DIRECTIVE
   5.4. SOLUTIONS BASED ON NATIONAL LAWS
6. CONCLUSION
7. REFERENCES
1. Introduction

How many of us know that in the EU, the public sector is the largest producer of information? Well, it is, and the range of information it produces or holds is extremely rich and diverse. It comprises among others reports, internal administrative documents, geographical maps and more broadly any mapping data, statistics, company information, census data, forms, technical reports, patent information, documentaries, and, databases, such as library and museum catalogues, guides, codes of practice, collections of deeds, trains and bus schedules and exam results. Not only is this information valuable, it is also generally complete and accurate and therefore reliable. This obviously gives a lot of power to the state. But there is more. The *sui generis* right (also called database right), which has been with us since 1996, creates a new intellectual property right (IPR) to protect the investment made to collect, verify or present information within a database. The right has been criticised for giving too much protection to database producers or even further for giving them a monopoly on information. Whilst this is often not the case, it can sometimes happen and state databases constitute a prime example. Indeed, most of the time, the information contained in such databases is for the reasons stated above, the most exhaustive and most accurate on the market, and therefore the only one or if not, at least the best. The *sui generis* right that the state has therefore gives it a lot of power as it can charge monopoly prices for it. Notwithstanding this anti-competitive effect, other reasons, the strongest being surely that it leads to double taxation, entail that “state *sui generis* right” is unacceptable.

However, the state is in a special position compared to private parties. National and European laws provide that it has to give access to its documents either free of charge or at minimal cost and allow its re-use. There is therefore a conflict between the *sui generis* right and this right of access and re-use. Or is there? How effective is the Directive on the re-use of public sector information (PSI Directive) to trump the state’s *sui generis* right and is the Database Directive really giving such a right to the state in the first place? Despite its importance, this topic has not been investigated in detail yet. This is what this paper sets out to do. Section 2 briefly reminds what the *sui generis* right is and what broad rights it gives to database producers. Section 3 concentrates on the PSI

---

* © Estelle Derclaye 2008. Ph.D. (London); Lecturer in law, University of Nottingham.

1 The terms public sector and state will be used interchangeably and refer to the same notion namely to the three state’s branches, legislative, executive and judicial.

2 [4]

3 [4]; [16], p. 622, 626, 628.

4 As noted by [43], p. 1, this is because “all citizens targeted by the legislation in question [are] required to provide it (...) and sanctions are envisaged for anyone giving false information.”


6 See e.g. [36], p. 10; [46], p. 94; [19], p. 268–273.

7 There is of course also a conflict between the database right on the one hand and the human right to information (art. 10 ECHR), national laws on abuse of right and competition rules on the other hand, but these are not explored here. For more information see e.g. [13], p. 3-23; [3], p. 233 ff.


9 Questions had recently been referred to the ECJ by the German Federal Supreme Court but the case has (unfortunately for lawyers) been withdrawn. See reference for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 24 April 2007, Verlag Schawe GmbH v. Sächsisches Druck- und Verlagshaus AG, Case C-215/07, OJ C 155, 7 July 2007, p. 12. For the underlying Decision of the Bundesgerichtshof, 28 September 2006, [2007] GRUR, p. 500-502. For a summary of the case with comments, see [30].
Directive. It gives the reasons why it is better that government information be available as widely and cheaply as possible and retraces the history of the Directive. It then describes what the PSI Directive provides. Section 4 looks at the situation in two Member States (Belgium and the UK) in relation to the database right, access and re-use of public sector information. The last section looks at the conflict and answers the question addressed by this paper, namely whether the Public Sector Information Directive affect state database right. As it concludes it does not, it proposes solutions, based on the Database Directive and national laws, to curtail state sui generis rights.

2. The database sui generis right

As the audience will be most familiar with intellectual property rights, the description below will be a summary of the most important provisions of the Directive relating to the sui generis right. Copyright concepts relevant to the discussion will be assumed.

The database right was introduced in 1996 by Directive 96/9/EC on the legal protection of databases. It is provided for in chapter 2 of the Directive (art. 7-11); articles 1 and 13 are also relevant. In 2004, the European Court of Justice (ECJ) interpreted the right and reduced some of its vague and overbroad aspects. Nevertheless, the right is still in many respects, as had been rightly criticised in the literature, over-protective of database producers’ interests in comparison to that of users. This summary will highlight the main features of the right with a focus on its negative, i.e. over-protective, aspects.

This new intellectual property right grants database producers a right to prevent extraction and reutilisation of the contents of the database (art. 7(1)). Databases are defined in article 1(2) as collections “of independent works, data or other materials, systematically or methodically arranged and individually accessible by electronic or other means”. Databases can be in any form, e.g. analog or digital, off or online (art. 1(1)). This definition is quite broad and it arguably includes collections of tangible objects. Despite its breadth, the definition is somewhat circumscribed as the items must be independent from each other. This will for example exclude statistical tables whose numbers are dependent on one another, i.e. no element has autonomous informative value. In addition, the elements must be arranged systematically or methodically. This will exclude haphazard collections.

The right accrues when a qualitatively or quantitatively substantial investment in the obtaining, verifying or presenting of the materials is proven (art. 7). There is no definition of investment. However, from the Directive’s recitals and the ECJ’s interpretation, it is clear that investment can be financial, material (acquisition of equipment e.g. computers) or human (number of employees, hours of work). What is substantial is also left undefined in the Directive and the ECJ has not ventured in giving an interpretation. Many national courts, and the Advocate General in its

10 The copyright on state databases will not be examined although most conclusions would be similar. This is because often the structure of databases will not be original and no copyright will subsist. When it does, it will often not have to be re-used as such as they are many ways of organising databases and different ones might be more useful to an industry than that created by the state. Therefore, no conflict will arise.

11 Four related decisions of 9 November 2004, Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairon (OPAP) (case C-444/02) [2005] 1 CMLR 16 (further referred to as “OPAP”); Fixtures Marketing Ltd v. Oy Veikkaus AB (case C-46/02) [2005] ECDR 2 (further referred to as “Veikkaus”); Fixtures Marketing Ltd v. Svenska Spel AB (case C-338/02) [2005] ECDR 4 (further referred to as Svenska Spel) and The British Horseracing Board Ltd v. William Hill Organisation Ltd (case C-203/02) [2005] 1 CMLR 15 (further referred to as “BHB”), also available on www.curia.europa.eu (last accessed on 29 August 2008). Unless indicated otherwise, all web sites have been last accessed on that date. For more detail on the sui generis right in general, see [15].

12 See [12], p. 275-298.
Opinion\textsuperscript{13}, have interpreted the requirement as being rather low. For example, a few days work or a few hundred pounds or euros may be sufficient to qualify the database. According to the ECJ, a quantitatively substantial investment refers to the amount of money and/or time invested in the database while a qualitatively substantial investment refers to the effort and/or energy invested in the database. The alternative requirement set out in the Directive (quantitatively or qualitatively) therefore allows the protection of databases which have required only a substantial investment in effort or energy rather than in money.

The ECJ construed the term “obtaining” as meaning only collecting the elements of a database. This excludes their creation.\textsuperscript{14} This interpretation is very important because a lot of so called spin-off databases, similar to those in question in the ECJ cases, i.e. horseracing and football fixtures, are now excluded from protection. This includes for example event schedules, television or radio programmes, timetables, telephone subscriber data, stock prices and sports results. If the substantial investment in the collection, verification or presentation of the materials is inseparable from the substantial investment in their creation, the right will not subsist. On the other hand, verifying and presenting have been given a straightforward dictionary meaning. Verifying thus means ensuring the reliability of the information contained in the database, monitoring the accuracy of the materials collected when the database was created and during its operation. Presenting refers to “the resources used for the purpose of giving the database its function of processing information, that is to say those used for the systematic or methodical arrangement of the materials contained in that database and the organisation of their individual accessibility”.\textsuperscript{15} The database producer is the person who takes the initiative and the risk of investing; subcontractors are not makers (recital 41).

The database right grants to the database maker, the right to prevent the extraction and the reutilisation of a substantial part, evaluated quantitatively or qualitatively, of the contents of the protected database (art. 7). The rights of extraction and reutilisation can be compared to the rights of reproduction and communication to the public in copyright law, as they are very similar. A substantial part has not been defined but the ECJ said it had to represent a substantial investment. The substantial part evaluated quantitatively refers to the volume of the data extracted or re-utilised from the database and it must be assessed in relation to the volume of the contents of the whole of the database. The substantial part evaluated qualitatively refers to the scale of investment in the obtaining, verification or presentation of the contents, regardless of whether that subject (or part) represents a quantitatively substantial part of the contents.\textsuperscript{16} Users can freely extract or re-utilise insubstantial parts so long as they do not do it repeatedly and systematically so that the accumulation of insubstantial parts becomes a substantial part.\textsuperscript{17}

There are three exceptions to the rights but they are all optional so Member States did not have to implement them. Thus the number of exceptions varies from Member State to Member State. According to article 9 of the Directive, lawful users, i.e. those who have acquired a lawful copy of the database\textsuperscript{18}, can (a) extract a substantial part of the contents of a non-electronic database for private purposes, (b) extract a substantial part of any database for the purposes of illustration for teaching or scientific research as long as it is not for commercial purposes and the source is

\textsuperscript{13} Opinion of Advocate General Stix-Hackl, 8 June 2004, case C-46/02 (\textit{Veikkaus}), para. 49, available on www.curia.europa.eu
\textsuperscript{14} See e.g. paragraph 24 (Svenska Spel).
\textsuperscript{15} Paragraph 27 (Svenska Spel).
\textsuperscript{16} Paragraph 70 and 71 (BHB).
\textsuperscript{17} Article 7(5) and 8(1) as construed by the ECJ, paragraph 86 (BHB).
\textsuperscript{18} No clear guidance is given in the Directive as to who is a lawful user and the ECJ did not have to interpret the term. This is our preferred interpretation as well as that given by several authors. See [15], p. 120ff. and authors cited.
indicated and (c) extract and/or reutilise a substantial part of any database for the purposes of public security or an administrative or judicial procedure. The right of the user to use insubstantial parts not amounting to a substantial part (art. 8) has been made imperative (art. 15) but not the three optional exceptions. Therefore, database makers can override them by contract and by technological protection measures (TPMs) provided, however, that article 6(4) of the Copyright Directive\(^\text{19}\) is respected.

Finally, databases are protected for 15 years from their completion or their publication (art. 10). Furthermore, each time the database maker reinvests substantially in the obtaining, verifying or presenting of the elements of her database and there is a substantial change, he or she gets a new term of 15 years. What is unclear however is whether he or she gets it on the whole new database which comprises the “old” elements (i.e. those whose term has expired) or only on the elements which have newly been included, verified or presented. Therefore, the right can last potentially perpetually.

Of particular interest to this article, because it touched upon state databases, is article 8 of the Directive Proposal which was finally deleted from the text. It provided for a compulsory licence and read: “1. Notwithstanding the right provided for in article 2(5) to prevent the unauthorised extraction and re-utilisation of the contents of a database, if the works or materials contained in a database which is made publicly available cannot be independently created, collected or obtained from any other source, the right to extract and re-utilise, in whole or substantial part, works or materials from that database for commercial purposes, shall be licensed on fair and non-discriminatory terms. 2. The right to extract and re-utilise the contents of a database shall also be licensed on fair and non-discriminatory terms if the database is made publicly available by a public body which is either established to assemble or disclose information pursuant to legislation, or is under a general duty to do so”. Also of interest for the purposes of this paper is article 13 which provides that the \textit{sui generis} right is without prejudice to other forms of protection of the database such as among others the legislation on access to public documents.

It can now be seen what is still problematic with the \textit{sui generis} right. While the rights are broad (even though not unduly), the exceptions are very narrow and in practice, their existence depend on each national law. Therefore, in some countries they may well be bluntly absent. Users, and lawful ones at that, can never reuse substantial parts of a database for commercial purposes without authorisation. If they want to reuse insubstantial parts, they must make sure that these parts do not amount to a substantial part. The terms “substantial part” being by definition vague and therefore subject to interpretation in each case, it puts users in an awkward situation when they want to decide whether to use bits of databases: should they ask permission or not? Finally, the right is in effect, for dynamic databases, perpetual. This is because there is no obligation for the database producer to identify those elements on which there has been no new investment, and if the user cannot identify them, he or she must always ask permission if he or she wants to use substantial parts in most cases.

3. The Directive on the re-use of public sector information

3.1. Rationale for open access to PSI and history of the Directive

Open access to government documents is not a new issue. It has its origins in government secrecy, which dates back to the Old Regime. Secrecy, which initially had to insure that tasks be efficiently executed by the administration, became a tool of power.\(^{20}\) The late 18\textsuperscript{th} and 19\textsuperscript{th} centuries’ philosophers and economists Jeremy Bentham and John Stuart Mill, among others, exposed the “evil” of secrecy namely that if the government can keep things secret, it will abuse its power.\(^{21}\) Indeed, as happened, when the government started cultivating secrecy vis-à-vis its citizens as well as the Parliament without this power shift being accompanied by the setting up of control by the Parliament or even by the citizen him- or herself, it was thought that this situation could not be considered satisfactory from the standpoint of democratic demands.\(^{22}\) It is now considered that freedom of information is the basis of democracy.\(^{23}\) Sweden was the pioneer, requiring open access to government information as early as 1766.\(^{24}\) In 1981, the Council of Europe took a recommendation to encourage members to adhere to this basic democratic principle. It recommends that members make “the utmost endeavour […] to ensure the fullest possible availability to the public of information held by public authorities”.\(^{25}\) The recommendation contains the basic principles concerning the recognition and organisation of an access right to information detained by administrative authorities. Its content can be summarised as follows.\(^{26}\) It is a right of access for all persons, natural or legal, which are under the jurisdiction of the state. Access is exercised by request. Requests must not be justified by a particular interest. Only restrictions necessary to the protection of legitimate public or private interests in a democratic society are admissible. Finally, refusal decisions must be justified and subject to an appeal. All national legislations adopted by the Members of the Council of Europe are similar to the recommendation.\(^{27}\) Even before the recommendation, some countries had legislation on access to public information mainly based on the U.S. 1966 Freedom of Information Act.

Of course freedom does not mean complete gratuity although this should normally be the rule\(^{28}\), as shall be seen below. Apart from the already strong reason mentioned above for the openness of government information, there are several other reasons for making government documents, and more generally public sector information, available to the public. They can be classified in positive and negative reasons.

\(^{20}\) [16], p. 19- 20.
\(^{21}\) [37], p. 2.
\(^{22}\) [16], p. 20, citing a great number of authors.
\(^{23}\) [16], p. 21; [24], p. 185-186. Recital 16 of the PSI Directive mentions this too.
\(^{24}\) [37], p. 30; [16], p. 169. See Freedom of the Press act 1766. On the Swedish law, see e.g. [42], in [37], p. 35-54.
\(^{25}\) See preamble of Recommendation n° R(81)19 of the Committee of Ministers of 25 November 1981 of the on access to information held by public authorities, available on http://www.coe.int/t/e/legal_affairs/legal_co-operation/administrative_law_and_justice/texts_&_documents/Conv_Rec_Res/Recommendation(81)19.asp
\(^{26}\) [16], p. 168.
\(^{27}\) [16], p. 168.
\(^{28}\) An argument can be made that “it is usually a small section of the public who wish [sic] to use a particular public sector information product and that the user should not be subsidised by the general public and that he should make some contribution towards the costs of production.” See [39], p. 6. Similarly, see [24], p. 192 (“Since in the end public sector information is paid for by the taxpayer, the question could be asked if public authorities have the right to charge for the access to their information. On the other hand, some information is only requested by a very small group of interested parties, and it would not be fair either to let those requests be financed by contributions of the general public.”)
Negative reasons:
Linked to the question of abuse of power described above, if the government can charge for its information and holds a monopoly it can of course abuse the latter and charge excessive prices. This has happened often in the not too distant past. Before the PSI Directive, several firms complained that governments were engaging in price discrimination to drive its competitors out of business. Secrecy is not only bad in itself but it creates inequality as, if the state keeps the information, it creates an inequality compared to the public who does not. Secrecy may also lead to corruption and waste of public money. Another major reason is that it is unfair that the government charges for the information. It leads to double taxation since public sector information is financed by taxpayer’s money. It is also unfair or perhaps even illogical to charge the public for the information because by delegation, the public is in fact the author of the information and could even be said to own copyright or related rights (such as the *sui generis* right) in it, again by delegation.

Positive reasons:
The strongest positive reason is perhaps that the right of access to information is a human right. Another reason is that open access to PSI will increase participation in the decision process. With this information, the citizen can fully participate to the *res publica*. It should strengthen the confidence of the public in the administration. In addition, “openness to governmental processes is essential to good governments”. If the public knows about the decision taken in its name and has the possibility to express its views on them, then the quality of the decisions will improve especially because so the makers can say that “they are acting in the public view”. It is also accepted that public service is governed by the principle of gratuity. “The only possible interpretation of this principle is that the civil service takes in charge all the costs necessary for the accomplishment of its mission. Certainly, the cost of a copy excepted, such would be the case if the public information service consisted of a simple right of view on site.”

The most important reason, though, is economic. Public authorities are afraid to lose revenue by freeing up their information for which they used to charge. Loss of revenue is therefore the main argument against freeing government information. But in fact numerous economic studies and simply experience in various countries have amply shown that by giving the information away, returns from taxation will far exceed the revenue public authorities expect from the sale of their information in the first place. In other words, cost recovery is less economically efficient than

---

29 [5], p. 87.
30 [60], p. 9 citing Switzerland and Germany as examples.
31 [37], p. 4.
32 [16], p. 23.
33 [5], p. 87; [32], 273; [7], p. 6.
34 Extending the argument of [20], p. 243 and ff. who discusses Crown copyright.
35 Article 10 European Convention on Human Rights (ECHR).
36 [16], p. 22; see also [58], p. 94 and Belgian law relating to the publicity of administration of 11 April 1994 (stating that the law’s goal is to break the distrust and incomprehension of the citizen towards the public authority); [24], p. 185-186.
37 See preamble of the recommendation.
38 [37], p. 2.
39 [37], p. 4.
40 [43], p. 7.
41 [5], p. 86.
42 [60], [61], p. 137 ff. In his paper, Weiss shows the benefits of open access in contrast with cost recovery, giving examples of failed or limited cost recovery experience both in the USA and Europe. For this, he cites a great number of
open access. In yet other words, if PSI is freed, it will create a new information economy. Investors will want to invest in value-added information services. This will create jobs and new products on which the government will charge taxes. The monies collected from these taxes will be higher than the amount it would make by charging businesses for the raw data in the first place. Therefore, “the free availability of public information directly conditions the competitiveness of the European industry.” A recent study commissioned by the EU estimates the overall market size for PSI in the EU to an enormous 10 to 48 billion euros. Other negative aspects of cost recovery are that it prevents the constitution of transnational e.g. environmental or meteorological databases and often leads to cross-subsidies between government branches. If the government wants to continue its information business, the best solution is to separate the commercial activities of the government from the non-commercial ones.

There are of course instances where secrecy is crucial. There are therefore commonly accepted exceptions to the general rule that government information should be free. These exceptions are mainly:

- Information concerning international relations and national security. The main reason is that each country needs to retain some secrecy regarding its defence plans and also that it might embarrass the government if information is disclosed openly to other governments and therefore endanger national security.
- Information relating to law enforcement and the prevention of crime. If the government disclosed the ways it finds criminals it would be counterproductive.
- Discussions, advice given and opinions expressed with the government. This is because many decisions are generally taken after long discussions which are often hotly debated and people change their minds. If such discussions were always open, government employees would feel more constrained when expressing their opinions. This would damage open debate which consequently would lead to less good decisions, to the detriment of the economic studies to which the reader is referred to. For instance, a study analysed the difference between commercial meteorology markets in USA and Europe, showing that of the USA is much healthier than that of Europe, owing again to differences in data policies. See his p. 8. He concludes his study, p. 17, by stating that there is even consensus that charging at the marginal cost of dissemination for PSI leads to optimal economic growth and “far outweigh[s] the immediate perceived benefits of aggressive cost recovery”. On this reason, see also [7], p. 6. For a recent UK economic study, see [38]. Many other studies are also quoted in the Explanatory Memorandum to the PSI Directive, COM (2002) 207 final, p. 5-6.

43 [60], p. 2. In addition, the state might not always have the resources to add value to the information. So if it does not allow anyone to do so, such valuable added service will never come to existence, which will decrease social welfare. According to interviews on lawyers and non lawyers about planning and environmental legal information carried out by [32], p. 272-273 whilst basic information is useful, what users want is editorial input to control and make the basic legal information coherent.

44 See e.g. [24], p. 185-186. See also [7], p. 6, noting that normally the administrations’ profits from charging for PSI are very modest. See also [60], p. 14 noting that the UK “Met Office” decided to make significant categories of data available free of charge because it does not make many profits from it.

45 [17], p. 133.

46 [9].

47 [60], p. 3.

48 [58], p. 97.

49 [60], p. 18. In Sweden, where the state practiced price discrimination, the Statskontoret recommended that the commercial arm of the relevant governmental department be completely privatised and that its data be placed in the public domain. Ibid., p. 10. [58], p. 97 also notes that cross-subsidies between government branches has led to the splitting in some countries of the commercial arm of the public sector organisation. See also recital 9 of the PSI Directive which aims to avoid cross-subsidies.

50 [37], p. 8-17 explains their rationale in detail.
government and the public itself.\(^{51}\) Of course, when the policy has been decided, secrecy is no longer required.

- Information obtained in confidence from outside sources. This is an obvious application of the principle of confidential information. Another justification to this exception is that the government needs to maintain sources of information which “may dry up if its informants cannot rely on any assurance of confidentiality given to them by the government”.\(^{52}\)
- Information which if disclosed would violate an individual’s right of privacy
- Information which “if disclosed or disclosed prematurely, would confer an unfair competition on some person or would subject some person, or the government, to an unfair advantage.”\(^{53}\)
- Information covered by legal professional privilege.

It is in this context and for most of the reasons explained above that the PSI Directive was adopted.\(^{54}\) Its origins can be traced back almost 20 years ago now, when in 1989, the Commission already drafted some guidelines for improving the synergy between the public and private sectors in the information market\(^{55}\) whose goals were similar to those now enshrined in the Directive. In 1992, the Member States themselves had invited the Commission and the Council of the European Communities to legislate to set up an access to information policy to the information that the Commission and Council hold. These exhortations led to the adoption by the Council and Commission of decisions setting up such access.\(^{56}\) Three years later the European Parliament did the same. The right now appears in article 255 ECT.\(^{57}\) The Council carried out its duty mentioned in paragraph 2 of article 255 in 2001 with Regulation 1049.\(^{58}\) The right to access PSI now forms part of the duty of transparency which is enshrined in article 42 of the Charter of Fundamental Rights of the European Union of 7 December 2000, as modified 12 December 2007. There is also a right of good administration in article 41 of the Charter, which is based on decisions of the Community courts. It concerns among others the justification of administrative decisions.\(^{59}\) The PSI Directive has its more direct origins in the Green Paper on Public Sector Information in the Information Society, issued in January 1999. After the Green Paper, the Communication “eEurope 2002: creating an EU framework for the exploitation of public sector information” was adopted on 23 October 2001. It announced a Directive proposal which led to the Directive, which was enacted on 17 November 2003.

\(^{51}\) [37], p. 11. See also [16], who notes at fn. 34 who also notes that this way government employees do not lose their time by answering questions on policies not yet decided.

\(^{52}\) [37], p. 14.

\(^{53}\) [37], p. 17.


\(^{57}\) It states that “1. Any citizen of the European Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to European Parliament, Council and Commission Documents, subject to the principles and conditions to be defined in accordance with paragraphs 2 and 3. 2. General principles and limits on grounds of public or private interest governing this right of access to documents shall be determined by the Council, acting in accordance with the procedure referred to in article 189b within two years of the entry into force of the Treaty of Amsterdam. 3. Each institution referred to above shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents.”


\(^{59}\) [10], p. 18.
3.2. Analysis of the provisions of the Directive

As rather discretely stated in recital 5 of the Directive, the main goal of the Directive is to stimulate the growth of the European information market by broadly allowing its re-use. Access is normally already an established fact because of the Charter and national laws on public access to PSI. Indeed, Europe wants to become “the most competitive and dynamic knowledge-based economy in the world. Estimates had shown the information industry in Europe to be smaller by a factor of five when compared to that of the United States.” To do so, it sets out minimum harmonisation conditions so that this growth happens without distortions of competition between the companies exploiting that PSI. Indeed, before the Directive Member States had varied policies concerning PSI; in some countries, it was freely available, in others, not. Thus incidentally, the Directive also aims to improve access to information.

The main provisions of the Directive can be summarised as follows. Chapter I sets out general provisions. The Directive’s first article says that the “Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.” It then proceeds to exclude a number of documents such as most importantly, those on which third parties hold IPR, those of public service broadcasters and their subsidiaries, those held by educational and research establishments, such as schools, universities, archives, libraries and research facilities including, where relevant, organisations established for the transfer of research results, and documents held by cultural establishments, such as museums, libraries, archives, orchestras, operas, ballets and theatres. It also does not apply to documents which are excluded by national access regimes including on the grounds of the protection of national security, defence, or public security, statistical or commercial confidentiality (art. 1.2). The Directive does not apply when citizens or companies have to prove a particular interest under a Member State’s specific access regime to obtain access to documents. The Directive is without prejudice to those existing national access regimes (art. 1.3). This should mean that when a document falls within the scope of both the national law implementing the PSI Directive and the national law on access to PSI, if the latter asks the person to prove an interest, the former does not apply. In other cases where none of the laws required an interest, it seems that again the latter will prevail over the first.

The Directive then defines what it means by public sector body, document and re-use (art. 2). A public sector body is the State, including regional and local authorities and bodies governed by public law. The latter are then further defined and include among others bodies financed for the most part by the State (art. 2.2.c). As rightly noted by a commentator about the similar provision in the UK implementation of the Directive, it is safer to write down who owns the information so that it is clear whether the provision on re-use of PSI apply or not. It should be added that such agreement does not prejudge of the actual ownership of the information. Indeed, if the contract states that the information is owned by a private party but it has been financed in most part by the state the Directive should still apply. This is problematic though in the sense that it might be in the state’s (and not only in the private party’s) interest to ensure that the information processing...
(gathering, verifying, representing etc.) is financed in most part (50.1% should do) by the private party so that it escapes the provisions of the Directive. Indeed, the state might strike a deal with the private party to obtain a percentage of the profits or any other advantage. There appears to be no safeguard on this point in the Directive. The Directive does not further define the State. Does that include all three branches? This is not as straightforward as it appears as some national access regimes do not include legislative and judicial documents.67

A “document means “(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording); (b) any part of such content” (art. 2.3.). Recital 9 specifies that the definition does not include computer programs. Recital 11 further states that “it covers any representation of acts, facts or information - and any *compilation* of such acts, facts or information - whatever its medium (written on paper, or stored in electronic form or as a sound, visual or audiovisual recording), held by public sector bodies (emphasis added).” This should therefore include databases. It is clear that the documents must already exist in the sense the public authorities are not obliged to *produce or adapt* a document for an applicant (art. 5).68 Finally, to put it simply, re-use is defined as the use of documents, for commercial or non-commercial purposes, by private persons (be they citizens or companies) other than public sector bodies.

Article 3 then contains the general principle: “Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. Where possible, documents shall be made available through electronic means.” Thus, the Directive does not really sets an obligation to Member States at all.69 There is a pre-condition for re-use. The latter must be allowed. Who decides this? The State. Simply because of article 3, the Directive may well be a hit and miss. As well stated by some commentators, the “Directive Directive thus seems to contain merely a moral duty for public sector bodies to facilitate the re-use of their information.”70 Article 3 and recital 9 “leave[s] it open to any public sector body to refuse to licence PSI as long as a reason is given. If practiced extensively, this provision would undermine the entire Directive.”71 It is even doubtful that the Directive sets out a duty to supply the information in the first place.72 However, “whilst it does not oblige public sector bodies to permit re-use of their documents, there is a presumption that information will be available for re-use unless there are good reasons otherwise.”73 Also, many Member States have access regimes in place.74 But these may not be similar (the law being therefore not harmonised at EU level) and can always be repealed. Also, strictly speaking, if a Member State does not want to supply information, it can safely shelter itself under recital 9.

The second and third chapters of the Directive concerns the procedural aspects of requests for re-use. It requires that public sector bodies should process such requests within a reasonable time consistent with that already stated in national access regimes or otherwise no longer than 20 days (an additional 20 days can be added if the request is complex or extensive), and process the request as well as give access to the documents wherever possible electronically (art. 4.1, 4.2 and 5.1). If

---

67 See Belgium below.
68 Nor to provide extracts, in this case at the condition however that it would “involve disproportionate effort, going beyond a simple operation.”
69 This is clearly stated in recital 9.
70 [3], p. 255-256.
71 [7], p. 7.
72 [3], p. 255.
73 [4]
74 On these, see below section 3.
the public sector body refuses, it must state the reason and the means of redress if the applicant wants to appeal the decision (art. 4.3 and 4.4.). Article 6 deals sets out the principles governing charging. Where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Article 7 then sets out a transparency requirement according to which the public sector body must publish conditions and standard charges for re-use of its documents. They can allow the re-use only at some conditions if they wish but they should not restrict competition (art. 8). Any conditions for the re-use shall be non-discriminatory for comparable categories of re-use (art. 10). If a public body re-uses its information in competition with private entities, it must apply itself the same conditions that it applied to them. Exclusive agreements are also forbidden, except when they are in the public interest (art. 11). Finally, the Directive would not be so useful if Member States had no obligation to indicate what their PSI is and where it can be found. Article 9 therefore provides that “Member States shall ensure that practical arrangements are in place that facilitate the search for documents available for re-use, such as assets lists, accessible preferably online, of main documents, and portal sites that are linked to decentralised assets lists”.  

As can be seen, the text of the Directive does not address the issue of the clash between the administration’s IPR on its documents and its “obligation” to let third parties freely re-use them. However, recitals 22 and 24 contain some indication. Recital 22 first clearly states the intellectual property rights of third parties are not affected by the Directive. This is a simple logical reminder as the Directive only deals with state materials. It then defines intellectual property rights for the purpose of the PSI Directive. They include only copyright and related rights, including *sui generis* forms of protection but not industrial property rights. The recital goes on to say, more controversially: “The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). *Public sector bodies should, however, exercise their copyright in a way that facilitates re-use*” (emphasis added). Recital 24 simply states that the Directive is without prejudice to the Copyright in the Information Society and Database Directives. These recitals certainly are the fruit of compromises between Member States partisans of open access and those more inclined to be able to continue charging fees for their documents wherever possible. It puts the finger on the, admittedly dolorous, issue that the Directive did not tackle and which it should have in order to achieve proper harmonisation, namely whether there should be any intellectual property right on state materials. Recital 22 almost gives conflicting messages. Your IPR are not affected neither in their existence, ownership and even exercise but you should exercise your intellectual property rights in a way that facilitates re-use. In fact, the sentence is even less broad, because it only mentions copyright. This means that Member States could always argue that they can continue exercising their related rights and their database *sui generis* right as fully and

---

75 [4], saying that “for example where the PSB could demonstrate that no commercial publisher was willing to publish the document without an exclusive licence and this would affect the provision of a public service.”

76 National laws may already provide for this obligation. See e.g. the UK Freedom of Information Act; [47], at 333.

77 On the respect of international conventions, see also art 1(5) of the Directive.

78 [40], at 41, cited by [32] p. 249.
disregard the Directive. As can be seen, to say the least, the Directive leaves a wide margin of manoeuvre to Member States.\(^79\)

The Directive had to be implemented by 1 July 2005 but many Member States were late and some were sued by the Commission (e.g. Belgium which was last to implement\(^80\)). Article 13 requires the Commission to carry out a review of the application of the Directive by 1 July 2008. A consultation has been launched to this effect and has been extended until 15 September 2008.\(^81\) The consultation document asks among others whether it “would be appropriate to include cultural establishments, educational and research organisations and public service broadcasters within the scope of the Directive” and whether “legislative amendments [should] be introduced in the Directive to make it more efficient, and if so which ones and why. The Commission also asks whether guidelines on proper implementation and application of the Directive would be useful.\(^82\)

4. The national experience

As seen above, the relationship between the *sui generis* right and government data is barely addressed in the Database and PSI Directives. What about the national laws implementing them? I chose two countries which present some differences and some similarities in this regard, and not only because one is from the civil law tradition (Belgium) and the other from that of the common law (the UK). Although the object of the article is not to look at them in detail, the national laws on access to public documents which existed before the PSI Directive and complement it (or access regimes as the PSI Directive calls them) offer points of comparison too. The following sections on Belgium and the UK will review in turn the laws implementing the Database Directive, with a focus on the *sui generis* right, the laws on access to PSI or administrative documents and the laws implementing of the PSI Directive.

4.1. Belgium

Before tackling the Belgian and British implementations of the *sui generis* right, a quick reminder of the international and national context on copyright on official documents is in order. We shall see that the origins of the problem (i.e. that official documents can be protected by copyright) is that the major international copyright convention does not settle the question.

Article 2 bis(1) of the Berne Convention provides that “Union Members may exclude from protection political speeches and speeches delivered in the course of legal proceedings.” Similarly, article 2(4) provides that “it shall be a matter for legislation of the countries of the Union to determine the protection to be granted to official texts of a legislative, administrative and legal nature and to official translations of such texts”. According to some commentators, there are two categories of official material.\(^83\) The first category is composed of sources of the law of the land i.e. statutes, statutory instruments and regulations, decrees, bills, reports of parliamentary debates and records of parliamentary committees, and judgments of courts and tribunals. In the second category we find “documentation of government departments, official reports and other material emanating

\(^{79}\) [58], p. 106.

\(^{80}\) [7], p. 2. It notified the Commission that it had done so only on 8 May 2008.

\(^{81}\) See http://ec.europa.eu/information_society/policy/psi/docs/pdfs/online_consultation/review.pdf

\(^{82}\) A recent paper has set out answers and recommendations to the consultation on behalf of the important organisation ePSIPlus. For details, see [7], p. 2.

\(^{83}\) [51], n° 6.35, p. 254.
from or in connection with the administration of the government.”84 The ways countries treat these two types of official texts varies considerably. Civil law countries often provide that material in the first category is not protected by copyright.85 However, government reports and documents prepared by government departments are generally not within this exclusion and are therefore protected by copyright according to the normal rules.86 By contrast, in the UK and the Commonwealth countries and other countries whose legal system is based on British law, the rule generally is that the Crown has copyright in Acts of Parliament and other items of official material created under its control and the Parliament has Parliamentary copyright in bills and other parliamentary material created under its authority.

4.1.1. Copyright and database right

What is the situation in Belgium in relation to the sui generis right?

The provisions relating to the sui generis right of the 1998 Database Act87 implementing the Database Directive do not address the issue of ownership of sui generis right in state information. The exception for official acts88 was added neither to copyright nor to sui generis right for databases. This is so although article 6(2)(d) of the Directive authorised implicitly such exception as it allows Member States to introduce exceptions traditionally admitted by their copyright law.89 However, one of the Database Act’s provisions (the new art. 20 ter), which modifies the Belgian copyright act90, states that unless provided otherwise by contract or in the statute of civil servants, the employer is presumed to have the economic rights relating to databases created in the non cultural industry by one of its employees or agents in the course of their duties or following the employer’s instructions. Therefore, it is implicit that the state can have copyright in its databases. This is so even if according to article 8(2) of the copyright act, official acts of the authority are not protected by copyright.91 Indeed, the notion is not defined in the act but it is considered that not all acts emanating from the administration are official acts.92 In addition, the notion of “official act” does not equate with that of “public document”. There are many public documents which can benefit from IPR and which are not official acts.93 It has been submitted that “official act” in the copyright act means acts, regulations and executive measures, parliament works, judgments and indictments of the Crown Prosecution Service.94 The criterion for an act to qualify as official is

84 [51], n° 6.35, p. 254.
85 See e.g. art. 5 German law which excludes laws, orders, government reports and decisions and similarly, art. 8 of the Austrian law; art. 5 of the Italian copyright act, which excludes “official acts of the state and of the public administrations whether Italian or foreign”.
86 [51], n. 6.36, p. 255. See e.g. article 9 of the Swedish copyright act which excludes official maps from the exclusion of copyright protection. [50], p. 232. France has a tradition of excluding public documents but there are also exceptions to this exclusion. See [34], n° 106, p. 90.
88 See next paragraph.
89 [16], p. 621. It is arguable however whether article 8 (paragraph 2 at least) is an exception to copyright.
90 Copyright act of 1994 as last amended by the act of 22 May 2005, implementing in Belgian law the European Directive 2001/29/EC relating to the harmonisation of certain aspects of copyright and related rights in the information society, M.B. 27 May 2005, p. 24997 (“Belgian Copyright Act”). The term “copyright” will be used throughout this section to mean “authors' right” although technically speaking the terms “authors' right” should be used as Belgium is a civil country.
91 In addition, article 8(1)(2) states that speeches pronounced in deliberating assemblies, public audiences of courts and tribunals or in political meetings can be freely reproduced and communicated to the public, but the author alone has the right to publish them separately.
92 [53], p. 780 citing [21], p. 437. See also CTB/96/7 and CTB/96/122, cited by [48], p. 37.
93 [16], p. 622.
94 [16], p. 620, citing [55], p. 5.
supposedly the exercise by the authority of its *imperium*. The act also implies that the state can have copyright as its article 3(3) mentions it as a possible employer and provides the same provisions for agents as for employees. Thus there can be a conflict between the Belgian legislation implementing the PSI Directive and copyright law. Since the database act is silent on this issue concerning the *sui generis* right, by analogy with the situation under the copyright act, one could say that the same conflict also applies to the *sui generis* right.

4.1.2. Access to information regimes

In Belgium, since 1993, the right to access PSI is a fundamental right. Article 32 of the Constitution provides that "everyone has the right to consult each administrative document that concerns him or her and to receive a copy, except in the cases and conditions laid down in the federal law, decree or rule provided for in article 134". The *travaux préparatoires* specifically mention that this right is necessary to ensure democracy. "It is the condition *sine qua non* of the effectiveness of the other rights and freedoms recognised to the individual and at the collective level, the condition *sine qua non* of an independent and efficient administration, by the existence of a greater external control". This constitutional right establishes the rule of publicity, and even of transparency, of the administration. In fact, as we have seen in section 2.1, this duty of transparency is now enshrined in the Charter of Fundamental Rights of the European Union. But the right of access is not absolute because the Constitution allows the federal and federate entities to derogate to it. In Belgium, the federate entities, which consist in six different regions and communities, can in addition to the federal level take decrees to do so. All six levels of power as well as the provinces and municipalities have adopted quasi identical provisions, all loyally following the federal law.

So what does the bulk of this legislation provide? First, the notion of administrative authority is also not indicated in the Constitution. So most of the federal and federate entities decided to refer to the notion in the article 14(1) of the federal laws on the Council of State coordinated on 12 January 1973. This includes among other more obvious authorities (such as the King and the ministers), less obvious ones such as the Belgian national railway company (SNCB), the national office for employment (ONE), the Banking Commission (Commission bancaire) and professional organisms of public law such as the Order of pharmacists and the Order of architects when exercising administrative missions. Article 32 of the Constitution does not define the notion of administrative document either but its *travaux préparatoires* give the broadest possible interpretation: “any information, under whatever form, that the public authorities hold […] all available information, whatever the medium: written documents, sound and visual recordings including data comprised in the automated treatment of...

---

95 [16], p. 620, citing [55].
96 [33], p. 57.
97 The two terms are not synonymous. Publicity is institutional whilst transparency is relational. Transparency is constituted of three things: knowledge (the citizen knows what information the public authorities have on him), intelligence (the citizen wants to understand why a decision has been taken in his or her favour or to his or her detriment; thus the administration must justify its decisions) and participation. See [10], p. 15-17.
98 [53], p. 765.
99 Communities and regions take decrees. However, decrees of the region of Brussels-Capital are called “ordonnances”.
100 [53], p. 766-767; [16], p. 248. The federal law on the publicity of administration was adopted on 11 April 1994.
101 [33], p. 35-37; 64-65. Some entities however proceeded by enumeration.
102 Of course, documents issued by him within his functions. The notion does not extend to his private correspondence and other private documents. [33], p. 78.
103 Members of ministerial cabinets are excluded.
104 [33], p. 79-81. This therefore excludes documents when the orders exercise their judicial functions.
information. Reports, studies, even of consultative non official Commissions, some minutes and reports, statistics, administrative directives, circular letters, contracts and licences, public inquiry registers, exam notebooks, films and photos that a public authority holds”. The federal laws, decrees and ordonnances have adopted this broad definition. The notion covers all documents which exist before or after the entry into force of article 32. It covers not only administrative acts but also the preparatory documents to decisions. However, administrative authorities can refuse to communicate them if their divulgation could cause misunderstandings because they are incomplete. The Council of State has decided that model answers to exams for admission in the administration are administrative documents. Opinions given by the legislative section of the Council of State are administrative documents. But the notion of administrative document does not cover legislative and judicial documents including documents from judicial investigations. Are also excluded the acts of the executive branch which are closely linked to the legislative or judicial functions. This includes nominations and resignations of ministers and decisions of administrative jurisdictions such as the Council of State.

The content of the right and the procedural aspects are well described by Lewalle, Donnay and Rosoux. According to the different legislative instruments, everyone can consult the document, obtain explanations about it and receive a copy of it. It is forbidden to require from the citizen that he or she justifies a specific interest. Article 32 of the Constitution supposes that the consultation is free but that does not mean that it must be gratis, especially if a copy of documents is requested. For the administration to be able to charge a fee, there must be an authorisation by the statute as such fee restricts the fundamental right. The fact that this right is fundamental means that it must have the broadest interpretation possible. Thus according to the case law of the Council of State, the exceptions to the rights must be interpreted restrictively and enumerated exhaustively by the statute. Administrative authorities must expressly avail themselves of the exception in the law and indicate clearly the cause of its refusal and operate concretely a balance of the interests in question. There is an autonomous appeal system if the administrative authority has refused the request. First, the individual must address a reconsideration request to the administrative authority. At the same time, the individual can appeal to the appeal Commission established to that effect, the Commission d’accès aux documents administratifs (CADA). A further appeal can be made to the Council of State. Only the decision of the public authority on request of reconsideration can be attacked before the Council of State. At no time can the justification of an interest be asked to the individual.

What does the legislation say concerning the relationship between IPR and access to PSI? First of all, worryingly, the different legislative instruments only mention copyright whereas other intellectual property rights also risk having a great impact in this area especially the sui generis

---

106 [33] etc., p. 63. See e.g. article 1(2)(2) of the federal law of 11 April 1994.
107 [33], p. 83.
110 See decisions of the Council of State, the Constitutional Court and the president of the tribunal of first instance of Brussels cited by [33], p. 63-64. The latter court (for the decision see Journal des Tribunaux, 1998, p. 710) clearly said that it does not concern the legislative and judicial branches only the executive one.
111 [33], p. 77.
112 See p. 67-73. See also p. 60-61. Also note that article 13 of the federal law on the publicity of administration adds that the act does not prejudice other legislative provisions which give a greater publicity to administration.
113 [33] etc., p. 60, citing the travaux préparatoires.
114 After implementation of the PSI Directive, a new organ replaces the CADA, which has two sections, one for appeals relating to the publicity of the federal administration and the other for re-use of federal administrative documents. The regions and communities indicated it would be the CADA or the appeal organ equivalent to CADA. See [17], p. 152.
The texts provide that if the administrative document is protected by copyright, the author’s authorisation is not required for the consultation of the document on the spot. But the authorisation of the owner (i.e. author or person to whom copyright has been transferred) is required if the work is communicated by giving a copy to the person that requests it. It has also been held that before the public authority in question communicates the document it must check whether it is protected by copyright. The rule applies when the copyright belongs to a third party not the administration itself. Therefore, it does not apply when the administration is itself the owner of the copyright, otherwise article 32 of the Constitution could be useless. As implicitly reflected in the texts, the conflict between the right of access and copyright will only occur if the person asks for a copy of the document as there is no right to prevent consultation or access in copyright law. Therefore, there is no conflict if the administration can satisfy to the demands of transparency when it reformulates in a new document only the information or ideas contained in the document protected by copyright. Since the Constitution gives the right to receive the administrative document itself and not a rewording of it, the conflict will generally occur. However, it will not if the reproduction in question falls within one of the exceptions to copyright (e.g. private use, parody, research). When the applicant wishes to reproduce the protected documents commercially though, there will be a conflict.

The several appeal commissions have given interesting interpretations of the legislation. The Walloon Appeal Commission for access to environmental information (Commission de recours pour l’accès à l’information environnementale (C.R.A.I.E.)) held that the Walloon region should normally introduce a clause in the contract concerning architect studies it commissioned, transferring the copyright to itself. Therefore the region cannot oppose this clause to the party wanting access, otherwise the right to information would be completely emptied of its substance. But on the other hand, when copyright still belongs to the third party, a copy of the document can only be delivered after agreement of the owner. Only when the owner cannot be found and the authority has made reasonable efforts to trace him or her can it deliver the architect’s plans to the person who owns or possess the building and who asks the plans in order to restore the building. Only that person can have access to the plans in this case.

The commissions also held that there must be a balance between access and copyright protection. There will be abuse of copyright if there is a manifest disproportion between the usefulness for the

---

115 [16], p. 248. However, see article D19(1)(e) of a convention of the Walloon region, available on http://environnement.wallonie.be, cited by [22], p. 654, which includes copyright and rights on databases. Some legislative texts are more general and simply mention intellectual property rights. See e.g. article D19(1)(e) the Environmental Code of the Walloon region, available at http://wallex.wallonie.be/index.php?doc=4549
118 There is some controversy about this though. Some believe that as the notion of “making available” in Directive 2001/29 does not exclude an individual access to the work, it could cover digital access to administrative documents. They therefore think that to allow the consultation of a protected work without the copyright owner’s authorisation could infringe unless it falls within one of the exceptions to copyright. See [11], p. 292-293. Contra: [52], p. 64 and [53], p. 772 ff. We share Strowel and Van der Maren’s views and add that the exception of article 5.1 of the Infosoc Directive applies to consultation on the spot of electronic documents. In addition, the making available right implies that the individual chooses the place and the time it accesses the document. So as the law provides that he or she accesses it in person where the administration is located (“on the spot”) and according to its opening times, this does not fall within the ambit of the right.
120 [11], p. 291.
copyright owner to prevent the reproduction of the document and the inconvenience for the other party not to receive a copy of the document.\footnote{53}, p. 781. See e.g. C.R.I.E., aff. n° 282, 23 May 2005, Amén., 2006/1, p. 25-26; also available on http://environnement.wallonie.be

Until recently the case law of the C.R.A.I.E. invoked copyright on architectural plans to refuse their communication. Municipalities also continue to refuse this communication forgetting about the federal law of 5 August 2006 which made copyright a relative exception subject to balance of interests.\footnote{22}, p. 655. But generally, the C.R.A.I.E. proceeds to such balance which often favours the person making the request.\footnote{22}, p. 655 and decisions cited at her fn 58. These concerned cases where the copyright belonged to a third party. In three recent cases concerning copyright belonging to the administration, the Commission held that the public authority has a mission of public service and must make publicly available environmental studies that it commissioned even if the study were to be copyright protected, as the law favours without contestation the divulgence interest.\footnote{22}, p. 655, citing C.R.A.I.E., cases n° 253, 254 and 256, 19 September 2007 (these three decisions have been appealed before the Council of State).

In conclusion, copyright can clearly slow down the diffusion of information if works contain information.\footnote{53}, p. 785. Appeal commissions must therefore operate a balance of interests according to proportionality. The right to prevent copying will often yield to legitimate access demands because the usefulness for the copyright owner to prevent the reproduction of the document will weigh very little in the scale compared to the inconvenience for the other party not to receive a copy of the document.\footnote{53}, p. 785. The same may be said of the database right, because of its similar principle and its less generous exceptions.

4.1.3. Re-use of PSI

How has the implementation of PSI Directive changed or added to this state of affairs? Most of the implementation laws reproduce faithfully the provisions of the Directive. But they are provisions which are more specific than those of the Directive and some which create some substantial differences with it. The more detailed provisions are as follows. First of all, to abide by the Directive, the federal law, the Flemish decree and the ordonnance of the region of Brussels-capital deleted the provisions of the publicity of administration provisions which forbade the commercial reuse of documents obtained through the access right granted by these legislative instruments.\footnote{17}, p. 153. As to the definition of document, all legislative instruments except the Flemish decree clearly express the idea that it is not raw data but data which have been treated previously by the public authority.\footnote{17}, p. 127-155, at 138. Only completed documents that public authorities hold and decide to make available to third parties are covered.\footnote{17}, p. 139-140. All Belgian implementation instruments say this except one. As to the format in which the document must be supplied, the travaux préparatoires of the Flemish
decree provide an example of requests which ask for extracts and do not demand a disproportionate effort, which goes beyond a simple manipulation, namely requests which ask to collect single data from different documents and put them in electronic format.\textsuperscript{134} Specifically in relation to IPR, Belgian legislation not unnecessarily provides that if a document is protected by an IPR, in order to be able to make them available to third parties, the public authority must have ensured that the IPR were transferred to it.\textsuperscript{135}

An important difference with the Directive is that the Belgian implementation instruments go beyond the Directive on the charging issue. If an authority asks for a fee the amount cannot go over the marginal costs of reproduction and distribution. It is only when the creation of the document requires several additional operations that the fee can include the collection, production, reproduction and dissemination costs, whilst allowing a reasonable return on investment.\textsuperscript{136} This provision therefore enables the re-use of PSI much better than the Directive, at least in principle. Indeed, an additional operation is not defined. Therefore, it may be that public authorities will quickly argue that there are additional (albeit in reality artificial) operations in order to go beyond the minimal fee…\textsuperscript{137}

On the other hand, some of the Belgian implementation instruments contain more restrictive provisions. Administrative documents which are made available unconditionally by a public authority, and which stay that way, are excluded; in other words, they are not subject to a request for re-use.\textsuperscript{138} This should mean however that the offer to re-use must be unconditional not only the diffusion.\textsuperscript{139} However, this is not what happens in practice. Most Belgian public authorities make legal documents available through their own respective Internet sites. But their re-use is not always allowed. For instance, the Council of State (the highest administrative court) indicates that “the content of the decisions on this site is freely accessible to all. It is however forbidden to reproduce (…) the selection and organisation of this information without the express consent of the Council of State and if necessary third parties, owners of these rights”. The Walloon region stipulates for its legal database “Wallex” that “texts, metadata, non official considerations, classifications, lay-out, illustrations and other elements constituting the site “wallex.wallonie.be” are protected by law. All this data is the property of the Walloon region. Unless otherwise provided, all this data can be used freely but so long as mention of their source is made and only for non-commercial or advertising use.” The web site of the region of Brussels-Capital states that “the information can be used for your personal use but the parliament of the region reserves all its IPR on the portal and the information made available.” The Flemish Community’s web site states the same thing. Neither the Official Gazette nor the Juridat web sites (the latter is an official site which contains judicial decisions) mentions anything. But the Ministry of Economy’s web site (on which these two sites depend) gives the same indication as those of the Flemish Community and Region of Brussels-capital.\textsuperscript{140} However, notwithstanding these mentions, re-uses of this information, as they are not offered unconditionally, are subject to the laws and decrees on PSI. Unfortunately, users who are not legal experts will generally not know this…

\textsuperscript{134} [17], p. 148, also noting p. 147 that the federal law, the Walloon and French Community decrees and the ordonnance of the region of Brussels-Capital provide that the documents must be communicated in the form requested if they can be so communicated without causing exaggerated (“inconsidérés”) costs. The term “inconsidérés” is vague.
\textsuperscript{135} [17], p. 141.
\textsuperscript{136} [17], p. 149.
\textsuperscript{137} [17], p. 149.
\textsuperscript{138} [17], p. 141.
\textsuperscript{139} [17], p. 141.
\textsuperscript{140} These examples are cited by [17], p. 141-142.
All legal texts except the Flemish decree, which is a little vaguer, require minimal demands for re-use i.e. mention of source, mention of date of last update and non-alteration of data, which are not objectionable. However, the Flemish decree requires other mentions to be indicated i.e. the copyright notice (!), the commitment to inform the public authority of any error discovered in the information transmitted or grant the public authority a free access to the product created with the information furnished.\footnote{141} This is amazing as it amounts to some sort of payment \textit{a posteriori} for the information which surely implicitly goes against article 6 of the Directive. In the same vein, the Royal decree executing the federal law and the Flemish decree require that the request must also describe the reuse that is planned and the aim of this reuse.\footnote{142} This justification requirement does not appear in the access regimes reviewed above which state that one does not have to reveal the purpose for which one wants the document.\footnote{143} The Flemish decree gives a sensible reason why such information is needed. It allows the adaptation of the conditions that will be imposed to the person making the request. Reuse for commercial purposes can therefore lead to more fees being paid or to publication conditions being more restrictive than for non-commercial reuse.\footnote{144} It is a pity that the Directive has not clearly stated that no justification is to be asked to re-use the information, although it could be derived from article 1.3 that applicants do not need to prove an interest.\footnote{145} As can be seen, this silence allows Member States to require such interest. Also as we saw in section 2.1., the Council of Europe recommends that a justification should not to be given.\footnote{146} Requiring a justification might indeed deter requests in the first place or give a pretext for the state to refuse access. However, simply being required to state that it is for commercial purposes is not objectionable since the public sector bodies are allowed to charge for the information in this case.

Also concerning requests, the same legal texts stipulate that the request must be addressed to the public authority which has the administrative document in question or which has deposited it in the archives. Unfortunately, the public register does not state which authorities hold these documents. If there is no means of knowing which documents the public sector bodies hold, the PSI Directive has in practice no sense. This is the reason why article 9 of the Directive requires that Member States facilitate the search for publicly available documents. More research would have to be done to see if Belgium complies with article 9 on this point though.

\subsection{4.2. United Kingdom}

\subsubsection{4.2.1. Copyright and database right}

It has been said that \textquoteleft\textquoteleft[T]he United Kingdom is not a country in which ideas of free access to, and free use of, government information flourish with any vigour. Were this so, there would have developed, as in the United States, much more embracing notions of public domain material in which no copyright may be claimed.\textquoteright\textquoteright\footnote{147}
This statement still holds true as the UK is one of the very few countries in Europe which grants copyright and database right to all works produced by the three branches of the state. However, these copyrights are tempered by some exceptions in sections 45-50 of the act. Accordingly, copyright is not infringed by anything done for the purposes of reporting parliamentary, judicial, Royal Commissions or statutory inquiries proceedings (s. 45(2) and 46(2)). Copies of reports of Royal Commission and statutory inquiries can also be freely issued to the public (s. 46(3)). Section 47(3) provides that “where material which is open to public inspection pursuant to a statutory requirement, or which is on a statutory register, contains information about matters of general scientific, technical, commercial or economic interest, copyright is not infringed by the copying or issuing to the public of copies of the material, by or with the authority of the appropriate person, for the purpose of disseminating that information”. But section 47(4) restricts this exception by stating that “the Secretary of State may by order provide that subsection (1), (2) or (3) shall, in such cases as may be specified in the order, apply only to copies marked in such manner as may be so specified”. Finally, materials comprised in public records can be copied without infringing copyright (s. 49).

Likewise, if one closely examines the implementation of the Database Directive in the UK, one can say that Cornish and Llewelyn’s statement at the beginning of this section must be nuanced. Regulation 14(3) and (4) of the Copyright and Rights in Databases Regulations taken in 1997 provide, by analogy with Crown and Parliamentary copyright that the Queen and the Parliament can be owners of sui generis right in the databases they make, in those made under their direction or control and those made by their officers or servants in the course of their duties. Like section 45-50 of the copyright act but in broader terms, Regulation 20(2) (Schedule 1 of the Regulations) provides exceptions to database right for public administration. Relevant to our discussion, paragraphs 3(2) and (3) state: “(2) Where the contents of a database are open to public inspection pursuant to a statutory requirement, database right in the database is not infringed by the extraction or re-utilisation of all or a substantial part of the contents, by or with the authority of the appropriate person, for the purpose of enabling the contents to be inspected at a more convenient time or place or otherwise facilitating the exercise of any right for the purpose of which the requirement is imposed. (3) Where the contents of a database which is open to public inspection pursuant to a statutory requirement, or which is on a statutory register, contain information about matters of general scientific, technical, commercial or economic interest, database right in the database is not infringed by the extraction or re-utilisation of all or a substantial part of the contents, by or with the authority of the appropriate person, for the purpose of disseminating that information.”

Similarly to section 49, paragraph 5 of regulation 20(2) provides that “the contents of a database which are comprised in public records […] may be re-utilised by or with the authority of any officer appointed under that Act, without infringement of database right in the database.”

Schedule 2 of the Regulations, although not addressing specifically administrative documents, can also be mentioned. It provides for the imposition of compulsory licences when the Competition

148 S. 163-166 of the UK copyright act. The Parliament and the Crown have different copyrights. The Crown has copyright on acts, whilst the Parliament on bills. In addition, they own copyright in any work which is made under their control or by one of their employees, officers or servants if created in the course of their duties. There is controversy as to who owns the copyright in judicial decisions (judges or the Crown), but there is no controversy that copyright subsists in them. On Crown copyright, see [28], para 22.37; [6], p. 564-566; [2], p. 126; [54], p. 279-280; [50], p. 204-240; and in English in [1996] 10 IPJ 157.
Commission issues “a report concluding that a database owner’s refusal to grant licences on reasonable terms or conditions in a licence restricting the use of it by the licensee operate against the public interest. In such circumstances, the conditions of a licence can be unilaterally cancelled or modified and, in addition, a compulsory licence may be granted. The terms of such a licence can be determined by the Copyright Tribunal, if necessary.”

This provision nicely complements the application of national and Community competition rules and applies to all database owners including the state.

Therefore, the UK implementation is rather generous and already had provisions allowing for the broad re-use of PSI. It is not clear but it may be argued, according to these provisions, that the state cannot charge for the information it is obliged to give, which would be a major step beyond the Directive’s obligations. They are also no conditions attached (except of course that the contents of the database must be open for public inspection according to a statutory requirement) and all the database can be extracted, not only a substantial part. These provisions certainly do not cover all PSI as defined in the PSI Directive (because they do not cover all PSI bodies and all documents) but they have the merit to exist in comparison to the silence of the Belgian law.

4.2.2. Access to information regimes

Cornish and Llewlyn’s statement must also be played down because of the Freedom of Information Act of 2000 (FOIA) and other access to information regimes. Like the equivalent legislation in Belgium, the FOIA, provides a general right of access to PSI. The regulations implementing the PSI Directive therefore complement it as they promote the re-use of PSI.

The main provisions of the act can be summarised as follows. The act’s title is “an act to make provision for the disclosure of information held by public authorities or persons providing services for them (…)”. It also amends the data protection and public records acts. According to section 1 of the act, any person making a request for information to a public authority has the right to “(a) to be informed in writing by the public authority whether it holds information of the description specified in the requested and (b) if this is the case, to have that information communicated to him”. The act gives a long list of public authorities. This covers over 100,000 individuals and entities. “All information held by public authorities is accessible unless exceptions provided by law apply.”

There are two series of exceptions (in part II of the act, s. 21-44). Some are absolute in the sense that the public interest disclosing the information is outweighed by the public interest in keeping it secret. These exceptions are: information accessible to the applicant by other means, information supplied by or relating to bodies dealing with security measures, court records, parliamentary privilege, prejudice to effective conduct of public affairs (if the information is held by the House of Commons or House of Lords), personal information (not falling within the second category of exceptions), information provided in confidence and prohibitions on disclosure by or under an enactment or community law. The second set of exceptions is subject to the balancing of interests. These exceptions are: information intended for future publication, national security,
defence, international relations, relations within the UK, the economy, investigations and proceedings conducted by public authorities, law enforcement, audit functions, formulation of government policy, prejudice to effective conduct of public affairs (if the information is not held by the House of Commons or House of Lords), communications with Her Majesty and honours, health and safety, environmental information, personal information (not falling within the first category of exceptions), legal professional privilege and commercial interests.

The request must be in writing and provide the name and address of the applicant as well as the information requested (s. 8). The public authority can charge a fee (s. 9). But fees are subject to regulation by the Secretary of State to avoid excessive prices. In practice, the law is so complex that authorities seldom charge for providing information. The authority must reply promptly and in any event no later than 20 days after the request was received (s. 10). If it refuses, the authority must state which exemption applies and why it does. Any person can complain to the Information Commissioner about such refusal (s. 50) and he or she can decide that the authority has failed to comply with its duty and indicate how it can remedy it. Such decisions can have binding character (s. 52). If the authority fails to comply, the Commissioner can take the matter to a court (s. 54). Both the applicant and the authority can appeal decisions of the Information Commissioner before the Information Tribunal, whose decisions can be appealed on points of law before the High court (s. 57-59). The Information Commissioner can give recommendations to public authorities and submits an annual report on the exercise of its function to both Houses of Parliament (s. 48 and 49). In order to facilitate access, public authorities must publish schemes in which they disclose the information they publish or intend to publish, the manner it will be published and whether the material will be available free of charge or not to the public (s. 19). What is important to note is that the FOIA does not grant a right to reproduce the information, so that authorisation must always be asked. This is where the PSI regulations are useful.

4.2.3. Re-use of PSI

Finally, is the same statement outdated thanks to the implementation to the PSI Directive? Most likely not, as an examination of the text of the Re-use of Public Sector Information Regulations 156 shows that it is quasi identical to the Directive’s text even if they are some slight and some more important differences. Of course, the public sector bodies are different in every country. Regulation 3 provides a precise list of those bodies. The complaints procedure is also laid out in more detail in the regulations (reg. 17-21). More importantly, regulation 6(d) provides that “a request for re-use shall state the purpose for which the document is to be re-used (emphasis added).” Although the Directive is silent on this point, it would be logical for the reasons seen above (section 3.1.3) that no justification be asked. Like at some levels of power in Belgium, the right of re-use given by the British text is for this reason considerably weakened. This is amplified by the fact that the distinction between access and re-use is unclear so that the same bodies are subject to both the FOIA and the PSI regulations and thus face to conflicting obligations. 157

Since the Office of Public Sector Information (OPSI), together with Her Majesty's Stationery Office (HMSO), is the body responsible for the management of most of the UK government’s intellectual property 158, its current policies provides a useful example of the practice based on the PSI

155 [59], p. 59.
158 [56], also noting that “OPSI is also the regulator of public sector information holders for their information trading activities.” C. Tullo is Director of the Office of Public Sector Information and a Director of the National Archives with
Firstly, it is worth noting that the Crown has waived its copyright on UK legislation.\textsuperscript{159} Thus, when accessing legislation on the OPSI web site, the documents reproducing the legislation contain a statement which gives a free but conditional licence. For instance, the text before the PSI regulations notes that “The legislation contained on this web site is subject to Crown copyright protection, it may be reproduced free of charge provided that it is reproduced accurately and that the source and copyright status of the material is made evident to users. (...) The text of this Internet version of the Statutory Instrument which is published by the Queen’s Printer of Acts of Parliament has been prepared to reflect the text as it was made. A print version is also available and is published by The Stationary Office (...).” The web page gives a link where the statutory instrument can be purchased. In the case of the PSI regulations, the price is £3. It is therefore clear that all government legislation (at least that made available on the OPSI web site) is freely accessible and re-usable. The existence of copyright or related rights in single elements of a database such as that of that OPSI makes available on its web site, directly affects the exercise of the database right. Indeed, even if an insubstantial part is extracted lawfully under the right, it must not infringe any right in that part itself (art. 7.4). The Crown waiver solves this problem.

On its FAQs web page, the OPSI web site goes on to say that Crown copyright includes not only legislation, but also government codes of practice, reports, official press releases, government forms and many public records. It also states that databases enjoy separate protection under the database right regulations so that they are not automatically covered by Crown copyright.\textsuperscript{160} OPSI also offers a “click-use licence” for other Crown copyright documents than legislation, and also for PSI and Parliamentary copyright. There is no charge to access all this information through this licence but there may be if the user contracts under the value-added licence depending on the type and amount of Crown copyright information [sic]\textsuperscript{161} re-used.\textsuperscript{162} However, other government documents which are managed by trading funds, such as the Ordnance Survey, still charge for their documents.\textsuperscript{163} After this taking stock exercise, the picture is therefore mixed. Whilst a huge progress has been made by the government through the waiver of its Crown copyright on many documents, a lot of other government documents are available but still at a charge. It is not clear whether trading funds comply with the Directive and corresponding regulations as they must make profits. Indeed, recently, the Treasury “indicated that in a climate of mounting concern about the soundness of government finances, the last thing it needs is an intellectual case for abolishing a stream of revenue”.\textsuperscript{164} So as has been rightly stated, “what is clear is that matters really have moved these past [few] years” in the field of access and re-use of government information be it or not protected by IPR.\textsuperscript{165}

\textsuperscript{159} See \url{www.opsi.gov.uk/about/faqs-crown-copyright.htm}
\textsuperscript{160} As we have seen above, this is partially true as the regulations more or less mimic the copyright act in this respect.
\textsuperscript{161} Since there is no copyright in information as such, this statement from the web site must be a figure of speech. Private parties will only have to pay if they re-use expressions and not only ideas and information from the Crown copyright documents.
\textsuperscript{162} See \url{www.opsi.gov.uk/click-use/index.htm}
\textsuperscript{163} \cite{56}, 272-274. This is because they are obliged to achieve a return on their investment. See also \cite{60}, [38].
\textsuperscript{165} \cite{47}, p. 335.

5.1. Preliminary question: does the state really have sui generis rights?

The preliminary question to the question posed in this article is whether the database right really subsists in most state databases. If not, then the answer to the question whether the PSI Directive trumps or at least dampens down considerably state sui generis rights is moot. One may wonder why this preliminary question should even be asked. Indeed, at first sight, it seems like most state databases will meet the requirements: their elements will be independent and logically organised and will be very substantial in size. Most of the time, the state’s sui generis right will last forever as it will regularly update its databases. A close examination of the Database Directive’s provisions on the sui generis right shows that it is not so clear and there is at least some uncertainty in this respect but that it cannot be excluded that in some cases, the state owns such sui generis right.

The Directive itself does not address this issue specifically so it can be said that state databases are included so long as they fulfil the requirements of the right. Moreover, the Directive and its preparatory materials implicitly indicate that states can benefit from the right. First, according to article 6(2) of the Directive, Member States can apply traditional exceptions existing in copyright laws for databases (which arguably include the exclusion of official material\textsuperscript{166}) but the Directive does not provide the same clause for sui generis right.\textsuperscript{167} This means that since the list of exceptions for to the rights of extraction and reutilisation is exhaustive, public sector bodies are entitled to sui generis right on their databases. Another perhaps stronger indication is the deletion of article 8 of the Directive Proposal from the final text of the Directive. This deletion implies that the state bodies can own sui generis rights.

So far so good. But can the state really be a database maker? The definition given by recital 41 of the Directive is that a database maker is “the person who takes the initiative and the risk of investing.” Surely the state most of the time takes the initiative to create databases; the question is therefore whether it can also be said to invest in the making of databases. If not, it cannot be considered a maker (or producer) and in any case does not fulfil the requirement of substantial investment that triggers the right’s subsistence. It is disputable that the state takes a financial risk when it creates databases.\textsuperscript{168} It already has the money to create the database in the first place and if not, can and certainly will collect it, with the almost total guarantee of being paid, from the taxpayer… Or state databases are generally not based upon a substantial investment which shall be recuperated on a market.\textsuperscript{169} As clearly exposed by a commentator, “public authorities collect and maintain governmental data because they have a legal mandate to do so; unlike private authors and publishers they do not need economic incentives to do their legal duty.”\textsuperscript{170} However, as the current interpretations of the terms “maker” and “investment” is either scarce or uncertain\textsuperscript{171}, there is

\textsuperscript{166} In most Member States however, official material is not covered by an exception, but is more categorically, excluded subject-matter so that copyright does not even subsist in the first place.

\textsuperscript{167} [44], p. 60.

\textsuperscript{168} In this direction [57], § 87b, para. 25 cited by [31].

\textsuperscript{169} This is if the state does not charge for the data. But even if the state were to charge, it would not mean that it had invested in the first place if the database making activity is fully funded by public money. An example of databases not (fully) funded by public money is the trading funds in the UK. On these see [60], [38].

\textsuperscript{170} [41], p. 8-9, adding that “logically, there is no justification for copyright in basic public information including actual data, the basic text of statutes and judicial opinions, and bitmaps or representation of geographic data”. The same could by analogy be said for the sui generis right.

\textsuperscript{171} See [3], p. 146; [12].
uncertainty on this point. It may then be argued that even if the state owns the databases it creates, the supposed investment the state makes is not qualifying because most of its databases are by-products of its activities (so-called spin-off databases). In other words, the information is not gathered, verified or presented but as in the British Horseracing Board and Fixtures Marketing cases\textsuperscript{172}, it is generated or there is no separate investment in the collection, verification or presentation of it. Although this is difficult to argue on the basis of the above-mentioned ECJ cases, the state might still in the end prove a \textit{sui generis} right. Anyway, in other cases, a particular state entity will really have collected, verified or presented data rather than created it (e.g. meteorological, geographical data).

As can be seen the cases where the state can benefit from a \textit{sui generis} right are normally rather rare. In the cases in which the public sector is uncertain it benefits from the right, it has two possibilities to help itself. First, it may try and ensure that its data is protected by outsourcing its collection, verification or presentation to the private sector, thereby also probably breaching the PSI Directive. This very question was addressed in the question the German Federal Supreme Court asked to the ECJ in the \textit{Verlag Schawe} case.\textsuperscript{173} Second, in any case, even if the \textit{sui generis} right did not accrue, the fact that the state in most cases is the only source of some data gives it a monopoly position, enabling it to charge a monopoly price. In these cases, of course, current EU and national competition laws can be of some help.\textsuperscript{174}

5.2. \textbf{Does the PSI Directive trump or dampen down objectionable state \textit{sui generis} rights?}

As the state will in some cases own \textit{sui generis} rights, the question posed by the article can now be tackled. Does the PSI Directive trump or dampen down such objectionable \textit{sui generis} rights? The answer, depending on how one reads the Directive, can be: not sure, not really or absolutely not. In any case, it is definitely unclear whether it does. The main reason is because article 3 and recital 9 do not oblige the state to allow the re-use of its documents. As stated in section 2.2, the Directive thus seems to impose a mere moral duty for public sector bodies to facilitate the reuse of their information.\textsuperscript{175} But even this is unclear because of conflicting recitals (mainly recitals 9, 22 and 24). Obviously the whole goal of the Directive was to facilitate re-use so in doubt, one could argue that the provisions should be interpreted in this light. More fundamentally, the Directive can be criticised for not tackling the core of the problem, namely whether the State should be allowed to own copyright and related rights (including the \textit{sui generis} right) on its documents.\textsuperscript{176}

There are other reasons why the PSI Directive does not trump or even dampen down the state’s \textit{sui generis} rights. First, it is unclear whether all three branches of the state are clearly within the scope of the Directive. Second, the fact that the Directive does not prevent public sector bodies to ask the

\textsuperscript{172} See above fn. 11.

\textsuperscript{173} The questions were as follows: “1. Do Article 7(1) and (5) and Article 9 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases prohibit a legal provision of a Member State, according to which an official database which is published as a matter of general information for official purposes (in this instance: a systematic and complete collection of all calls for tender documents emanating from a German \textit{Land}) does not benefit from \textit{sui generis} protection under the directive? 2. If the answer to Question 1 is in the negative: is this also the case where the database is constructed not by a public body but by a private undertaking on its behalf, to which all bodies of this \textit{Land} issuing calls for tender must directly submit their calls for tender documents for publication?”

\textsuperscript{174} See [14], p. 206-225, discussing the UK Atheraces case (Atheraces Ltd, Atheraces (UK) Ltd v. British Horseracing Board Ltd, BHB Enterprises Plc [2007] EWCA Civ 38) which involved such a situation.

\textsuperscript{175} See [3], p. 256.

\textsuperscript{176} [40], at 41, cited by [32] p. 249.
applicant to prove an interest has allowed Member States to provide they can thereby discouraging (at least some) requests in the first place. Third and most importantly, public sector bodies can charge for “the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment”. This is very close to the price that a database producer would charge in a competitive environment, even if the firm holds a *sui generis* right. It is however highly disputable that the public sector’s mission is to make profits. However, many studies showed that full cost recovery is economically inefficient. One study showed that public sector information available in digital form should be made available by the public sector at no more than the cost of dissemination whilst another study also shows that data should be accessible at no more than marginal cost of reproduction. Most levels of power in Belgium has opportunely gone beyond the Directive’s obligation by requiring that the fee does not go over the marginal cost of reproduction and dissemination (unless the request requires several additional operations on the part of the public sector body). Unfortunately, the Flemish community even requires the applicant to grant free access to the state to the product it made out of the information so communicated… Fourth, whilst the Directive arguably addresses competition concerns by prohibiting exclusive arrangements (art. 11) and arguably excessive prices (art. 6, 8) as well as forcing the state to apply to itself the same conditions as private companies if it decides to market its own data (art. 10), the Directive will in many cases not push the prices down by much in comparison with other database markets. Some discriminatory practices, exist; for instance “the inclusion of a small proportion of third party data on a data set exempts the whole data set from the provisions of the Directive” and sometimes “subsets of data are priced at the same (higher) cost of licensing the whole set”. There is also no guidance on how the term “reasonable” in article 6 might be measured. “If applied widely to establish high charges based on no transparent calculation of how prices were arrived at, this provision could also undermine substantially the implementation of the Directive in the longer term by enabling public sector bodies or their agencies to trade in manner which is essentially commercial and competitive with private sector re-users”.

The overall picture is therefore rather grim. In plain words it can be summarised as follows. We are not sure whether the state might have *sui generis* rights in some its databases. If and when it does, the PSI Directive does not change much to its rights, if anything: the state may not charge excessive prices - but what is an excessive price anyway? - and that was already prohibited by competition law. One can wonder why we are paying the European institutions. Or maybe we should put this example down to the fact that in democracies, many decisions and solutions are inevitably the fruit of compromises. But then, it is generally better not to vote a law than to end up with a bad one, worse than the *status quo*… The consolation prize is however that the Directive also applies to the Community institutions. *De lege ferenda*, it would obviously make sense that the EU excludes once and for all state databases from copyright and *sui generis* right protection altogether (as many Member States have done long ago for copyright laws anyway, it should not be so difficult).
Alternatively, in the same vein, the EU should oblige “Member States to extend, mutatis mutandis, all the exemptions and limitations applying to works protected under copyright also to sui generis protection of non original databases. The obligation should be phrased so as to establish a dynamic link between both fields, to the effect that limitations set out in new copyright legislation would automatically become applicable, under the suitable terms and circumstances, also to the sui generis right.185” “Otherwise a certain bias with respect to the sui generis right would be perpetuated and cemented in the system of Community law although there is no reason, for example, to exclude digital private copying in this field completely (see Art. 9 (a) Directive) as compared to the situation in general copyright law where this exception remains an optional possibility for the Member States (see art. 5 (2) (b) Infosoc Directive).”186

5.3. Solutions based on the Database Directive

Whilst waiting for a European Godot, what solutions are there to remedy this problem de lege lata? A strict interpretation of the Directive in the footsteps of the ECJ 2004 decisions will already restrict the number of cases where the state owns sui generis rights. Courts should in particular not allow the circumvention of the Directive by the state through the outsourcing of its database activities to private companies. However, according to some, this solution “fails with respect to collections of data which have been compiled by private commissioners which by their service fulfil a public task.”187 Another solution can be based directly on an analogical and teleological interpretation of the Database Directive. Courts could apply the exception or exclusion of official documents to the sui generis right by analogy with their respective copyright laws.188 Indeed, article 13 of the Directive included a reference to laws on access to public documents to complement article 9 because the latter does not explicitly provide an exception for databases made by governmental bodies. 189 Certainly, “[t]he admissibility of an equivalent exception for databases should preferably have been made clear in the Directive by expressly including such an exception in articles 6 and 9.”190 The application by analogy of the copyright exception to the sui generis right would also avoid contradictions between different Directives in the field of copyright and related rights (such as the Database and Infosoc Directives).191 It is a shame that the questions asked to the ECJ by the German Federal Supreme Court have now been withdrawn as they addressed these two points.192

5.4. Solutions based on national laws

The second type of solution is based on some national laws, mainly those of the Netherlands and France, which could serve as examples to other Member States. Article 8 of the Dutch Database Act is refreshing. It reads: “1. The public authority shall not have the right referred to in Article 2, paragraph 1, with respect to databases of which it is the producer and for which the contents are formed by laws, orders and resolutions promulgated by it, legal decisions and administrative decisions. 2. The right, referred to in Article 2, paragraph 1, shall not apply to databases of which

185 [31] citing [27], p. 557.
186 [31]
187 [31]
188 For similar arguments, see [29], p. 790; with the same result on the basis of a fictive waiver of rights, [18], n° 611 ff; See [30] [2007] GPR, p. 190-194 commenting on the Decision of the Bundesgerichtshof (German Federal Supreme Court) of 28 September 2006 [2007] GRUR, p. 500-502.
189 [18], p. 177, n° 730.
190 See [3], p. 254-255.
191 [31]. See further [30].
192 The text of the questions is reproduced at fn. 173.
the public authority is the producer, unless the right is expressly reserved either in general by law, order or resolution or in a particular case as evidenced by a notification in the database itself or when the database is made available to the public.” 193 The Netherlands felt that it was desirable to introduce equivalent provisions to articles 11 and 15(b) of the Dutch Copyright Act for the *sui generis* right. 194 This is in line with one the solutions advocated above. Sadly, article 15(b) of the copyright and 8(2) of the Database Act specifically provide that the *sui generis* right can be reserved. It would have been in the public interest (including that of taxpayers who can end up paying twice for the same thing) “to deny, on principle, a public authority any rights in databases containing laws and the like”. 195 Unfortunately as well, some Dutch commentators believe that when a database does not qualify for copyright or *sui generis* right protection, it can still benefit from the *geschriftenbescherming*. 196 We think along with other commentators that this is an unfortunate omission by the Dutch legislature. 197

The French experience of ensuring access to legal databases made by a public authority is also worth noting. A 2002 Decree imposes a legal duty on the French government to produce databases containing (inter)national legislation and case law and to make available on the Internet and to licence their contents merely against distribution costs. 198 This decree seems to serve the public interest better than the Dutch provision, as it puts the French government under a legal duty to actually produce such online databases, which the Dutch law does not so require. On the other hand, these French legal databases do enjoy protection by the *sui generis* right so that a licence is required to use substantial parts, unlike such databases made by a Dutch public authority. 199

The efforts of these countries go in the right direction although they still are not sufficient. Several ways to improve the access and re-use of PSI based on the French and Dutch experience could be found. For instance, a combination of the provisions of French and Dutch laws would already form a better system. But arguably excluding all PSI from IPR would be the clearest, simplest and most effective solution. Despite this general unsatisfactory state of affairs, it is reassuring to see, that national laws on access to PSI and their current practice (at least that is what the examples of the UK and Belgium show) already generously allow access, if not re-use, to PSI. 199 In both countries, applicants must not justify their requests of access. In Belgium, as the right to access PSI is protected constitutionally, it must be interpreted broadly and exceptions to it, restrictively. Accordingly, most of the case law states that public authorities must grant access to their documents

---

193 Databankenwet, Act of 8 July 1999, Staatsblad, 303. This English text appears in [3], p. 221 without indication it is an official translation of the Dutch text.
194 See [3], p. 221-222 citing the Explanatory Memorandum to the Database Act, Kamerstukken II 1997/98, 26 108, no. 3, p. 20. Article 11 of the Dutch copyright act establishes that no copyright exists in laws, orders and resolutions promulgated by the public authorities, legal decisions and administrative decisions. Article 15(b) states that reproducing or making available works which were made available by or through the public authorities is not considered an infringement of copyright, unless the copyright is explicitly reserved.
195 See [3], p. 223.
196 [49], para. 3.57, p. 136 and [45]. The *geschriftenbescherming* is the ancestor of the *sui generis* right, as it was taken, along with the Nordic catalogue rule, as a model for it. On those see e.g. [23], p. 83; [25], p. 67.
197 See [3], p. 223; [18], p. 151, n° 614.
199 In addition, many Member States also have laws, which are often based on European Directives, requiring former state monopolists (e.g. privatised telecom operators or broadcasting corporations) to grant access to information. See [3], p. 254-255, citing at fn. 101 the French Code of Posts and Telecommunications which requires France Telecom to supply anyone who requests it with “a consolidated list of all the information contained in the general telephone directory (the *annuaire universel*) at a price reflecting cost.”
even if they have an IPR on them and must even grant access to IPR-protected subject-matter which belongs to third parties if it is in the public interest. Unfortunately however, documents subject to the Belgian access regimes only include those of the executive branch and not the legislative and judicial branches. In the UK, the database regulations already free up a number of public databases and also allow their re-use. In addition, the FOIA forces the state to adopt publication schemes and although the Crown has waived only some of its copyright, charges are rarely sought for accessing PSI. There is an important dent in this generally satisfactory situation is the continuing charging practice of trading funds.

6. Conclusion

So does the PSI Directive affect the state’s *sui generis* right? The answer is a rather clear no. Nevertheless, the Belgian and British national implementations of the Database and PSI Directives have in some ways gone beyond the Directive’s obligations, which is a good start. Also their national access regimes are generally rather generous when it comes down to access but also re-use of IPR-protected PSI. Although the review of the PSI Directive may come a bit too early, it will be interesting to read the results of the consultation launched in anticipation of the Directive’s review. When reviewing the Directive, the Commission should compare the situation before and after the Directive. Proper (economic) studies should again be made to see if the Directive goes far enough or not. Most probably it does not but it cannot be said that it is such a bad start. At least the intention was there. It will also be interesting to see what the second review of the Database Directive leads to, which should practically be done at the end of this year as well. More needs to be done if the EU information industry is to compete on a level-playing field with the USA but more importantly for the citizen and in fact the whole world to be adequately informed. This is of the utmost importance in our times in view of the increasing dangers caused by humans to the planet, not to mention global warming. If we want to react adequately, we need information and such information is generally detained by governments. As we have all subsidised it, we arguably all have a right to have this information available free of charge and to re-use it as freely as possible. For such acute global problems, time is of the essence. Public sector information needs to be freed now not in five or ten years’ time.

7. References


---

200 [7], p.2. As many Member States have just finished implementing the Directive, there is not yet much practice or case law.

201 Technically the first review should have been occurred in 2001 but happened in 2005. A new review must be conducted every three years (art. 16(3) of the Directive).

202 [17] at 134 also notes that we can legitimately worry about the fact that the information services market is still dominated by the USA, as this leads researchers, companies and even European decision-makers to depend on American sources and therefore, there is a danger on relying on a single source in case of refusal to supply or simply source dry-up.


DIGITAL HERTITAGE & COPYRIGHT

Erich Schweighofer¹, Andreas Rauber²

Abstract
Mere preservation of the artefact is no longer sufficient to ensure long-term accessibility of digital content. New conservation concepts called migration and emulation are thus needed to avoid the risk of losing electronic publications. Content and “look and feel” can be only preserved if artefacts are migrated to new IT environments or emulation of former IT environments is done. Thus, changes to the object as a result from preservation actions are unavoidable. The WIPO Copyright Treaty leaves this important question to the national legislation. However, limitations and exceptions are subject to the so-called three steps test. So far, national laws are quite conservative and extend only the obligation to deposit of electronic off-line and on-line materials. Extensive conservation rights are still subject to contractual arrangements. Thus, an international solution to these challenges in the form of treaties or private licences is definitely desirable for the near future.

1. Introduction

Digital media has a relatively short life expectancy as the digital publishing media on which they were originally made available deteriorates quite fast. Additionally, digital materials become unreadable due to changes in coding, formats, software, operating systems and hardware. Gone are the days when the preservation of the artefacts was sufficient. Thus, preservation of the documentary heritage, or as the UNESCO [26, 27] names it, the Memory of the World, requires a decisive change in the methodology. Otherwise, digital information is in serious danger of being lost, creating a so-called digital “Dark Age”. Existing protection of knowledge rights however still focuses on the artefact and does not leave sufficient space for required presentation steps.

2. Recent initiatives

Following the UNESCO charter on the preservation of the digital heritage 2003, many states have taken initiatives for implementing the goals of the charter. Of particular relevance are EU initiatives.

Digital libraries are a key aspect of the i2010 initiative of the European Commission [6]. Following a request by the Heads of State and Government of France, Germany, Hungary, Italy, Poland, and Spain of 28 April 2005, the digital libraries initiative was established [7] and strongly supported by the Culture Council of 14 November 2005. Further, the Commission adopted a Recommendation on the digitization and online accessibility of cultural material and digital preservation [8], calling on

¹ University of Vienna, Center for Computers and Law, Department of European, International and Comparative Law, A-1010 Vienna, Schottenbastei 10-16, Austria, Erich.Schweighofer@univie.ac.at.
² Vienna University of Technology, Department of Software Technology, A-1040 Vienna, Favoritenstrasse 9-11, Austria, rauber@ifs.tuwien.ac.at.

Part of the work presented in this paper is partially supported by European Community under the Information Societies Technologies (IST) Programme of the 6th FP for RTD – Project IST-033789.
the Member States to take concrete measures. The Education, Youth and Culture Council welcomed this Recommendation and unanimously adopted very positive conclusions.³

Major support for the digital libraries initiative will come from co-financed research. The Sixth and Seventh Framework Programmers for research and technological development⁴, the eContentplus and Culture programmes and regional funds can be used for related research and actions. An overview of these activities can be found at the related websites.

### 3. Solutions for physical deterioration and digital obsolescence

As media for digital data deteriorates after some decades or even after years, the preservation of artefacts is no longer sufficient [2, 4, 9, 16, 32]. Due to rapid development, technology for using digital data is abandoned (e.g. software or decoding technology is no longer used or a hardware device no longer produced).⁵ The resulting short life expectancy of digital media requires that the intertwined linking between artefact and content must be given up for the sake of preservation. By a new approach of preservation, the so-called “significant properties” of a digital object, e.g. content, meta data and “look and feel” have to be preserved to a sufficient degree. Interaction with and modification of a digital object may be necessary at several levels and during several stages of a digital preservation process. It is quite obvious that a co-operative rights management has to replace existing one-off solutions of delivery of works to preservation institutions. In 2006, the Online Computer Library Center (OCLC) published a four-point strategy for the long-term preservation of digital objects:⁶ The risks for loss of content created by using technology variables such as commonly used proprietary file formats and software applications should be assessed. The digital content objects should be examined to determine type and degree of format conversion or other preservation actions. Appropriate metadata needed for each object type and how it is associated with the objects has to be determined. Access to the content has to be provided.

During the last couple of years, a lot of research has been done to define, improve and evaluate single preservation strategies [26]. The main proposed methods are refreshing, migration, replication and emulation. Research on technical preservation issues is focused on two dominant strategies, namely migration and emulation. Scientific results on migration, which is at the current time the most common preservation strategy, were published for example by the Council of Library and Information Resources (CLIR) [13], where different kinds of risks for a migration project are presented. Migration requires the repeated conversion of a digital object into more stable or current file formats.

A migration system for preservation of any type of document, created on any application or platform, and delivered to the archives on any type of digital media is presently jointly developed by The National Archives Electronic Records Archives and Lockheed Martin.[20]

Work on the second important preservation strategy emulation was advocated by Jeff Rothenberg together with the CLIR [21], envisioning a framework of an ideal preservation surrounding. More recently, the Universal Virtual computer (UVC) and modular emulation [29] have been proposed as promising solutions [25]. Emulation aims at providing programs that mimick a certain environment,

e.g. emulating a certain processor or emulating the features of a certain operating system, allowing users, for example, to run Microsoft WORD on a Linux operating system using the WINE windows emulator. Specifically for more complex digital objects, such as database applications, games and interactive animations, this may well constitute the only possibility to provide a reasonable preservation of the core characteristics of a digital object.

In recent years, more focus was given to the preservation of metadata. This digital file includes information on creation, access rights, restrictions, preservation history, and rights management. ASCII is considered as the most durable format for metadata, however, the information should be structured using XML.[18]

In order to support these activities, ISO has developed the Reference Model for an Open Archival Information System (OAIS) (ISO 14721:2003).

A core requirement in this context is the development of a sound preservation plan ensuring that appropriate resources to preserve digital objects have been taken. This is supported e.g. by a well-defined planning process documenting respective requirements for a given preservation setting, as well as the evaluation of tools performing the actual preservation actions.[24]

Further, authenticity of digital objects has moved into the focus. Henry M. Gladney introduced the term trustworthy digital objects (TDOs).[10] Such TDOs contain as a record of their change history so future users can know with certainty that the contents of the object are authentic.

4. Legal challenges

Resulting legal challenges of the preservation strategies of extraction, standardization, conversion, encapsulation and emulation are quite important. Depending on the chosen preservation strategy, several different processing steps may be applied repeatedly over time interfering with knowledge rights [11, 28].

Changes to the artefact: The important content of the digital object with respect to preservation requirements is extracted and preserved separate from the original object (e.g. extracting all text information from a PDF file and storing it as ASCII or UNICODE text file). The object is modified with reduced information. Part of its content and characteristics are split into several different objects. The file may be converted to another file format, be it in the same format family (e.g. migrating a WORD 2003 document to Word 2007), or into a different format (e.g. converting a WORD 2003 document into RTF, PDF, Postscript, OpenOffice, TIFF or JPEG file) again modifying content, functionality, look-and-feel, sometimes at a degree that cannot be determined in advance resulting in a different than the original object. Files may be transformed in any way to conform to certain standards imposed by the digital preservation system (such as e.g. down-sampling all image files to a certain resolution, certain color depth, audio files to a certain bit sampling rate, etc.).

The preservation may consist of some necessary changes, sometimes also be subtle and hard to detect. Limitation of liabilities for damages incurred by these unnoticed changes are a crucial issue, as is a need and method to specify which characteristics of a digital object are crucial and may thus not be changed under all circumstances.

Recreation of the object environment: Digital files or specific objects require usually protected
software for presentation and use. Most objects require a specific infrastructure to be accessed, e.g. a website containing a flash animation may require a special version of a flash player, running within a specific web browser, running on a specific operating system on a given hardware platform. In order to be able to emulate a certain system, an emulator needs to be provided by the producer of the original software or hardware, which currently is not the case for most standard applications and systems (partially also due to the high complexity of such endeavors). Thus, it may be necessary to acquire rights and store and activate not only the object as such, but also the complete environment including all layers of software and hardware or hardware emulators that are required.

Protection methods: Technological measures for copyright protection and access control constitute a specific problem. Such impediments may need to be removed or bypassed for preservation activities.

Access restrictions and data protection: Time and extent of providing access requires balancing the needs of both the digital preservation institution, the content owner, the range of rights owner in the value chain, as well as the individual with respect to privacy issues. Collection of user information (e.g. a web archive allowing tracing all individual statements and changes made by a person across the world throughout his or her entire life) may require specific legal access limitations as the collected data as such constitutes a completely new set of information, potentially severely inflicting privacy regulations.

5. Deposit of electronic publications

The digital world requires a dramatic change of preservation strategies and thus also a change of the legal environment of legal deposit. “Simple” deposit of the artefact will be replaced by deposit or harvesting of electronic materials. The standard of ownership with an exhausted distribution right will be partly replaced by sophisticated access regimes, at least for the time of commercial exploitation taking into account the different distribution methods of publishers by renting the tangible product or providing on-line access. This necessity for change is known for a long time [22, 23]; however, change is quite slowly and only step by step.  

Guidelines for Legal Deposit Legislation were published in 2000 by UNESCO. Legal deposit legislation for digital publications was given further endorsement in a UNESCO resolution on the preservation of the digital heritage 2001 and in Recommendation 2006/585 of the European Commission on the digitisation and online accessibility of cultural material and digital preservation.

Countries with provisions on legal deposit of electronic publications have mostly extended the obligation to deposit to some or all such digital materials. Automatic harvesting is quite common as a practical tool to gather the increasing quantities of online material. Explicit provisions on ingest

---

7 See also the study on the German situation [11].
8 These Guidelines are not a UNESCO Recommendation but a research work. They were written by Jules Larivière, Director Law Library, University of Ottawa, Canada and constitute a revised, enlarged and updated edition of the 1981 publication by Dr. Jean Lunn. Website: http://www.ifla.org/VII/s1/gnl/legaldep1.htm.
10 A recent proposal for an amendment to the Austrian Media Act expands the legal deposit to periodicals and websites. Techniques as web harvesting should be used as much as possible. The proposal contains also provisions for balancing with copyright law: Access can be restricted for a year after deposit if the media access is subject to fees. Electronic materials can be used only on-site in the preservation institution. Further, a prohibition of electronic copying is foreseen.
to a digital preservation system, acquisition of meta-information, extraction of digital objects, conversion, standardization or encapsulation are still not existing in legal deposit laws.\textsuperscript{11} Preservation institutions have so far focused on the quality of deposited materials and are active in related projects for migration and emulation.

Further, voluntary deposit schemes have been implemented in many countries. A model for the drafting of local voluntary deposit arrangements is available that was also endorsed by the Conference of European National Libraries and the Federation of European Publishers.\textsuperscript{12}

As preservation institutions do not have the necessary rights so far for a long-term preservation (in some countries not even for collection of materials), close cooperation and arrangements between preservation institutions and producers and owners of online material is required due to the higher complexity of online materials. This fact may be also responsible for the mentioned step by step approach in most countries.

It has also to be noted that liability questions are getting important, in particular if preservation institutions are archiving important materials for firms that may be still required for business activities some day.

Contractual arrangements may provide a solution for the time being. However, clearing rights is difficult and resource-intensive. Existing models are the NESLi2 Licence for Journals \textsuperscript{[17]} or the OCLC/RLG Working Group on Preservation Metadata \textsuperscript{[19]}. Although these contractual arrangements seem to be successful it is evident that they have to be incorporated in legal deposit acts in the near future in order to guarantee the completeness of the collection of the national heritage.

International arrangements may be the best solution for the future given the global information infrastructure. The future may see some competition between public institutions like UNESCO or WIPO and private initiatives like Creative Commons\textsuperscript{13} for providing the necessary legal rights for preservation purposes. A Creative Commons licence for preservation seems to be a quite promising solution if an international treaty on preservation cannot be concluded in the near future.

6. Rights for migration and emulation of digital media

The Agreed Statement of the WIPO Copyright Treaty\textsuperscript{14} concerning Article 10 permits contracting parties to carry forward and appropriately extend limitations and exceptions into the digital environment. The limit will be always the so-called tree steps test. Such limitations or exceptions are allowed only for special cases. They should not conflict with a normal exploitation of the work and should not unreasonably prejudice the legitimate interests of the author (Article 10 (2) of the WIPO Copyright Treaty).

Legal deposit or permanent storage of electronic publications is without question a special case. This exception is well established in existing copyright laws of contracting parties of the Berne Convention. Normally, access to deposited material does not conflict with a normal exploitation of the work because access can be given only to a limited number of users at the same time on-site.

\textsuperscript{11} A good overview on legal deposit provisions in various countries can be found in [30].
\textsuperscript{12} http://www.nl.lib.ee/cenl/docs/05-11CENLFEPE_Draft_Satement050822_02.pdf .
\textsuperscript{13} http://creativecommons.org/.
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society\textsuperscript{15} (Copyright Directive) explicitly does not change legal deposit requirements (Article 9). Further, the Copyright Directive contains also a special exception for reproductions. Article 5(2)(c) of the Copyright Directive allows exceptions “in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage”.

Therefore, it is up to the national law to find appropriate solutions for preservation of digital materials. The obligation to legal deposit is easily covered; migration to new media can still be subsumed as an act of reproduction. However, “editing for preservation” does not comply with this provision. Such acts are the prerequisite of the author and are not covered by any of the exemptions of copyright.

The Copyright Directive protects technological measures and rights-management information as any circumvention of any effective technological measures is prohibited (Article 6 of the Copyright Directive). Preservation requires sometimes a circumvention of effective technological measures. The Copyright Directive does not contain an explicit exception but Member States should take appropriate measures to ensure that the exceptions or limitations of Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) are available to the beneficiaries. It remains unclear if a Member State can allow a preservation institution to circumvent effective technological measures.

According to Recommendation 2006/585 of the European Commission on the digitisation and online accessibility of cultural material and digital preservation, Member States should establish national strategies for the long-term preservation of and access to digital material with full respect of copyright law. Such a national strategy should contain the organizational approach, specific action plans, information exchange and legislative measures:

\begin{quote}
9. make provision in their legislation so as to allow multiple copying and migration of digital cultural material by public institutions for preservation purposes, in full respect of Community and international legislation on intellectual property rights;
10. when establishing policies and procedures for the deposit of material originally created in digital format take into account developments in other Member States in order to prevent a wide divergence in depositing arrangements;
11. make provision in their legislation for the preservation of web-content by mandated institutions using techniques for collecting material from the Internet such as web harvesting, in full respect of Community and international legislation on intellectual property rights;”
\end{quote}

Thus, the Recommendation clearly recognizes the required change in existing preservation legislation, however, does not give precise rules. It is up to the Member States to find appropriate solutions in accordance with intellectual property rights.

Long-term preservation requires besides extensive copying and migration in an archiving system also some “editing” of materials, in particular necessary modifications due to the preservation methods or changes in hardware and software. It may be noted that this situation is not that new. Also in former eras, materials had to be copied or edited for preservation purposes, migrated to new

standard media (e.g. then to printed books, now to digitalised books like the Google Books initiative) or adapted to new orthography or changing language use. However, then, copyright did not exist or terms of protection had expired for a long time. Digital media deteriorates so quickly that terms of protection are still running and copyright is still decisive.

Copyright law does not allow any changes of the work without the permission of the author [12, 14, 28, 33]. At the moment, only contractual arrangements between authors, publishers and preservation institutions can give them the rights for such “editing for preservation”. Such contractual relations are costly and difficult to establish even for preservations institutions but impossible for small and medium sized enterprises (SMEs) or private persons.

The so-called three steps test does not seem to prohibit national provisions for “editing for preservation” but requires appropriate balancing of interests. The existing practise of projects and contractual arrangements may result in balanced models that can be transposed into general rules, maybe at national, European or international level.

7. Reverse engineering

Authenticity of long-term preservation requires maintaining to the utmost possible degree the same environment of presentation, e.g. the “look and feel”, the functions of the various programmes and data formats etc. As mentioned above, storage and migration will be performed by a huge computer system containing the national heritage. Existing hardware and software will disappear and with them the hardware and the software package allowing the use in a technical way. Therefore, this environment may have to be emulated by reserve engineering of functionalities of hardware and software.

Decompilation and reverse engineering of such programmes may infringe the copyright of the rightholders. Article 6 of the Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs16 is quite restrictive. As the aim of emulation is not interoperability but substituting the program as such, reverse engineering is not covered by the Copyright Directive [33].

For standard software environments, it can be expected that emulations will be developed by software producers in agreement with the rightholders. For other hardware and software, preservation institutions have to conclude contractual arrangements allowing reengineering of existing hardware and software solutions for the purpose of access to the national heritage. In the medium term, preservation institutions should have statutory rights for reverse engineering of IT environments for this limited purpose.

8. Protection of data

The huge archiving repositories contain much personal data, and with existing search tools, will allow a much more sophisticated access to this information. The present trend of publishing private data on the Web 2.0 illustrates the problem of keeping short-term publications for a longer period. Present standards of data protection (e.g. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data17 (Data Protection Directive) are not very

---

helpful as those materials have been made available to the public by the data subject and are thus no longer subject to data protection laws [5].

So far, no special provisions can be found in national laws or case law concerning this special situation due to now existing powerful archiving and searching options. The international situation is very different as the example of publication of court decision shows. Some countries practise already anonymisation whereas others, e.g. the European Court of Justice, still publish personal data of parties of a court cases.

In the future, the application of general principles of data protection requires that limits for access or anonymisation are established that are appropriate to this new archiving environment. Some helpful insights may be available from anonymisation practises of courts (e.g. that of the Austrian courts18).

Thus, preservation institutions should develop their own practises for the time being in co-operation with data subjects. In the future, appropriate safeguards should be incorporated in national preservation laws.

9. Conclusions

Mere preservation of the artefact is no longer sufficient to ensure long-term accessibility of digital content. New conservation concepts called migration and emulation are thus needed to avoid the risk of losing electronic publications. Content and “look and feel” can be only preserved if artefacts are migrated to new IT environments or emulation of former IT environments is done. Thus, changes to the object or its environment as a result from preservation actions are unavoidable, requiring permission to inflict changes to an object in order to preserve it.

The WIPO Copyright Treaty leaves this important question to the national legislation. However, limitations and exceptions are subject to the so-called three steps test. So far, national laws are quite conservative and extend only the obligation to deposit to electronic off-line and on-line materials. Extensive conservation rights are still subject to contractual arrangements. Thus, an international solution to these challenges in the form of treaties or private licences is definitely desirable for the near future.

10. References


18 The Austrian courts can be considered as good practice. Cf. http://www.ris2.bka.gv.at; cf. [1] and [25].


Cited websites were last visited in August 2008.
INFORMATION GOVERNMENT
AND LEGAL INFORMATION

Athi Saarenpää

Abstract
In recent years we have talked a great deal about e-government. At its simplest, e-government means government that relies heavily on information technology, especially data processing. More sophisticated forms embrace e-transactions and the dissemination of information on networks. If we consider that government in the modern constitutional state is a set of information processes, all phases of which are legally significant, we would do well to change the terms we use. We have every reason to speak of information-driven government or even information government. In the midst of this change, a new, important consideration has emerged: how the public sector communicates what is right and what is law. Legal information, as part of our social capital, is readily visible on networks, but not necessarily readily comprehensible. Reading legal texts and court decisions requires sound legal literacy. This is something lay people generally do not have. And yet, more and more often they are just lay people who use electronic legal texts in net. Communication as to what is right fails. At least three remedies can be found for this new problem facing the modern network society. First, we should pay far more attention to like when conveyed in legal texts and signs. Second, we should create a totally new shared conception of the ways in which the public sector does tell about legislation, guidelines and legal practice and what liabilities there are involved. A third and more far-reaching solution is interactive legislation. Using IT we could create legal knowledge spaces in which legal texts are supplemented by additional legal source information. This would make the what and the why of law and justice visible at the same time. Understanding would be easier. Mere linear text, fraught as it is with semantic inaccuracies, is ill suited to serve as legal text in the network society.

1. The Network Society

When we talk about e-government, we should never overlook the fundamental question of the kind of society for which that government is being designed. In its day, the introduction of office automation in government was seen primarily as a technological advancement. Today, the transition to e-government involves a significantly different development. Society at large is also undergoing profound change. The issues we must address go well beyond technology.

Like many others, in recent years I have described the society we live in today as a network society. What we are building in Europe, and largely in the context of EU policies, is a new e-government for a new network society.2

---

1 Professor of Private Law, Institute for Law and Informatics, Faculty of Law, University of Lapland, Finland. email: asaarenp@ulapland.fi
2 See for example Saarenpää Towards legal information and legal knowledge some basic issues in Finnish perspective, pp. 509-525
To date ‘network society’ has been anything but a crystal clear concept, and I will provide a definition before going further. In my view, it is a society where we are dependent to a significant extent on the daily use of information networks and the services and information they make available. What has emerged is a new public, general information infrastructure. It is an unprecedented infrastructure, one that is absolutely crucial to society. And using the potential of this infrastructure to the full is a crucial aspect of e-government too. Government in the network society is government on networks.

What of the Information Society, which we still hear so much about? It is a regular feature in many national and international statements of policy. I personally regard the Information Society and the Network Society as two rather different societies. The merely static information society has become the dynamic, more and more interactive network society. The transition to e-government is an essential element in this change. Very many government services indeed are being put on networks and tailored for delivery in various interactive applications.

In recent years, e-government has – in technological terms – taken the steps familiar to us from the transition to e-commerce or, put more accurately, electronic markets. The public sector is well known for being slow. Just creating web pages for different government offices took time. Web pages are essential in the Network Society, but represent only a fraction of what e-government as a whole entails. Then again, to the citizens who use them, these web pages are a reflection of the government that created them and thus merit particular attention.

An essential, but often overlooked issue in e-government is what kind of national core (basic) registers and similar stores of data government should maintain and how these may be used. It is in such data stores that the fundamental social tension of e-government lies. Compiling and using registers is becoming technically easier by the day but little effort has been expended on discussing the legal framework for them. What we see here is by no means a technical, i.e., back office, activity.

Modern data protection legislation and the often very divergent laws on public access to be found in different countries cannot provide a clear framework for core registers in the modern constitutional state. Then again, data protection as such does go a long way to stopping us from slavishly following the technological imperative.

The essential link between e-government and the legal Network Society is graphically and impressively reflected in a Finnish court decision handed down in 2006. The issue was the right of a disabled person to receive screen magnifier and voice synthesizer programs from the municipality as social assistance in order to be able to use information networks. The Supreme Administrative

---

3 In Finland the term used in political programmes is ‘knowledge society’. However, this means the same as ‘information society’.

4 Guidelines have been issued in Finland aimed at harmonizing the design of government home page. As early as 2000, Juhta, - the advisory committee on information management in public administration, published the first guidelines on creating web pages.

5 In the capacity of expert I have written a report, which appeared in September 2008, on legislation governing core (basic) registers. One proposal is that a general information security act be enacted that would guide the information security of basic information stores.

6 For example, the Data Protection Authority in Sweden has, with good reason, taken a negative position on a proposed plan to create an extensive, national employment register essentially covering all the workers in the country that would make it possible to process data on the small group of people who do not belong to any of the unemployment funds. The procedure would push the limits of acceptable proportionality in interfering in a individuals’ privacy.
Court set out the grounds for its affirmative judgement (KHO:2006:18) in the following terms: “In light of the fact that public and private services are becoming increasingly and primarily network based, A’s request for assistive devices does not constitute support for a hobby but, rather, will enable him/her to function socially, to live independently and to cope in his/her daily routine.” Here, the Court was very much abreast of the times.

The notions of a network society and networking must be distinguished however. Networking among individuals, groups and communities is merely one facet of the overall transformation. The new infrastructure makes it possible to create new types of networks and to make existing ones more effective. But this is only one interesting facet of the Network Society.

Yet networking as a phenomenon merits our attention if our aim is to develop e-government. The digital environment that networks provide allows government officials and their data processing to network. This is a desirable aim in our quest efficiency in government, but it is legally a somewhat problematic ambition.7

Where government authorities are concerned, networking becomes particularly interesting phenomenon when we talk of transnational network communities, which have also been described as ”the new diasporas”. One of the many questions involved is which languages we should serve these communities in on the network. Another is what kind of legal information they should be provided with in the new infrastructure. A third consideration is what effects the legal information on the network might have for them. To date, we have given very little thought to these questions.

Networking also proves interesting as regards legal information and communication if we think of the freedom to produce information on networks. The media, subject as they are too many restrictions on free communication, are by no means the sole spotlight for current events - any more that is. In the age of WEB 2, home pages and blogs are important channels offering unfettered communication and opportunities to exert influence with content ranging scientific findings and personal views. For users of information, the problem is that is increasingly difficult to determine how or if the information one has found is connected with what is known as the prevailing conception. Reliable, pseudoscientific and narcissistic information seem to converge. As Dr. Hannu Lauerma has most aptly put it: “Self-styled expertise is not hard to create with the publicity offered by the Internet and uncritical weekly magazines.”8

2. Legal information

I should also describe briefly what I mean by the term “legal information”. I use the term broadly to refer to any information that has an impact on our conception of what is right or just.

Thus I am not referring solely to official information as such. For example, media coverage of legislation and trials, as well as the various new legal blogs on the Net, constitute bona fide legal information in the network society. It may be difficult to influence the content of these sources but in reality they are influential. They have an impact on citizens’ conception of what law is and what is right.


8 Lauerma Usko, toivo ja huijaus p.150
Likewise, the legal views and reservations put forward by e-government on its home pages or in other forums are information that cannot be overlooked in the Network Society. In the network environment we cannot be content to stare merely at the traditional, official (theoretical) sources of law.

It is particularly important to point out that the average citizen may have trouble distinguishing between information that the government places on networks by way of guidance and advice and information that has been made available because the governments want to provide information about different matters.

For example, one express obligation of data protection officials is to guide practices. For this reason, the information on their pages is by definition more significant than that provided by officials that are merely providing information about their particular activities.

For the average citizen, the latter kind of official information is often no more than self-help. This information forms a basis on which people develop their personal views of law. These may not be correct but the spirit of good governance says we should be able to trust in them. We should never forget the role of information in good governance. Good governance produces – it must produce – high-quality legal information.9

The core resource here is however the basic store of legal information – the sources of law, e.g., legislation, government bills, official guidelines, case law, and legal literature. This resource must be given special attention in the digital environment of the Network Society.

The Network Society forces us to supplement the old saying “law in books” with an equally important “law on the net”. In the worst case, law in books, law on the net and law in action may well take separate paths. Ideally, they will complement one another seamlessly. Given the extent to which open networks are used we may be looking at a serious problem where communication is concerned.

The next step may well be to ask what should law be in the relationship between the citizen and the state. We have become accustomed to speaking of prohibitions, orders and guidelines and the consequences of observing or violating them. While we cannot disregard these questions in the constitutional state, but we must give equal attention to defining what law is in terms of social communication and different information stores. The question, “What is law?” also goes to the very core of the constitutional state.

3. Law as social capital

In a democratic constitutional state, law belongs to us all. Law is not merely a matter of detrimental consequences for those that fail to observe it. Nor should we assess the quality of legislation and other legal information solely from the perspective of officials, civil servants and lawyers – the mentality that prevails in the traditional administrative state. Similarly, it is often assumed in practice that people need experts to help them with their legal affairs. This keeps the markets of legal life going.

9 In Finland, the Administrative Procedure Act uses the more precise legal term ‘good administration’..
If we want to find something essential and something urgently in need of change in the traditional thinking of the legal profession, it is doubtless the deep-seated notion that legislation is primarily intended as a message for lawyers who use it as a tool in their work. This is of course what laws are for but there is more to them, a lot more and important.

We can and should, as for example Virginia Wise and Frederick Schauer have so persuasively done, speak of legal knowledge as an important form of social capital. A country is built – so the old saying goes – on law. It belongs to us all. What we need is a clear conception of the significance of the core legal information resource, how it should be developed and what constraints apply to its use.\(^\text{10}\)

Yet this is not the case anywhere to speak of. This shared conception is lacking or, at least at this writing, very deficient both nationally and internationally.\(^\text{11}\) Legal cultures vary significantly from country to country and – although we often forget it - legal information and how it is produced is a core feature of a legal culture.\(^\text{12}\)

I believe one can say that despite the tightening grip of international publishers in recent years, the production of legal information and the market for it are still largely part of the national legal culture, which has often developed haphazardly. For example, the compilation of laws long used by the Finnish courts – Suomen Laki – is the outcome of the work of a committee and cooperation between the Ministry of Justice and a national lawyers association. The work, which is a collection of the key legislation used in legal life and citations of higher court decisions, has long been a prominent part of Finnish legal culture and as such a certain source of pride.\(^\text{13}\)

The legal information products that have been developed for lawyers are of course many and varied. In fact, their creation represents the essential open market for legal information market; otherwise we would not be living in a democracy. We need a sophisticated information environment which gives us an opportunity to develop and change our legal culture. Social capital requires appropriate care and maintenance.

Today the essential point of departure is however more and more the citizen’s right to legal information. The forum in which we as citizens encounter the law has changed a great ideal. The steadily increasing legal information we see on open networks presents us with a new situation when trying to read and understand the law. It is more and more frequently the case that the primary user of a legal text is in fact a layperson. Texts are read and people try to understand them without any particular legal skills. This is the crux of what I have called the change of forum – meeting point - in law.

\(^{10}\) Virginia J. Wise and Frederic Schauer illuminatingly juxtapose the work of legal publishers in their communication with lawyers and legal information as social capital. For more details, see Wise – Schauer Legal Information as Social Capital, Law Library Journal 2007 p. 267 ff.

\(^{11}\) The Recommendation of the Council of the OECD on Improving the Quality of Government Regulation, adopted in 1995, is an important international document but has not received the attention it deserves.

\(^{12}\) See Wahlgren, Peter The Quest for Law – Law Libraries and Legal Information management of The future p. 20 ff.

\(^{13}\) The first volume of Suomen Laki was published in 1955. Today the work comprises three volumes and is sold by a commercial publisher and available in electronic form. Recently, in 2007, the Ministry of Justice, primarily for financial reasons, produced a version of the work for use by the courts in collaboration with the state-owned publisher. And the ministry pays the costs of purchasing this work directly from the publisher.
We interact with our social capital mostly on a computer terminal on a what-you-see-is-what-you-get basis. In this context, even the question *how legislation appears on the screen* becomes an important consideration. This is not something those creating legal information have considered. To be sure, we have progressed to the point where the old Courier type is nearly extinct, but the legal text we read on our computer terminals is still linear.

Yet, written laws are only part – often a small part – of legal information. Our right to legal information is a far broader and more complex question. Communicating legal information to the citizen is an involved matter – and will certainly be no less so in the era of e-government. It is not enough that legislation and court decisions are made available as such on networks. In the discipline of Legal Informatics, making such information available has traditionally been considered a natural point of departure but not even this has been implemented everywhere. The crux of e-government is not only the application of the rules and regulations that affect us directly but also our right to know what rules government operates on and what our rights are in that context. If this point of departure is not taken seriously, the transition to *information government* will end up being sadly deficient where the rights of the average citizen are concerned.\(^\text{14}\)

We often overlook the fact that the path information must travel in the digital environment of the Network Society is a complicated one. There are many factors that determine the form in which we ultimately receive the legal information we need on a given occasion. Social capital is not created in a vacuum; it cannot mature or develop without quality requirements. Accordingly, I will go on to take a closer look at the role of legal information stores when communicating about law. *Law is communication*, as researchers in Legal Informatics are quite rightly fond of saying. Successful legal communication depends to a considerable extent on the stores of information available and their quality.\(^\text{15}\)

### 4. The Information superhighway and legal information

The issue at hand is a far more complex than reading traditional law. It is a question of the attitude towards the *basic store of legal information* (basic resources).\(^\text{16}\) We still lack an agreed conception of the importance of that information and the requirements it must fulfil in the Network Society and, by extension, in e-government. We are used to living in a world where government, lawyers and the discipline of law – at least traditionally – take legal material as given without subjecting it to any particular scrutiny.

Not surprisingly, this has been cited as one of the shortcomings of the *legal culture* in most countries today. It is a direct outcome of the traditional legal education in most countries. The production of information and legal and administrative work are seen as wholly distinct pursuits and, in the worst case, as the work of different professions.\(^\text{17}\) With this mindset one easily overlooks one of the

---

\(^{14}\) One hears the term *information government* – used in the title of the article – with increasing frequency. It represents an effort to distinguish the early stages of e-government from the new e-government that is based on the effective use of information stores in a digital environment. See Mayer-Schönberger - Lazer *From Electronic Government to Information Government* p. 1 ff.

\(^{15}\) See *Wahlgren*, *The Quest for Law – Law Libraries and Legal Information management of The future* p. 143 ff.

\(^{16}\) By *information store* I refer to a body of information that is societally significant and is used primarily on a digital network. The concept can be attributed to *Timo Kuronen*, a well-known Finnish social scientist and researcher in the Information Sciences. He introduced the concept in the Nordic debate in 1998 when he wrote a report on the importance of information processes for democracy in the Information Society.

\(^{17}\) In the Nordic countries, for example, the number of librarians who hold a degree in law is very small. This has to do with how important such a degree is considered, a lack of cooperation between the professions and, of course, salary.
central elements of our traditional professional skills – one of the basic methods - the requirement of justifiable doubt. This could also be called the requirement of a critical approach to one’s sources. The democratic constitutional state must be built using sound legal information. With few exceptions, professional producing and communicating that information require personnel with sufficient legal training.

The core of the basic store of legal information consists naturally of official material. Today we can find this material along the information superhighway, produced and maintained with various degrees of success. The observation that using the information along the highway is like collecting the litter of those who have gone before us is in fact an apt one in many respects. Publishing different kind of legal or semi-legal material on networks is technically straightforward but the end result can even be chaotic. Yet, an increasing number of people – and, sadly, quite a few practising lawyers too – search for legal information primarily using Google and other search engines in networks. Here we can and should invoke the notion of “ignorance is bliss” and remain mindful of the dangers of such bliss.

Offsetting the fragmentation of official information we find on networks are the government portals for official and legal information that now operate in many countries. These are, although we do not always realize it, a natural aspect of the development of e-government, although e-government is of course more than just be able to carry out their official business on networks. Interestingly, legal information – largely thanks to the work of the Council of Europe – has served as a catalyst element in this regard.

The EU offers a premier example of how difficult it can be to take information produced at different times and in different ways and shape it into a uniform whole. What initially might seem to be a simple process readily becomes a difficult and expensive undertaking. Summer 2007 saw the opening, after a long wait, or the consolidated digital legal reference of the European Union. It is now far easier to access up-to-date EU law but the resource is unofficial. The information in it has been productized - processed and repackaged for us. In the process it has lost, or so we would be accustomed to think, its original reliability. It is however time to change this tradition as well. The producer of official information should clearly take responsibility for all of its information stores and products.

In addition to the traditional portals for legal information, we find today an increasing number of more general portals for the public sector. The simple – and acceptable – idea behind these is to

---

18 I divide the basic method into three components: procedure-, knowledge- and skill-related. The requirement of justifiable doubt, one of the general features of science, is part of the skill-related component of the basic method. We should know how to doubt the correctness of information.

19 An illustrative example is a recent decision handed down by the Finnish Parliamentary Ombudsman in a situation where the directions provided by the Social Insurance Institution of Finland on how to sign documents being submitted electronically were based on the old law - a law which had been amended some four years earlier.

20 In the Finnish literature, I have frequently emphasized that every legal unit that puts its information maintenance solely and primarily in the hands of staff that lacks legal training is a risk where legal safety is concerned.

21 The description is drawn from the work Tiedon partaalla (On the threshold of knowledge: how to manage information chaos?) by Dr. Tuominen, who examines the benefits offered and threats posed by open information networks. Dr. Tuominen is a researcher in the information sciences who works in the Library of the Finnish Parliament as one of its leading information experts.

22 As long ago as the 1970s, the Council of Europe encouraged its member states to develop extensive legal databanks. In the Nordic context, the Finland’s Finlex (www.finlex.fi) and Sweden’s Lagrummet (www.lagrummet.se) are illustrative examples today of such extensive national portals for legal information, also known as vortals.

23 The collection can be found at eur-lex.europa.eu/en/legis/avis_consolidation.htm
counteract the fragmentation of information noted earlier. Portals guide users looking for public information who are less experienced in information retrieval. Then again, they are essential tools given that few countries had the foresight to coordinate management of the information they placed on network information. Open information networks surprised public, yes even public, information management.

Let us now go from portals to the sources of legal information. When we think of legal information as social capital – a common good – and endorse the idea of a person’s right to sound legal information, we would do well to examine the issues in terms of human rights. Administrative expediency and market forces as developers of information products are poor guides to look to for solutions to matters of this magnitude. Accordingly, we should take a closer look at the principles on which we should construct the import stores of legal information in the Network Society and the opportunities we provide for using these resources. We must seek principles that will make the legal superhighway from human and fundamental rights to individual legal provisions and the guidelines for their application as logical and dependable as possible.

5. Perspectives on stores of legal information

To my understanding, at least four principal issues can and must be distinguished in examining the basic store of legal information and its use from the point of view of citizens’ rights: a) the use of the information infrastructure, b) the principles governing the information store, c) the change in the doctrine of the sources of law, and d) the idea of new, interactive legislation.

These considerations – but perhaps some others as well – have a crucial impact on the development of information government and of the modern constitutional state. Legal information – increasing as it is - has really taken on a new importance in our society. As regards the quantity of regulation, sociologist Risto Heiskala has spoken out critically in the Finnish literature about an artificial society. In Heiskala’s view, society is artificial when detailed regulation replaces what would be ordinary behaviour. This observation is an important one where the development of the constitutional state is concerned. Excessive regulation naturally engenders hostility and ill feeling that can only erode people’s sense of what law is. Similarly, excessive regulation can lead to a situation where the average citizen increasingly needs legal assistance in his or her daily affairs. This cannot be considered natural in a democracy.

I will now briefly describe the principles on which we might best build the new legal information superhighway that I referred to earlier:

5.1. Where the information infrastructure is concerned, the critical issues are access to networks and the anonymity of the citizen when using public legal information. Information superhighway is a very special highway.

---

24 The content of the Finnish government portal (Suomi.fi) is described as follows: The Info Bank website contains essential information on how Finnish society works and what opportunities are available.
25 It is symptomatic that in Finland even the web addresses of the ministries do not have a uniform format. Some are Finnish and some are English abbreviations of the name of the ministry.
26 The Auditor General of the Finnish National Audit Office, LLD Tuomas Pöysti, has put it aptly: The right to understand law and justice is a basic civil right and the foundation of active citizenship.
27 Heiskala’s ideas are based to a large extent on those of Anthony Giddens too. See for example Heiskala Society as Semiosis. Neostructuralist Theory of Culture and Society, passim.
Given that we are dealing with the use of a new public social capital in a new public infrastructure, access to networks should naturally be easy. Otherwise we could not speak of a public infrastructure or of genuine e-government. We have to follow information all along its journey, and not dwell on the user friendliness of government pages and services.

Although access to networks has generally become easier in recent years, real access is still not a given everywhere nor is it particularly cheap either. One reason for this is that when elaborating the legal framework for electronic communication in Europe, discussion about competition and regulation of it largely ignored considerations of citizens’ rights. We have yet to undertake the much-needed analysis of the societal significance of the new information infrastructure.

And seeing that a remarkable fundamental right – the access right to information – is involved, the anonymity of the user must be ensured. It is here that a certain tension arises in information government: we should have a secure link to the basic store of information and, at the same time, be guaranteed anonymity when getting and using that information. The strong identification of an individual is an ill-suited approach here. Supervision of the kind of public information that individual citizens use is simply not an option in a democracy. The matter becomes even more acute when we consider the use of information by national minorities, immigrants and transnational communities. We should be able to dispel even the slightest doubt that anonymity might be compromised in such cases.

5.2 There has been very little discussion indeed on the general principles governing basic stores of information. Efforts to improve the quality of legislation have been confined primarily to simplifying it. This is a natural enough ambition in a democratic constitutional state, but it is not really enough. We must also seriously consider what needs to be regulated that we have not regulated as yet. To my understanding it is here that information stores become an important object of regulation. At the same time we see a difference between the administrative and the constitutional state. The development of society’s stores of information can no longer be a routine, administrative matter that requires no regulation or that can be regulated without express consideration of citizens’ rights.

Such regulation is far from being a simple undertaking, however. Upon closer scrutiny, we find that we would do well to distinguish at least the following seven fundamental features: availability, accuracy, accessibility, searchability, understandability, usability and reasonable cost. These prompt a wide range of serious questions. As all of these have bearing on the development of information government, I will take up each briefly.

The availability of official information is linked to its being public. Basic legal information in information resources must be available in a form as complete as possible. This is in fact one of the core questions of democracy. We cannot accept “secret”, hidden legislation. For example, the gap in

---

28 The question of price affects all electronic communication. Tellingly, the Finnish Parliamentary Ombudsman has had to point out to ministries and authorities a number of times that it is not allowed to organize telephone connection, including queuing, as the markets do. In most cases, queuing for a service when calling from a cell phone was very expensive.

29 Of course it is a different matter that the request concerns documents containing personal data. The cases then involve the processing of personal data and the possible restrictions on set out in the law.

30 See also Saarenpää Towards legal information and legal knowledge. Some Basic Issues in Finnish Perspective, Festskrift till Peter Seipel p. 517 pp.
our knowledge of court practice that follows from confidentiality of court records runs contrary to the principles of the constitutional state.

Accuracy is such an obvious principle in the case of information resources that it is not often mentioned separately. Yet there is ample reason to. Especially when the quality of the mechanisms for producing information leaves something to be desired and information has to be edited for network applications, the risk of error increases.

This problem has typically been addressed through various disclaimers. When the principal uses of legal information change from those of the original documents to ones required by a network, such disclaimers become rather suspect. They should not be used to mask quality problems in production.

What I mean by accessibility of official information in this connection, is that official material can be used in as up-to-date a form as possible and without restrictions that might be imposed by region, different ways of storing it or cost. Here the efficient use of the new information infrastructure has brought a significant and positive when it comes to citizens’ rights and legal culture. The balance of information between actors can be achieved more easily in the digital environment when accessing information stores on networks.

Searchability is the essential basis of all information organization. Its traditional form is seen, in libraries for example, where literature is indexed or classified using key numbers and words. The problems associated with searchability in the case of electronic information are far more complex. They range from the use of notation to document structures and from uniform use of legal terms to the interface between legal and ordinary language. All of these must be taken into consideration in drafting legislation and writing up court decisions. Similarly, in developing e-government, the point of departure should be to plan the information processes such that the documents relevant to the e-services that government provides and the legal framework of the processes can be found easily.

Understandability is a natural and basic requirement of all official information. In terms of internal and external readability, official legal source material must be understandable to as many people as possible, not merely legal professionals. This is however one of the everlasting basic problems in written communication.

Usability is a relatively new demand that has been placed on information resources by information work. The essential issue here is how information can be without problems transferred from the resource to the user’s own systems. Thanks to the lacking standards it has not been so easy.

The seventh essential requirement in assessing and developing information resources is that basic information should be available at a reasonable cost. The use of basic information resources should be free of charge or at least very inexpensive. If the flow of information to citizens is allowed to become dependent solely on the market and free pricing, we have overstepped the bounds of the democratic constitutional state.

It should be noted that, as Maximilian Herberger has pointed out, the term ‘access’ is sometimes in a broader sense to encompass availability. See Herberger Access to Law, JurPC Web-Dok. 106/2007, Abs. 1-78

Directive 2003/98 on the re-use of public sector information deals with this issue in an important way, although the instrument is often overlooked. Article 6 states: “Where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together
These principles are more than just theoretical approaches; they all have practical implications. Indeed, recent years have seen a very visible discussion in the United States concerning the impact on the legal culture and how lawyers work of the classificatory system used by long-standing market leader Westlaw.\textsuperscript{33} Even the way an individual court writes its judgments is an important facet of legal communication. And that is very much what law deeply is — communication. And this aspect only becomes more important as e-government becomes more common.

5.3 Everything I have mentioned thus far pertains primarily to official information. It is undoubtedly the type of information that interests us most when we consider the new information government. But we cannot overlook how other legal source materials are changing. The legal literature in particular plays a key role in shaping the basic store of legal information. The changes in the new literature would merit a study of their own if we consider the work of lawyers. Clearly, there is no opportunity to undertake such a study here; what I will do is to reflect on a number of potential changes in the doctrine of the sources of law.

The doctrine of legal sources, that is, the sources that we should and may use, has varied a great deal from country to country. For instance, the status of travaux préparatoires — e.g. government bills - has been different in different countries although they belong to the same group of legal cultures. And one interesting traditional research focus in comparative law has been how the doctrine of legal sources differs from one legal system to another.\textsuperscript{34}

Given that our conception of law and justice is based on various narratives of law in addition to legislation, we cannot avoid a certain harmonization of the European doctrine of the sources of law. Contributing to the process are the recitals in directives, although the standard we see in recitals still varies quite a bit.\textsuperscript{35}

Every bit as important is that we take note of the increasing importance of expert organizations in legal life. They — for example Epic and Privacy International — influence authorities and influence ordinary citizens.\textsuperscript{36} The expression “watchdog” is most appropriate. The information they produce, all available on the networks, is in fact part of the legal material that is essential today. Among other things, it offers the user an opportunity to examine official material in the light of critical perceptions of the same matters. However, one must be able to distinguish expert organizations from others, for example, different kind civic or semi expert organizations. This is no easy task for laypeople or for lawyers for that matter.

One prominent feature of e-government is the increase in legal information being provided on government web pages. This highlights in a novel way the basic question of the tripartite division of powers. Legislative, judicial and executive powers are different, very different things indeed. This

\begin{itemize}
\item with a reasonable return on investment. Charges should be cost-oriented over the appropriate accounting period and calculated in line with the accounting principles applicable to the public sector bodies involved."
\item \textsuperscript{34} It is essential that we remain aware that information seeking is becoming increasingly international. In our everyday work in the profession there is a heightened need for legal information that spans the borders of different countries and legal cultures. Here especially lawyers are becoming increasingly international.
\item \textsuperscript{35} An instructive example of a rather extensive, good recitals section is that found in the European Personal Data Directive.
\item \textsuperscript{36} See Electronic Privacy Information Center pages in www.epic.or and Privacy International pages in www.privacyinternational.org
\end{itemize}
will soon become one of the core problems in e-government when we move from original material to various government guidelines. The significance of this phenomenon is increasing as the network visibility of the guidelines improves.

An important but often overlooked element in this development is the possibility that official communication will stray from the requirement that it be neutral. In a constitutional state, official communication should be factual and neutral. Bringing in factors that increases the effectiveness of the message easily brings one into the realm of marketing, where communication is anything but neutral. The views of communication experts on the success of communication are not necessarily compatible with the legal and administrative content of the messages.37

5.4. The most challenging task we face, however, is to reshape our conception of legislation. A traditional law is a one-sided message telling us what is right and what is wrong. It has been and is – with the exception of traffic signs – traditional linear text. And it is text which, in keeping with good drafting, may not have too much or too little of anything. This principle is not implemented successfully. And where it is, the resulting law might well be too abstract for the average citizen.

Producing better legislation is a pan-European ambition today. For example, efforts are being made in the EU to both clarify the drafting processes and to simplify legislation.38 As such it is desirable to try to make better laws as text, but it would be more important to develop a more multifaceted legislation that would provide background to the text of the law in an authoritative manner. In a word, we should stop and think whether traditional linear text is good enough in the Network Society and its information government. Is it not time we entered the era of interactive legislation?

What I have in mind here is replacing linear text with an interactive structured body of texts and images that shows the structural depth of the legal provisions. When searching for legal information on a network, citizens would be able to see the legal rules on the legal information superhighway. They could then easily distinguish genuine rules from descriptions which government official disseminate for a variety of purposes as part of their effort to implement in formation government.

Information technology and network-based communication provide every opportunity for implementing this. All that we need is a new way of looking at things. In legal communication, it is very often every bit as important to know why as to know what! Traditional legal text does not generally answer this question. Interactive legislation would guide the reader, showing him or her the depth of legal sources involved. What and why would be equally visible in the legal knowledge space.

6. What to do?

There is of course no single approach offering a solution to the problem of improving legal information and communication in information government. The role of information stores in the Network Society and the constitutional state is so complex that even a tentatively identifying the key prob-

37 There are many examples of this in Finland. When, for example, the Ministry of Justice recently prominently marketed on its home pages that citizens could call legal aid offices and present their case to the secretary, the central aim of legal aid was forgotten: the citizen’s right to receive expert legal assistance from a lawyer.

38 See, e.g., COM(2002) 275 final; the Better Lawmaking and Better Regulation pages at ec.europa.eu/governance/better_regulation/index_en.htm. In Finland, special attention has been directed to anticipating the impacts of laws. See the guideline on this : Impact assessment in legislative drafting, Guidelines, in address www.om.fi/1210773148629
lems – however tentatively – is fraught with difficulties. I believe we have seen this in what was said. But a number of very important strategies can be found.

Just developing the principles of the basic information stores on the European level would be a commendable aim. We are dealing with a public commodity whose use the government should guide and supervise. The principles developed will have repercussions for the markets legal literature and information services as well.

Another way to remove obstacles to communication is collaboration between legal and other professions – essential to developing information government – and the associated legal design of information systems.

Nor should we forget the need to increase legal education at the lower levels of the educational system. The notion that for the most part legal education begins only at university level is utterly obsolete and incompatible with the principles of the constitutional state. We need broader-based legal education in the network society.

The most important thing to remember is that law should be simple in the democratic constitutional state. For this reason we need a new doctrine of legislation and a new conception of what rules look like – on the Net or off.

39 An insightful example of how to approach an important problem, but one drawing on the traditional concept of a statute, can be found in the report titled “Legal Informatics and Management of Legislative Documents”, prepared at The Global Centre for ICT in Parliament under the direction of Giovanni Sartor. See www.ictparliament.org/resources/WP002_legislativeinformatics.pdf

40 In India, for example, the United Nations Development Program (UNDP) is currently trying to create systems by which rules can be communicated in a simple manner. This is somewhat different from simplifying legislation, however. See, e.g., www.undp.org.in/index.php?option=com_content&task=view&id=321&Itemid=232
7. References


HERBERGER, MAXIMILIAN Access to Law, JurPC Web-Dok. 106/2007, Abs. 1 - 78


LAUERMA, HANNU Usko, toivo ja huijaus ( Confidence, Hope and Fake), Duodecim (2006)

MAYER-SCHÖNBERGER, VIKTOR - LAZER, DAVID From Electronic Government to Information government, MIT Press 2007


SAARENPÄÄ AHTI Towards legal information and legal knowledge some basic issues in Finnish perspective, pp. 509-525 in Magnusson-Sjöberg – Wahlgren (ed) Festschrift till Peter Seipel, Norstedts Juridik 2006

SAARENPÄÄ, AHTI Reading and Comparing Legal Sources, Subtech 2008 papers


SAARENPÄÄ AHTI Oikeudellinen tieto verkkoyhteiskunnassa ( Legal Information in Network Society) pp. 117-140 in Tuominen, Kimmo Tiedon partealla; kuinka hallita informaatiotulvaa (On the threshold of knowledge: how to manage information chaos), BTJ Kirjastopalvelu 2006


Extended abstract

In 2003 in the case of Lindqvist (C-101/01), the European Court of Justice held that the act of identifying a natural person on an internet site by name or other personal identifiers constitutes "processing" of personal data within the meaning of Article 3(1) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive). The Court also found that such processing is not covered by the exception in Article 3(2) of the Directive which exempts processing "by a natural person in the course of a purely personal or household activity". The Court concluded that that exception related only to activities which are carried out in the course of private or family life of individuals and that this is clearly not the case where personal data is made accessible on the internet to an indefinite number of people. This suggests that personal information may only be disclosed on a publicly accessible website where at least one of the conditions set out in Articles 7 and 8 of the Directive is met.

Since the Lindqvist decision, the internet has undergone a seismic shift, away from being a purely consumptive medium to becoming a platform defined and developed through user-generated content (Web 2.0). Social networking sites, wikis and blogs have played a particularly important role in this transformation. They have altered modes of communication particularly among the younger generation and changed the way in which information is presented to and accessed and assessed by members of the information society.

It could be argued that the online communities that have resulted from these innovations depend to a large extent on the exchange of information, including sensitive information, by their members about each other. Social networking sites, in particular, have changed the act of exchanging gossip, whether benevolent or malicious, from a one-to-one to a one-to-many activity: information that individuals disclose about other people is no longer available only to a selected few, but to a wider audience. While in some cases disclosure to the wider public may be intended, in other cases, speakers may be unaware of just how widely the disclosed information is distributed by the online platforms they inhabit. The may also not appreciate the unrelated purposes for which that information may be used.

Although libelous statements published in this way will be subject to the available statutory and common law sanctions for defamation, information with a basis in fact or truth is often considered non-defamatory and thereby exempt from such protection. And yet, individuals often have a vested interest in not having information about them brought to the attention of a wider audience even if it

1 University of Central Lancashire, e-mail: jrauhofer@uclan.ac.uk.
is true because it may affect a person’s reputation or cause them to suffer material disadvantage. Medical histories and criminal convictions as well as pictures showing people in inappropriate situations could all be seen as falling within this category of data. Apart from such disclosure having the potential to cause embarrassment, emotional damage and friction with friends and family, the use of such information by schools, universities and employers for the purpose of vetting and monitoring existing and potential students and employees has led to fears that a few, well publicised “youthful indiscretions” may affect the career prospects of the current FaceBook generation for decades to come.

However, were the Lindqvist decision (mediated only by the provisions of Articles 7 and 8 of the Directive) to be interpreted as an undifferentiated ban on posting information about other people, this would raise another question: can the disclosure of such information be defined as being carried out for journalistic purposes or for the purpose of artistic or literary expression and is it therefore protected by the right to freedom of expression referred to in Article 9 of the Directive? Or can the data protection principles set out in Article 6 of the Directive be restricted on the basis of its Article 13(1)(g) in order to protect the rights and freedoms (including freedom of expression) of others? Is there a case to be made that through the imposition of restrictions on such online disclosure, now common modes of human interaction would be stifled with not yet foreseeable consequences for individuals and society as a whole? Or, more importantly maybe, would such restrictions open the floodgates for more intense intrusions on the right to freedom of speech leading to a situation where well-known individuals like celebrities and politicians could use the law not only carefully to manage their reputation and public persona, but also to exploit that persona for commercial gain?

Despite the clear guidance given in the Lindqvist decision, very few cases for violation of the EU data protection regime have been brought by those whose data is appropriated in this way against those who disclose that data on their websites, blogs and FaceBook profiles. It may be that this is due to the uncertainty surrounding the legality, or lack of it, of such behaviour. This must come as a welcome surprise to data protection commissioners, who would no doubt be unable to cope with an influx of complaints in this area given their limited funding and enforcement powers in most member states. At the same time, any duty “more honoured in the breach than the observance” must give rise to the question whether changes are required to a regulatory system that seems to outlaw an activity so many engage in without any apparent awareness of its potential unlawfulness.

On the other hand, if the privacy right sought to be protected by the Directive is engaged in cases of online disclosure of personal information and if the conclusion could be reached that the individuals’ right to the protection of their information is not outweighed by a corresponding right to disclose it, does this mean that other ways of protecting that right ought to be put in place if the current regime is found to be ineffective? Approaches mooted in the relevant literature include code-based solutions such as a requirement for stricter privacy defaults, custom-based solutions such as the introduction of specific acceptable use policies and regulatory solution including the imposition of intermediary liability on the operators of the relevant platforms who benefit commercially from the disclosure of the data.

This paper will look at the regulatory and self-regulatory regime that governs speech on the internet. It will consider the harm, both material and dignitary, that the uncontrolled disclosure of personal information can cause to those who are subject to it. It will examine the role that the disclosure or exchange of personal information about third parties has in bringing together members of society and facilitating social interaction. It will examine whether technology-mediated speech, particularly where the speaker hides his or her true identity behind an online pseudonym, is likely to exacerbate
the harmful effects of gossip and malicious rumors and whether the remoteness and, where applicable, the anonymity of such technology-mediated speech removes or lowers inhibitions speakers would normally have if they made the same statements face-to-face and with their identity revealed.

The paper will question whether an outright ban on such disclosure will jeopardise the fundamental right to free speech or if there is a case to made for the claim that “not all gossip is created equal”, that the legal response must have as its target the nature of the information and the circumstances in which it is disclosed rather than the mere fact of its disclosure.
THE GLOBAL INFORMATION ASSEMBLING: VIEWING THE DATA RETENTION JUST AS A CHILD PLAY

Radim Polčák

Abstract
There is now a significant group of information society intermediaries that hold the mass of information that is desirable to any intelligence service in the world (regardless of whether we speak about the service of a state or a corporate multinational business). The states started to recognize and pursue this fact namely by imposing the data retention duties to some of the information society intermediaries and also by legislating the access rights in favour of some of the governmental agencies. However, these efforts are highly problematic and disputable namely in the terms of proportionality and efficiency. Out of many problematic elements, we decided to discuss within this paper the jurisdictional limits to the data retention and access rights, the question of ultimate surrender of rights in exchange for a good service and natural technical restrictions to factual enforcement of legal regulations of data assembling.

1 Introductory note on information assembling
Various information society intermediaries, from business units to state agencies, make in fact the on-line life to happen. Their information infrastructure (both logical and physical) is used as the true ground for building the information society. Moreover, as the on-line world is not primarily based on territorial or in general physical grounds, the information society intermediaries represent in fact the most legally recognizable link between the on-line and the off-line world.

The crucial role of information society intermediaries can be seen also in the way in which the states enforce their laws in the on-line environment. Whenever there is issued an injunction that regulates some on-line activities, its enforcement cannot take place directly, i.e. just as a simple consequence the activity of some state enforcement agency like the police, executors etc. In fact, the direct enforcement would be possible only in the (extremely rare) case when the state would physically provide the respective service of the information society. In all the other cases, there is always a need to enforce the respective injunction through relatively independent providers of information society services.

The specific position of providers of information society services has been up to now widely discussed namely with the respect to their role and consequent responsibilities in mediating of problematic on-line communication. In particular, we mostly focus on the role of

1 JUDr. Radim Polčák, Ph.D., Workgroup for Law and ICT, Faculty of Law, Masaryk University, Brno, Czech Republic. The paper was written under the research project No. MSM0021622405.
telecommunication companies in transmitting of illegal data (and possibilities of takedown), the role of exchange servers in mediating of unlicensed file sharing etc\textsuperscript{4}.

There is, however, also one fast developing aspect of activities of information service intermediaries that started to drag massive attention not just of lawyers but also intelligence agencies - let us name it the global information assembling\textsuperscript{5}.

The state-run or even supranational intelligence bodies focus namely on gathering and processing information that serve primarily in order to facilitate the governmental or intergovernmental decision making or policy making. These information, however, do not have to be primarily focused on the security, political or economical interests of the stakeholders. Of course, direct information about development of nuclear weapons, about organization of a terrorist network or about subversive activities within governmental agencies, are of crucial relevance. This kind of information is, however, mostly impossible to be acquired directly. Therefore, the intelligence services and similar governmental bodies work namely with loads of indirect associated information.

When there were revealed information about the fact that one of the Czech folk-signers, formerly deemed as anticommunist, collaborated with the communist intelligence agency, some fans defended his dignity by the argument that the intelligence that he submitted to the communist agents had nothing to do with the mere anticommunist activities (in other words that submitting these information did not harm the underground at all). In fact, he just gave the agents information about everyday personal life of the anticommunist underground which he was a part of. Although this seems as prima facie an innocent activity (and so might it had seemed to the signer-agent), the information about the personal profile of those who are in focus, is just the right thing for the intelligence service to work with. Using the acquired information from multiple sources and proper data mining tools, the skilled information specialist is then able to retrieve a complex and precise descriptive data that can be further used for broad variety of purposes.

Today, the internet is already full of the aforementioned indirect information and the amount still grows. Moreover, almost all of the information is created, stored and communicated via the services of the intermediaries. Blogs, webmails, IP telephony, social networking and other services represent hardly believable source of data that can be precisely and successfully mined for very particular purposes including the state intelligence. Up to that, the personal life of the information society stakeholders (that is so much interesting for the intelligence agencies) does not take place on the official (governmental, university, defence) service platforms, but on FaceBook, GMail, eBay, ICQ and others.

2. Jurisdictional limits

The jurisdictional questions or in general the applicability of law on the information society is one of the first areas that have attracted the attention of academics together with practicing lawyers\textsuperscript{6}.


\textsuperscript{5} One of the very few publications that discuss this problem in particular is EVANS, E. From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications, in Michigan Telecommunications and Technology Law Review, vol. 10 (2004), p. 445.
The question over the traditional criteria for delimiting the applicability of national laws initiated even core debates over the general approach to the internet legal issues and the needs for the development of specific methodology. The recent achievements in the development of methods of assessing the jurisdiction and law applicable on internet issues are namely to be seen on the fields of private law. However, even the criteria that are being repeatedly discussed for centuries in doctrinal publications and judgments like *lex loci delicti*, *lex loci solutionis* etc., still do not have any commonly accepted interpretations when it comes to the internet.

Unlike in the case of international private law, most of the disciplines belonging to the public law do not even have such a long tradition in assessing of the collision criteria in general. Especially in the case of laws and regulations that protect the vital interests of the states, namely the penal law, law of armed forces or the law of intelligence services, the applicability of legal rules always strictly depended on the territorial criteria. In other words, these laws were applied always strictly on the territories of the respective states.

The application of the physical territorial criteria makes sense only in the case when the physical location of the regulated subjects or objects matters. On the contrary, when the physical criteria are irrelevant in relation to the regulated activities their application might lead to factual limits and inefficiencies of legal regulation. However, when it comes to investigations, inquiries or any other activities of law enforcement agencies, they can be taken only against a subject or technological infrastructure that is physically placed on the territory of the respective state.

As to the global information assemblers, it obviously depends a lot on where are they settled and where is physically placed their infrastructure. At this point, we might object by saying that when, for example, personal data of EU citizens are being assembled, the EU data protection laws should apply. Similarly, an IP telephony operator should be bound by the data retention laws applicable in the EU when the service is provided to the European users. Theoretically, the laws might apply, but there is no enforcement possible, as it would have to take place outside the territory of the EU when, for example, the respective ISPs are settled in China.

Consequently, the local law enforcement agencies on the fields of data protection, crime investigation or security are practically helpless when the users choose a service beyond their reach. There are, of course, various international agreements on the assistance and cooperation in various

---

6 As to the general grounds of the problem, see for example SAMUELSON, P. New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy, in California Law Review, vol. 87 (1999), p. 751
8 There were just published two specialized monographs mapping the whole field – see KOHL, U. Jurisdiction and the Internet, Cambridge University Press, Cambridge, 2007 and SVANTESSON, D., Private International Law and the Internet, Kluwer Law International, 2007. In both of them, there is a comprehensive set of methodological approaches and arguments, but almost no definite answers.
9 The strict dependence on the territorial criteria that are favourable to the country on whose territory is the defendant physically present still prevail despite of the fact that there were already issued some rulings of international courts on delimiting the jurisdictions like in the case of Permanent Court of International Justice in the Lotus case – see KOHL, U. Eggs, Jurisdiction and the Internet, in International and Comparative Law Quarterly, vol. 51 (2002), p. 555.
matters. However, these agreements always contain a lot of safeguards preventing from infringement of territorial competences of the local law enforcement agencies and moreover, there is up until now no such agreement that would cover the case of global information assembling.

When the data are communicated by, for example, Austrian citizens using a freemail or blogger service settled in Singapore, there is no supervision of the Austrian data protection officers and there is also no possibility for the Austrian Police or the intelligence agencies to access and use them for the purposes of saving the vital interests of Austria. However, the factual impossibility to control the way of handling with information that originate at the national subjects in the cases when the ISP is settled outside the territory of the respective state represents just a half of the problem. The second half is in the fact that the respective data are, on the contrary, accessible to the state agencies and other subjects on the “territory of destination,” i.e. that the foreign data might be under the survey or use by the state authorities or business units of the state under whose jurisdiction they are being stored. It implies that the local state agencies and business units might easily access the data and use them in accordance with the local laws. It is to be noted here that such competences are to be seen as clearly legitimate. It is then obvious that under the circumstances that, to certain extent, any state is an enemy of any other, it is always in general very unfavourable situation to those states, whose users are using the foreign information services.

This problem is emerging especially in the cases when the user data are being processed in countries that allow the state agencies or other subjects to easily access and use them. On the contrary, most of the European countries have relatively strict rules that delimit the powers of police forces, armed forces or intelligence agencies and that lay down strict limits also for other subjects that might get in touch with such data. However, none of these limits apply when there is the consent of the data subject.

3. Surrender of rights and technical limits

The ISPs are under normal circumstances strictly limited in their possibilities of processing and use of the data that are provided by the users. Consequently, the ISPs might not freely process the user data or to assemble them into personalized profiles. However, that applies only in the case when the users do not give an explicit permission to an ISP to do so. Below, please note some of the examples of contractual clauses relating to the processing of data communicated by users of information services:

ICQ End User License Agreement:
“ICQ has the right, but not the obligation, to monitor such content available on or through the ICQ Services, to determine compliance with the ICQ Terms of Service and any other operating rules that may be established by ICQ from time to time.”

FaceBook Terms of Use:
“When you post User Content to the Site, you authorize and direct us to make such copies thereof as we deem necessary in order to facilitate the posting and storage of the User Content on the Site. By posting User Content to any part of the Site, you automatically grant, and you represent and

11 In this case, the principle volenti non fit iniuria applies almost in the full extent.
12 The concept of voluntary permission, transfer or surrender of privacy rights or rights to the protection of personal data is grounded on the so-called property concept of privacy. Under this concept, privacy is a value of private interest that might be fully controlled by the subject (including surrender) – see for example PRINS, C., Property and Privacy: European Perspectives and the Commodification of Our Identity, in Information Law Series, vol. 16 (2006), p. 228.
warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.”

Mail.com Privacy Policy:
[We won’t without your explicit permission] open or read messages in your account: unless, we believe, in good faith, that such release is necessary to:

a. Comply with the law. We reserve the right to disclose your personally identifiable information as required by law and when we believe that disclosure is necessary to protect our rights and/or comply with a judicial proceeding, court order, or legal process.

b. Enforce or apply the terms of our user agreement, or

c. Protect the rights, property, or safety of mail.com, our users, or the public.

Apple Safari Licence Agreement:
You agree that Apple and its subsidiaries may collect and use technical and related information, including but not limited to technical information about your computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any) related to the Apple Software, and to verify compliance with the terms of this License. Apple may use this information, as long as it is in a form that does not personally identify you, to improve our products or to provide services or technologies to you.

As it can be seen, users of various services of information society give their explicit consent to the respective ISPs to almost freely process the communicated data. Regardless of the local laws or regulations, such consent often acts as blanket permission for the ISP not just to use the data in the regular course of business (including assembling them into personal profiles), but also for almost any other purposes.13

It is then disputable whether the users might legally surrender their rights without knowing what such surrender might in fact bring to them14. It is also highly disputable whether the surrender is valid in terms of its general legal admissibility when it is designed as total or extremely broad15.

In any case, the possibility to let the individuals to surrender their rights represents at the moment very strong and efficient instrument. Compared to the processing and assembling rights laid down

---

13 We should note that the permissive formulations are often very broad and consequently they allow almost unlimited extensive interpretations.

14 Especially in electronic contracting, the consent is in many cases given by users that are not properly uninformed. Thus, such consent might be automatic and negligent – see GAUTRAIS, V. The Colour of E-consent, in University of Ottawa Law & Technology Journal, vol. 1 (2003-2004), p. 189.

15 In this respect, we might formulate an illustrative question whether it does not go beyond the limits of private law (extremely broad, indeed) when someone permits some entrepreneur to freely enter his private sphere and use the acquired data in any way in the course of business activities. See for example a study on the Canadian example in AUSTIN, L. M., Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA, in University of Toronto Legal Research Paper, No. 11-05 (2005).
by the data retention legislation, the surrender of rights, when used, gives the entitled subjects the following benefits:

- It is possible to store the communicated content (data retention: it is possible to store only the identification data)
- It is possible to process the data almost freely (data retention: it is possible to process the data only in the ways expressly defined by the law)
- There is no jurisdictional limit when it comes to the access. In other words, the controller might sell the data to any institution anywhere in the world (data retention: only the local empowered authorities have the right to access the data)
- There is no limit regarding the assembling of data (data retention: the retained data might not be combined with other types of personal data)

Besides the legal reasons, i.e. the jurisdictional limits and use of waivers of rights, there is another important incentive for the global information assemblers to engage in massive collecting and processing of the content communicated by users. Let us call it the survey-proof nature of the proprietary information infrastructure.

Whenever some subjects control multiple types of information that might be of a personal nature, there applies the general legal limit prohibiting them from assembling these information into complex personalized profiles (this limit does not apply in the case of surrender – see above). However, such an assembly might take in practice just a couple of seconds or at the maximum a pair of minutes in individual cases. Besides that, such an activity can be performed totally unseen and it does not leave behind any evidence that might be later used to prove that prohibited assembling took place.

The info-lord has then factual possibility to unseen operate with user-provided data without any danger that these operations will be revealed, investigated or prosecuted by the supervisory state institutions. Frankly said, whenever the data protection officers or similar bodies enter the information space that is under technical control of one subject, they can see only what they are technically allowed to. The only possibility to reveal anything what is covered by the technology veil might be then revealed practically only in the case of appearance of a whistleblower.

4. Concluding remarks

This short paper intended neither to describe the global information assembling nor to discuss its bright or dark sides. We even did not have any ambitions to lay down some recommendations on how to handle it. The only aim of this paper was to point out that the global information assembling is an existing and emerging phenomenon and to highlight its legal implications and regulatory paradoxes.

---


17 We decided to focus here namely on the position of a state. The role of individuals, limits of privacy and development of subsequent concepts represent yet another interesting area of research – see for example BOYLE, J., Foucault in
The first paradox we find in the fact that the combination of jurisdictional questions, technology features and legal possibilities of waiving the rights to privacy and data protection gives the information assemblers a possibility to infringe the personal sphere of individuals to an extent that would not be thinkable in the case if it should happen upon the law. In other words, the named features give the ISPs competences that go far beyond the imagination of police, armed forces or intelligence agencies.

The second regulatory paradox, consequent to the first one, is to be found in the changing position of a state and its agencies in the information society. While traditionally, the state represented the sovereign power that had to be limited, we now start to have the state in a position of a weaker partner or even a petitioner that asks the factual powers for a help. It was, of course, not always the situation that all the states would be ultimate rulers, but at least they ruled over their own people. With the development of global information society services and information assembl ing, we might find out that even this “rule over own people” is in decline. Moreover, we might even predict that the notion of “own people” might change in the way that we will not even speak about “own people” (or nationals under the rule of law) of the Czech Republic, but of Google or FaceBook.

In general, we did not want to draw here some shocking theories of conspiracy or postmodern visions of states and their laws being in terrible decline. We rather wanted to highlight some aspects of the development of the information society that are continuously showing that standard grounds of legitimacy of state powers and laws are changing together with the development of information society. This change is not theoretic or conceptual, but empirically provable. Any negligence of this development by the legal doctrine might therefore be highly dangerous and leave the law and its institutions in the long run in a position of passive spectators rather than actors.

5. References


Legislation that would give some subject a right to freely process, aggregate and use the content communicated by users of some service would be inevitably found as unproportional and unconstitutional in most of the civilized countries. The constitutional proportionality applied on cyberspace is extensively discussed in LESSIG, L. Reading the Constitution in Cyberspace, in Emory Law Journal, vol. 45 (1996), p. 869.


THE PROCESSING OF TRAFFIC DATA IN THE PRIVACY DEBATE

Mikolaj Sowinski

Abstract

The status of traffic data under European privacy law is a significant issue with important ramifications for IT security. BSA believes that individuals who can be directly identified by their Internet providers, telecom operators or by online services providers based on traffic data must continue to benefit from the full protection of European privacy laws. Without a valid court order or a decision by the competent data protection authorities, ISPs or other online services providers should not be allowed to disclose such information or reveal the identity of their individual users.

But without the legal authority to analyze traffic data, government and private entities that provide online services cannot technically ensure the security of their services, including the privacy of persons using them. Critical security solutions deployed by banks, hospitals, retailers, IT companies and government agencies all process traffic data to help protect the personal data of European citizens.

In order to ensure effective security online, it must be clarified that the processing of traffic data is consistent with Community data protection law when such data cannot directly lead to the identification of a specific individual. This will prevent the Internet from becoming a space where hackers and other anonymous individuals can steal personal data, jeopardising the user trust that is critical for the success of the European Information Society.

1 Mikolaj Sowinski, Partner, SKS legal, Warsaw, e-mail: Mikolaj.Sowinski@skslegal.pl.
DATA RETENTION: HOW THE HUNT FOR "COPYRIGHT INFRINGERS" IS RAping FREEDOM

Ricardo Cristof Remmert-Fontes

Abstract

In politics and law enforcement the idea is wide-spread, that law enforcement in a technological society is just a question of technology, of what can be done by technical means.

Among others, the instrument of data retention of telecommunications has been introduced as an instrument to investigate on terrorism and child pornography. It was also said, that this instrument will prevent from those crimes.

But is this instrument effective? Or is it possibly affecting basic principles of a democratic society?

And does data retention, what it is meant to do? One key argument for data retention has always been the necessity for access to traffic data for law enforcement authorities in cases of serious crimes. A study by German federal police (“Bundeskriminalamt”) showed, that traffic data as a key evidence is raising the success of law enforcement by a hilarious 0.0059% [1].

Of course, this figure does not mention the importance of traffic data used to investigate on copyright infringements on a non-commercial scale. Due to some surveys, 17% of all internet users in Germany are downloading music [2] - this makes an approx. 42 Million down loaders as potential targets in Europe [3].

But what makes data retention so dangerous is not (only) law enforcement, but intelligence investigation: traffic data is revealing the connection between people and between organizations.

And this is the most important point: what happens to a society, when the people know, that their communication and thus their connections are completely transparent?

In my lecture, I will show that data retention is not an appropriate instrument to hunt down child abusers and terrorists, but with the extension to even copyright infringers it is getting worse: overriding fundamental rights, such as secrecy of telecommunications, by implementing legislation, which affects everybody, is a serious threat.

And this threat is driven by an alliance of content industry, security sector industries, law enforcement authorities, secret services - and politicians, who serve a subjective illusion of security to the masses.

1 AK Vorrat (Arbeitskreis Vorratsdatenspeicherung [Working Group on Data Retention], Berlin, e-mail: rcrf@comcarte.net.)
Therefore, data retention is just a nail in the coffin besides others from the point of view of a human rights activist.

References


[2] Forschungsgruppe Wahlen, 4-6 2008, deutsche Erwachsene (n=2.376);
   http://www.forschungsgruppe.de/PM_Strukturdaten/

SHOULD A NEW RE-USER RIGHT BE CREATED IN COPYRIGHT LAW AND HOW CAN IT BE OPERATIONALIZED?

Robin Elizabeth Herr$^{1,2}$

Abstract
The concept of re-use has been thrust onto center stage because its basic tools are available at a cheap cost to anyone with a computer. Yet the productive potential of the re-use culture has not been fully embraced in legislation. A compelling question is whether copyright law can be adapted to encourage re-use while at the same time it can continue to be supportive of creative processes that require traditional protection in order to recoup investments.

One suggestion is to recognize the rising importance of those who productively re-use the creative works of others by establishing a new re-user right in copyright law. The goal of this paper is to begin to define the concept of the re-user and to explore the principles under which re-use could be regulated. Three types of re-users are defined: the traditional re-user, the aggregator and the productive transformer. Principles under which their re-use could be allowed involve weighing cost savings coupled with the harm done to the original producer. In cases where there is both cost savings and little or no harm or an actual benefit to the original producer, then re-use may be allowed.

1. Introduction

In a boldly-titled book, *The Wealth of Networks*, Yale Law School Professor Yochai Benkler argues that the near ubiquitous ownership of tools for creative production is fueling a post-industrial economic model which can be more efficient at producing culture, knowledge and information than the previous capital-intensive industrial model.[2] Inputs to this new economy include the networked computer and, although not named as such by Benkler, the re-use of copyrightable content. Policy decisions that support this revolutionary development, which Benkler terms the networked information economy, can make or break its outcome. He suggests that we have about ten years to make these decisions.

My question is whether copyright law can be adapted to encourage this new economy while at the same time it can continue to be supportive of creative processes that require traditional production incentives to recoup capital-intensive investments. The goal of this paper is to provide background information in order to begin to define the concept of the re-user and to explore the principles under which re-use could be regulated. Pending further refinement, a general definition of the re-user is a secondary user who transforms original contents for another productive purpose whether it is to

---

1 J.D., M.S., Ph.D., Assistant Professor at CBS Copenhagen Business School, Denmark. E-mail: reh.jur@cbs.dk.
See also [1].

2 This is a working paper subject to revision and refinement. Kindly do not cite or quote without the author's permission.
create a non-competing or complementary copyrightable work or to engage in another valuable activity such as scientific research.[3]

To my knowledge, no one else has forwarded the idea of recognizing a new stakeholder called the re-user and of exploring whether their needs should be explicitly regulated. A precedent has been set by the recognition, for the first time, of the rights and obligations of the ordinary user within the 1996 Database Directive.[4] Moreover, the Directive on the Re-Use of Public Sector Information is designed to specifically encourage re-use.[5] Most recently, the Commission has sought feedback on whether an exception for user-created content should be implemented.[6]

There exist several compelling reasons to seriously explore the concept. First, the reality is that many successful business models are built around re-use and, as a result, the phenomenon begs further investigation. Second, economic analysis of the law suggests that the greatest productivity can only be achieved through encouragement of a certain amount of re-use.[7] Lastly, an application of economic principles could be used to encourage re-use without unduly hurting producers of original content.

In fact, a thorough articulation of the concept of re-use and how it should be regulated could have profound consequences. To date, the overall legislative approach to the digital revolution has been to strengthen copyright and to narrow exceptions and limitations in an effort to prevent unauthorized copying and dissemination. But the addition of the re-user reveals an important stakeholder who is dependent on both protection and access. At the conceptual level, the result could be an acknowledgement that production incentives and access are of equal importance. At the policy level, it could spell the introduction of a new re-user right. At the level of our society, it could invigorate creative production.

2. Methodology

Although there are many potential areas where re-use could be encouraged, I will begin by focusing on the exceptions and limitations of copyright law. Towards this end, the following factors will be considered: (1) the testimony of various categories of re-users and the legal difficulties they encounter; (2) an exploration of re-use in economic analysis of the law; and (3) suggestions of economic principles under which re-use could be potentially governed.

Because the concept of the re-user is so new, this paper is meant to serve as background knowledge for discussion. At the conference itself, I plan to evaluate the testimony of the re-users, to further refine the concept of re-use and the principles under which it should be governed, and to consider whether any reforms of the exceptions and limitations of copyright law are necessary and, if so, what they should be.

3. Who is the Re-User?

Whether we are talking about artistic creativity, software innovation or encyclopedic rendition, we all know that society’s achievements are not derived out of thin air, but are based upon the work of others. While re-use has always been around, recent developments have multiplied the potential for this type creativity on a global scale. Yet the productive potential of the basic tools of this new culture – cutting, pasting, annotating and transforming – has not been embraced within the regulation of copyright.
The notion of re-use has been thrust onto center stage because its basic tools are available at a cheap cost to anyone with a computer. Given the heightened prevalence of these tools, it is worth considering: 1. what types of re-users exist; 2. what kinds of re-use are employed; and 3. what legal obstacles are encountered. Discussion will be limited to re-users who could potentially fall within the exceptions and limitations of copyright as they, themselves, have testified to the Commission and to the UK Government. In the absence of any detailed study, it must be noted that these descriptions are not comprehensive, but rather represent a sampling.

Re-users operate in every sector of the economy from commercial to noncommercial to public to commons. They depend on various types of re-use ranging from traditional re-users whose practices fall within a copyright exception, to aggregators who repeatedly re-use incremental amounts to transformers who engage in productive re-use. The problems they encounter include inconsistency in the various Directives that affect their activities, a lack of clarity in the exceptions and the impossibility of performing certain types of re-uses without risking liability.

The media provide an example of a traditional re-user whose actions comprise the exploitation of a limited amount of content in order to report, critique or review. Their activities fall under the scope of copyright exceptions such as Article 5(3)(c) which allows use by the press on current topics and in connection with the reporting of current events and Article 5(3)(d) which allows quotations for criticism or review. However, the scope of these exceptions is narrowed in a few Member States.[8] Even though such use is permitted in the majority of Member States, the presence of technical measures may render such re-use impossible in practice if not under the law or the application of the database content right may render the re-use illegal.[9]

Other traditional re-users include those who use materials for teaching or scientific research. They face the same problems as the media and may have it even worse due to greater inconsistency in implementation among the Member States.[10] In order to perform their jobs, all traditional re-users, no matter what copyright exception they fall under, require consistency among the Member States and among the various Directives that regulate copyrightable works.

A new type of re-user can be called the aggregator. They harvest, compile and sort online content. Examples include www.aok.dk, which provides a city guide to Copenhagen, Yahoo! Europe, which serves as a management resource to the online world and www.rottentomatoes.com, which is primarily a guide to movies. These websites offer a valuable service to users by helping them access, search, analyze and understand the plethora of content available online. Content producers also benefit when users become aware of their websites.

Aggregators engage in repeated takings and displays of small amounts of online content. Yahoo! Europe is dependent on being able to harvest information from other websites and to display the search results which may contain thumbnails, references and links to the original content. The legality of some of their activities remains unresolved. For example, there exists conflicting case law regarding whether or not a thumbnail picture is an unauthorized reproduction.[11] Although websites can place technical measures so that Yahoo! web crawlers will not take their information, this does not always occur. Even if permitted under the Copyright Directive, it still may infringe the database contents right of the Database Directive if the cumulative takings qualify as an unauthorized extraction or re-utilization.[12] In order to carry out these normal activities without
risking legal action, aggregators need to be ensured that their actions fall within the scope of copyright exceptions.

The last type of re-user, the productive transformer, takes part of the contents of a work and transforms it into another productive work. It could be a graphic artist who incorporates parts of paintings into his or her artistic expression. According to the Arts Council of England, “Many creative practices and strategies fall outside the narrow confines of copyright law. Some creative work also runs the risk of breaking the law, as legal systems often do not take account of the network and distributed nature of contemporary art.”[13] There could be many types of productive transformers from commercial artists to producers of educational materials to amateur dabblers.

The European Commission is tackling part of the transformers’ problems by eliciting feedback on the possibility of creating an exception for user-created content. They employ the OECD’s definition of this activity which is, “content made publicly available over the Internet, which reflects a certain amount of creative effort, and which is created outside of professional routines and practices.”[14] The question here is whether a broader category of transformers should be covered, what activities should be encouraged and under what precise circumstances.

4. Economic Principles

According to the incentive theory of intellectual property, legal protection is needed to provide an impetus for production.[15] At the same time, however, it is well-recognized that creativity does not emerge out of thin air, but is based upon the works of others. Some empirical evidence suggests that cheap access to public sector information encourages re-use which results in greater economic productivity.[16] The fact is that unauthorized copying can be productive, “Uncompensated gains are pervasive and universal; our well-being and survival depend on them.”[17] Moreover, copying can be good for competition, “Freedom to imitate, to copy, is a cornerstone of competition and operates to minimize monopoly profits.”[18] Thus, copyright laws worldwide contain mechanisms such as a fixed duration and copyright exceptions in order to grant access.

Despite a general acceptance of the necessity of legal incentives to encourage production, empirical evidence is inconclusive as to whether such incentives work. Landes and Posner maintain that “the economic arguments that we make for intellectual property protection are not based primarily on a belief that without legal protection the incentives to create such property would be inadequate. That belief cannot be defended confidently on the basis of current knowledge.”[19] Indeed, empirical and theoretical studies on the book and periodical industry, for example, offer evidence that certain sectors could function in the absence of copyright law.[20] Moreover, an empirical study on the effect of performance rights royalties on musicians found that no additional incentives were provided.[21] Lastly, in the area of patent law, it has been shown that an increase in patent duration may or may not increase innovation depending on the relationship between competition and innovation in the particular industry.[22]

Because the veracity of incentive theory is inconclusive and it is impossible to tell where exactly the balance should lie, various opinions exist on how much production incentives are needed and how much access should be granted. In their 2003 book *The Economic Structure of Intellectual Property Law*, Landes and Posner show that the optimal level of copyright protection is lower than that provided by absolute rights, thus substantiating the importance of re-use to achieve the maximum level of production. The authors explore the relationship between the level of copyright protection
and total social welfare.[23] They focus on the production of copyrightable works by both copiers, which is a somewhat narrower category than the re-user, and by producers of original works.[24]

The authors conclude that an increase in copyright protection decreases welfare per work but increases total social welfare because the producer creates more works than any reduction in production by the copier. In order to arrive at such a conclusion, it must be demonstrated that the benefits of protection are greater than the costs. The benefits of higher protection, according to these academics, are that producers can meet their fixed costs and be more productive. The costs of protection are that costs will increase for both producers and copiers and that welfare per work will decrease as well because there is less access.

The authors admit that their determination is speculative.[25] The bottom line is that we simply do not know what the impact of stronger protection is, especially where access may be a priority and the need for protection is unproven. Where re-use is an important factor in production, it may be that stronger protection decreases total social welfare. For example, when copiers stop making new works total production could actually drop. Thus, it is worth exploring whether in certain sectors of the economy the logic of a standard law and economics analysis is inadequate when all re-users are factored back into the picture.

Brett M. Frischmann of Loyola Law School and Mark A. Lemley of Stanford Law School attempt to pinpoint exactly where the positive effects of re-use, which they term spillovers, are so important that open access should be granted.[26] Open access is defined as access to anyone regardless of identity or use. It does not mean that a product is free. They claim that economic analysis of intellectual property has not reconciled the fact that spillovers encourage greater productivity and social value. Instead, spillovers are considered uncaptured benefits which distort demand signals and for which producers should receive compensation in order to recoup their investment.

In an article entitled “Property, Intellectual Property and Free Riding,” Lemley explains that because intellectual property rights are not a response to scarcity like real property rights, but actually a conscious decision to create scarcity, efforts to capture the full social value are even more suspect.[27] Potential problems include pushing markets away from the competitive norm, interfering with the ability of other creators to make use of a work, high enforcement costs and rent-seeking. Thus, when it comes to production incentives, the authors advocate minimum incentives, which they define as enough to recoup the fixed costs that subsequent producers do not face and no more.

The authors argue that when intellectual property functions as a generic infrastructural input the productivity gains from re-use are so significant that such inputs should be managed in an openly accessible manner. Examples of such inputs include basic research, the Internet, operating systems, abstract ideas and peer-to-peer file sharing technology.

However, a problem emerges in clarifying when demand signals distort enough to require open access. The authors state that in terms of commercial production, the demand signals can be adequately calibrated according to willingness to pay. But it could also be true that demand signals are wrong for a commercial product. For example, a private good could be used as an input for noncommercial production. Or use of a good could benefit third parties in such a way that the value to society is not met by satisfying private demand. The question then becomes when is re-use so important that open access is required, and why draw the line at generic infrastructural inputs?
If it is discovered that re-use enhances production of copyrightable works in certain sectors of the economy, then it may be argued that a regime of minimum incentives should be established. Rather than focusing on defining precisely what kind of works require open access, it may be worthwhile pinpointing the conditions under which re-use should be allowed. Once again, the work of Landes and Posner provide a valuable starting point.

The authors provide a whole new twist on fair use analysis, the U.S. equivalent to the statutory exceptions detailed in EC copyright law, “The question for an economist is not production or transformation versus reproduction or suppression, as such, but the impact of the copying on the demand for the original and the potential cost savings and other benefits that are likely to arise from reducing the cost of creating a new work that builds upon the original copyrighted work.”[28] The first factor is whether the use saves on the transaction costs of licensing. In other words, does it lower the costs of copies? The second factor is whether the use harms or benefits the original producer. For example, does it expand demand for the product?

Several reinterpretations of fair use cases are detailed. They begin with the employment of quotations as a clear example of a high transaction cost, no harm case. Quoting saves licensing costs and causes no harm to the original producer because transaction costs are so high that the producers would not be able to capture those benefits anyway. Alternatives to licensing, such as a liability rule or a compulsory license, they assert, would be equally expensive.

The next series are implied consent, negative harm cases. The easy case here is book reviews. Even though the original producer would lose money on a licensing fee, book reviews are a form of advertising that can increase sales. In addition, book reviewers save on transaction costs.

The case of *Sony Corporation of America v. Universal City Studios* concerns whether or not VCRs facilitate copyright infringement.[29] Time-shifting, or the taping of TV programs to watch at another time, was considered to be a substantial noninfringing use and a benefit to the original producer because otherwise that section of the audience would be lost. The decision was criticized because it failed to balance the harm from infringing uses against the benefits of noninfringing ones. The authors state, “Striking the correct balance might be impossible, since from a social standpoint the harm is not the reduction in copyright revenues but the reduction in consumer and producer surplus caused by the impact of infringement on the creation of new copyrighted works.”[30]

In attempting to pinpoint what kind of re-use should be allowed, it is important to ensure the ability of the original producers to recoup their investment. The analysis conducted by Landes and Posner may provide a potential test. The test would weigh the costs savings for the copier coupled with the harm done to the original producer. In cases where there is both cost savings and little or no harm or an actual benefit to the original producer, then the re-use may be allowed. Additional elements worth considering, of course, would come from the fair use doctrine itself.

## 5. Conclusion

The purpose of this paper is to provide some background information on the possibility of creating a new stakeholder within copyright law called the re-user, who that re-user is and what kind of principles should regulate the re-user’s activities. Armed with this information, the task at the conference presentation is to evaluate whether the needs of re-users affected by the copyright
exception are valid and are being met, and, if not, how they can be addressed. Such an evaluation requires a more rigorous legal analysis and a more critical mindset.

6. References

[1] A native Californian, Robin Elizabeth Herr graduated from Columbia University’s School of Law (J.D.) and its Graduate School of Journalism (M.S.) in New York City. In 2008, she completed a Ph.D. degree in law at the Copenhagen Business School in Denmark. As Assistant Professor at CBS, her research interests include adapting international copyright law to the Internet culture.


[3] The re-user can be contrasted with the ordinary user who simply uses a copyrightable work for their own consumption. A producer can be defined as the first producer of an original work.


[10] For a description of the differences in implementation of the exception for teaching and scientific research, see the European Commission, 2008 Green Paper, pp. 16-19. According to the Institute for Information Law’s 2007 Report on the Implementation of the Directive, the exception on incidental uses has not been implemented by Austria, Belgium, Czech Republic, Estonia, France, Greece, Italy, Latvia, Luxembourg, Poland, and Slovenia.


[15] Parts of this section come from or are inspired by Robin Elizabeth Herr, Is the Sui Generis Right a Failed Experiment? (Ph.D., Copenhagen: DJØF Publishing, 2007).


[19] Ibid., pp. 9-10.


[23] They define total social welfare as a function of welfare per work, which is the sum of consumer and producer surplus generated for each individual work produced, plus the total number of works created, both copies and originals. In terms of welfare per work, for consumers, it amounts to how much each individual is better off as a result of buying on the market. For producers, it is the amount of income received minus the cost to make each additional unit of a product.

[24] While copiers seem to be only involved in duplication or transformation of an original work into another copyrightable work, re-users extend to those who use a work to engage in a completely different activity such as scientific research.


A PRIVATE AFFAIR IN THE UK:
COPYRIGHT LAW IN TRANSITION –
PRIVATE COPYING AND FORMAT SHIFTING
EXCEPTIONS

Dinusha Mendis¹

Abstract
This paper looks at the private copying exception and its application to format-shifting as recommended by the UK Gowers Review of Intellectual Property, December 2006. This latest development in copyright law, whilst heralded by consumers has been criticised by the Music Business Group representing music managers, songwriters, publishers and performers and as such has been shrouded with controversy, particularly in relation to the levy or compensation system. The paper sets out the different arguments for and against such a system, considers the impact of the private copying exception within the context of the file-sharing and mobile reader devices before setting out an analysis and a conclusion.

1. Introduction

Intellectual Property law in the UK is in a phase of transition: in December 2006 the Gowers Review of Intellectual Property (hereinafter Gowers Review) was published, recommending changes to various aspects of Intellectual Property law. In the area of copyright, the most contentious issue was UK Intellectual Property Office’s proposed recommendations to implement an exception for private copying and format shifting without compensation. At present, UK Intellectual Property Office’s current recommendation also leaves the UK at odds with the rest of Europe. In every other major European territory an exception for private copying is counterbalanced by mechanisms such as a levy system that compensate creators and right holders.² However, whilst, the Gowers Review advocates a private copy and format shifting exception, it is very much against introducing a levy system and this paper will particularly take an insight into the issues which have arisen as a result.

This paper will initially and by way of background briefly set out the current UK law surrounding copyright exceptions before moving on to introduce the Gowers Review of December 2006. Thereafter, the paper will set out the proposed recommendations relating to the private copying exception and format shifting. This proposed change in the law is at present under scrutiny and has raised a number of issues which this discussion will highlight. For example the paper will address and discuss the contentious issue of the absence of a compensation system in the wake of introducing a private copy exception and also whether the private copying exception legalises peer-to-peer file-sharing which has also been a source of concern for right holders. Thereafter, the paper

¹ LLB(Hons) (Aberdeen); LLM, PhD (Edinburgh); Barrister; Lecturer, University of Central Lancashire, UK.
will move on to address the question of the classes of work which the exception applies to: would it apply to sound recordings, films and also literary works? For example, would the private copying and format-shifting exception cover the transfer of an entire literary work to a mobile reader device such as the Sony Reader (similar to transferring a CD to a MP3 player)? As such, which acts exactly would be non-infringing? How many format shifts would be allowed? This paper will address and answer these questions amongst others.

2. The Law: Copyright Exceptions

The current copyright law as set out in the Copyright Designs and Patents Act 1988 (hereinafter 1988 Act) does not provide for a private copying exception. The exceptions to copyright which are ‘permitted’ under the copyright law in the UK are set out in Chapter III of this Act. The permitted acts are broken down into a number of categories of which some include fair dealing for purposes of research and private study; criticism and review; incidental inclusion of copyright material; exceptions relating to education; exceptions relating to libraries and archives and so on. Nowhere in the Act, is ‘private copying’ or ‘format-shifting’ – i.e. transferring copyright material from one form of media such as a compact disc (CD) to another form of media such as a MP3 player – to be found. Therefore as the law stands, copying a CD to a computer for use with a MP3 player is an infringement of copyright under section 17 of the 1988 Act – reproducing the work in any material form, including storing by electronic means. Section 70 of the 1988 Act bears a resemblance to the proposed private copying provision, but was designed with ‘time-shifting’ in mind as opposed to ‘format-shifting’. Section 70 – recording for purposes of time-shifting – reads as follows:

70. –The making for private and domestic use of a recording of a broadcast or cable programme solely for the purpose of enabling it to be viewed or listened to at a more convenient time does not infringe any copyright in the broadcast or cable programme or in any work included in it.

Although this section does not explicitly use the words ‘private copying’ it does imply that copying is permitted for recording of a broadcast or cable programme if it is carried out for private and domestic purposes with the sole purpose being to view or listen to it at a more convenient time. However with rapid technological development, there has come into being various ways in which media can be accessed and stored in different formats – from CDs, DVDs, Internet to MP3 players such as Apple iPod and to mobile-reader devices such as the Sony Reader. These developments has meant that the music industry is finding it increasingly difficult to turn a ‘blind eye’ on the vast amount of copying, both for private and public use which is going on, at present.

The lack of a specific private copying exception in the UK has now become more pronounced than ever before. Without such an exception, and as the law stands, it makes it illegal, for example, to copy music from a CD that one has purchased on to a computer or MP3 player that one has also legitimately purchased. Much of the British public is unaware or unconcerned that their actions are prohibited under the law. In June 2006 the BPI announced that: “we believe that we now need to make a clear and public distinction between copying for your own use and copying for dissemination to third parties and make it unequivocally clear to the consumer that if they copy their

---

4 The exceptions relating to education are set out in sections 32-36 of the 1988 Act.
5 Libraries and Archives exceptions can be found at section 37-44 of the 1988 Act.
6 For an overview on the introduction of the private copying exception, see, Rose N., An overview of the proposed introduction of a private copying exception into UK copyright law [2008] 19(4) Entertainment Law Review, pp. 75-77.
CDs for their own private use in order to move the music from format to format we will not pursue them”.

3. An Introduction to the Gowers Review of Intellectual Property

The foundation for the Gowers Review was laid two and a half years ago on 2 December 2005. Mr. Gordon Brown, the British Chancellor of the Exchequer at the time, announced that there was a need to review the intellectual property rights in the UK, and called upon Mr. Andrew Gowers, former Editor of the Financial Times to lead an independent review into intellectual property rights. On 23 February 2006, a formal call for evidence was published and on 21 April 2006 the Review’s call for evidence closed. Eight months later, on 6 December 2006 the Gowers Review was published.

The Review set out the following as one of the main reasons for re-assessing the intellectual property rights in the UK:

“Intellectual Property is a critical component of our present and future success in the global economy ... the IP framework must balance the need … to encourage firms and individuals to innovate and invest in new ideas and creative works … [and] ensure that markets remain competitive and that future innovation is not impeded.”

In other words, the Government reiterated that the intellectual property laws should reflect a fair balance to benefit both the creator and the user. Furthermore with the widespread use of the Internet and with an aim to provide a long term strategic vision for Intellectual Property (IP) policy, based on sound economic principles a number of practical issues remained to be addressed with the existing framework.

4. A Copyright Levy: Love it . . .?

Recommendation 8 of the Gowers Review proposed to introduce a ‘limited private copying exception by 2008 for format shifting for works published after the date that the law comes into effect’. This recommendation also went on to state that there should be no accompanying levies for consumers. Whilst the limited private copying exception for format shifting brought about issues of its own, the ‘no accompanying levies’ suggestion, has proved to be the most controversial.

Recommendation 8 states that format shifting from one format to another, such as from a CD to another media such as the iPod is an entirely legitimate activity which should be clearly set out in the law: it should be explicitly stated in the legislation, rather than leaving it to implication. As such, the proposed private copying exception per se does not pose too much of a problem.

However, under the Information Society Directive, countries are able to enact a private copying exception provided that ‘fair compensation’ is given to rights holders. Article 5(2)(a) and (b) of the Information Society Directive (hereinafter InfoSoc Directive) reads as follows:

5(2).- Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

---

8 Evidence from BPI to House of Commons Select Committee for Culture, Media and Sport Inquiry into New Media and the Creative Industries.
10 Directive 2001/29/EC
(a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the right holders receive fair compensation;

(b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned...

In accordance with Article 5(2) of the Information Society Directive, countries such as France, Germany and many others have imposed levies on hardware and blank media. Known as the ‘copyright levy’ system in many EU countries, the levy is charged on blank discs, MP3 players and other electronic products which can be used in the pirating of copyrighted material.11

Contrary to the practices of such countries, the Gowers Review points out that one of the main problems with levies is that “they are blunt instruments: the amount is fixed and therefore does not reflect the number of times a device is used, nor can it compensate for each individual copy”.12 The Government insists that the levy systems lacks a clear system of accurately distributing the royalties to rights holders as it is very difficult to determine whose music is being copied. It is possible that the Government may have arrived at this decision for a number of reasons. At present the European Commission is to consult on whether to change the current controversial surcharge on devices or storage media which can hold music or video.13 The levy is controversial because it assumes that all such devices are used to some extent for copying purposes.

In the wake of these concerns over the levy system, the most recent amendment of the German Copyright Act14 re-confirms the lump sum remuneration as a fair compensation for private copying. However, the Bill modifies the determination of the remuneration, where until now the rates were calculated according to an Annex to the German Copyright Act. According to the new law, interested parties themselves will settle any disputes. This means that the associations of the producers of devices and carriers will have to negotiate the remuneration together with the collecting societies. This in turn means that any devices and carriers will be subject to the payment of a remuneration, which can be used for the making of lawful private copies, although this will not hold true if those same devices or carriers can only theoretically be used for such purposes.15

Addressing the criticism forwarded by the European Commission and distinguishing UK’s private copying exception from countries such as Germany, the UK Government emphasised in February 2008 that since the proposed private copying exception is narrow in scope, there is no obligation for payment under the InfoSoc Directive for a limited format shifting exception. Their reasoning for this decision was based on the fact that no significant harm to the right holder can arise from a limited exception which would need to be compensated.16

Unfortunately this has not been a welcome suggestion and has raised more questions for right holders, the music industry and the consumer rather than making the position clear, as the Gowers Review had hoped to do.

11 Ibid., and op. cit., Gowers Review n. 7 para. 4.75.
15 For a discussion of the Bill, see, op. cit., n. 2 Vahrenwald A., p. 18.
16 Ibid.
4.1. . . . Or loathe it?

Whilst the Government has made it clear that it does not wish to embrace the levy system which most of the other European countries have in place, the Government also does not suggest an alternative form of compensation in the Gowers Review. This could have consequences on the music industry and record companies could reflect the cost of copying in the sale price of CDs and downloads. This can only mean one thing: it implies that the price of CDs will go up and begs the question whether the new private copying exception will be used as an excuse to ‘hike’ the prices of CDs.  

Whilst the Government does not provide an alternative system, it is clear from reading the Gowers Review that the UK favours the system proposed by Recital 35 of the InfoSoc Directive. Recital 35 states:

In cases where right holders have already received payment in some other form, for instance as part of a licence fee, no specific or separate payment may be due. The level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive. In certain situations where the prejudice to the right holder would be minimal, no obligation for payment may arise...

If right holders know in advance of a sale of a particular work that limited copying of that work can take place, the economic cost of the right to copy can be included in the sale price. The “fair compensation” required by the Directive can be included in the normal sale price. This means that any private right to copy cannot be extended retrospectively as copies of works already sold would not include this “fair compensation”.

The alarming response to this issue as suggested by Andrew Gowers is to charge a block licence fee for consumers’ back catalogues: collecting societies may wish to consider making a single block licence available to allow consumers to format shift their back catalogues effectively. Apart from being a controversial suggestion, it can be questioned whether it is practical to request a consumer to pay £200, for example, for the right to retain their collection of music on their iPod, which has been transferred from CDs which have already been bought and paid for? It further raises questions on enforcement and implementation.

Whilst the Government has put forward strong views against a levy system, the UK music industry appears to have other ideas. The UK music industry on 08 April 2008 strongly rejected the Government’s proposal to legalise the transfer of music from CDs to MP3 players without a levy. The music industry called upon a ‘tax’ on devices such as iPods which the industry said should compensate artists for the transfer. The Music Business Group (MBG), a trading body which represents music managers, songwriters, publishers and performers and comprises organisations such as BPI, AIM, MCPS-PRS has rejected plans set out in the UK Intellectual Property Office’s (IPO) consultation document to allow transfer without any extra charge being levied. In a statement, MBG stated that last year alone over 20 million MP3-capable portable devices were sold in the UK, and over 90% of music on such devices contained music which had been copied (as opposed to be

---


20 British Phonographic Industry (BPI); The Association of Independent Music (AIM); Mechanical Copyright Protection Society (MCPS) – Performing Rights Society (PRS).
About 10 days after this press statement, a thriving discussion was inspired on ‘Dot.life – A Blog about technology from BBC News’ titled ‘The iPod tax Resurfaces’. Arguments for and against a levy system were presented on this Blog (although arguments against a levy system dominated the discussion), of which an argument for and against from the discussion have been extracted:

“If the record industry (and if this goes ahead, I am sure that the film industry will want their share as I have a couple of DVDs copied to my iPod) wants to charge us for transferring the music from one format to another, surely, they are getting in to the realms of selling us the rights to the music. Therefore, if I have an accident with a CD, they should be required to replace it (at no cost to me) as I have purchased the rights to listen to the music, independent of format, and not just brought a CD that I currently have to replace if it gets damaged”.

“Actually although you think this is laughable, this sort of things has happened for years. Companies that produce background tapes for shops have to pay a licence to the BPI for the right to copy. Same applies to aircraft music, radio stations who wish to copy on to another format … It is all about protecting the rights of the people who write the music. With the internet, the public and the media have just assumed that it now means that anyone can do as they please and to hell with the writers. The tax is probably impractical, but to be honest, there is no control left and really no one gives a damn”.

Whilst arguments can be presented for and against the levy system, the curious fact about the argument presented by MBG implies that creators and right holders receive a fair share from sales, which they could now be missing out, due to format-shifting. However, whether in the UK or elsewhere in the world, the fact that right holders receive a fair share from sales appears to be more of a myth than a reality. A study carried out in US in 2007 which gives an insight in to the ‘CD Cost Allocation Figures’ unravelled the following story. According to the study, $7.00 (approximately 39%) goes to the retail store that sells the disc to the customer. $9.50 (approximately 53%) goes to the record company that produces the disc and typically owns the copyright in the sound recording. The record company’s share, in turn, is subdivided as follows:

<table>
<thead>
<tr>
<th>Allocation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2.57</td>
<td>14%</td>
</tr>
<tr>
<td>$0.95</td>
<td>5%</td>
</tr>
<tr>
<td>$1.42</td>
<td>8%</td>
</tr>
<tr>
<td>$1.52</td>
<td>8%</td>
</tr>
<tr>
<td>$0.76</td>
<td>4%</td>
</tr>
<tr>
<td>$0.19</td>
<td>1%</td>
</tr>
</tbody>
</table>

This study is further enhanced by the words of a former musician (now lawyer) who also describes how the system works:

22 iPod Tax Resurfaces at http://www.bbc.co.uk/blogs/technology/2008/04/the_ipod_tax_resurfaces.html
There’s a saying among musicians: before you sign a record deal, get out your dictionary and look up the word “recoupable.” Recoupables have been a part of major label contracts forever, and they work like this: your band has paid its dues, generated a buzz, and potentially stands ready to reap the benefits of this work in the mainstream marketplace. A label approaches you and says, we’ll spend maybe a hundred thousand on recording and releasing your record. We own the masters. You get roughly a tenth of the money we make from selling it, but all the money we spend on recording, on manufacturing, on promotion, on touring, on deli trays for the music writers is taken out of your tenth. If the record looks like a hit, the label will keep spending the band’s small share on more processing, promoting, and so on. Why not? Once the act is selling, it behoves a label to spend as much of the band’s future income as possible and reap virtually all the returns. This is why a major release frequently needs to sell 500,000 copies — go gold — before sales proceeds begin reaching the band’s pockets... All in all, the deal offered to artists by a major record label is, you get the glory, and we get the money.24

If this is the reality of the situation, then one has to question who exactly will benefit from the levy system. Ultimately the question remains whether in accordance with the Government proposal the price of CDs should be raised or in accordance with the MBG the price of all hardware such as iPod should be raised, through the introduction of a levy system. Whichever path is chosen and irrespective of who will ultimately benefit from this new system, one factor remains certain: it is inevitable that it is the consumer who will be affected the most by these latest changes to the copyright laws in UK. It will be the consumer who will have to face increased charges either in the form of increased CD prices or an increase in hardware such as computers, MP3 players and potentially mobile-reader devices, as a result of the levy system.

5. From a private copying exception to file-sharing and mobile-reader devices

In view of the above arguments, it is also interesting to consider peer-to-peer (P2P) file sharing. The concern which arises here is whether the private copying exception could be seen to legitimise P2P file-sharing. Although a reading of Recommendation 8 of the Gowers Review does not make the position ‘crystal clear’, UK Intellectual Property Office’s (IPO) Consultation (which closed on 8 April 2008)25 has re-iterated that the proposed exception would be subject to limitations as set out above – ‘the owner would not be permitted to lend, sell or give away the copy made, nor share it more widely’26 – which captures P2P file-sharing. For example in Germany, private copying remains lawful also in the digital world, but the private copying limitation “is not applicable, if the copy is made from an obviously unauthorised reproduction and, as the Bill states expressly, if the obviously unauthorised reproduction is offered for download online”.27 This means that the prohibition of private copying extends to peer-to-peer Internet Service if it was obvious to the user – or should have been to him – that the offered film or music was an unlawful offer, for example, if the work was only recently published so that no private person could have the right to offer the work for download.

A further indication that P2P file-sharing is clearly disallowed in UK under this new exception arises from the fact that the recommendation goes on to state that the owner would not be entitled to retain the copy if they no longer had possession of the original (even though in practical terms this will be a provision almost impossible to enforce): one of the reasons for the music industries’

continued concern. In any case, the intention of the exception is clear: ‘format-shifting’ is meant to, and should apply purely for personal use.

In the present context and due to the unclear status of the types of work, it is also interesting to consider the validity of a mobile reader device such as the Sony Reader and the use of format shifting for this purpose. The Sony Reader was first launched in September 2006 and entered the US market in April 2007, and on 2 October 2007, an updated version of the Reader (PRS-505) was released.28 Not long after it first emerged in the US market in 2006, Sony was asked a number of questions about its latest device.29 One of the questions put to Sony was whether the Reader permits the sharing of books? In response to the first question, Sony answered that: “although you cannot share purchased eBooks on other people’s devices and accounts, you will have the opportunity to register five Readers to your account and share your books accordingly.”30

In accordance with the Gowers Review, it appears that uploading a book to a mobile-reader device such as the Sony Reader or iRex iLiad is permissible as long as an intermediate step has been taken to transfer the book to a mobile-reader device. This could be done either by visiting a site such as Project Gutenberg31 - which stores a large number of books available free of charge – and temporarily storing the eBook in one’s computer, ready to transfer in to the mobile-reader device. A second method would be to transfer any file from the computer to the Sony Reader or the most complex system would be to scan an existing book in to electronic format, before uploading it on to the Sony Reader. The Gowers Review does not provide any guidance on format shifting in the area of literary works or on hardware such as mobile-reader devices. The discussion is very much focused on music and MP3 players. However, in reality, the mobile-reader devices have entered the market and devices such as Sony Reader do exactly what Apple iPod did for music, and could potentially pose a bigger threat than MP3 players.

As pointed out above Sony Reader admitted that “although you cannot share purchased eBooks on other people’s devices and accounts, you will have the opportunity to register five Readers to your account and share your books accordingly”.32 Could this be interpreted as multiple copying or multiple-access which according to the Gowers Review’s recommendations is not allowed? However with a lack of guidance on this area and with the Gowers Review having only considered MP3 players as far as format-shifting is concerned, the debate remains open.

6. Analysis and Conclusion

This paper has drawn a line through the existing exceptions to copyright, the proposed exception on private copying and format shifting and considered the issues arising from such a proposition. The paper focused on the copyright levy system and the push by the MBG to introduce levies on technological devices such as computers, iPods etc. who argued that a private copying exception if introduced, should be supported by a compensation system. Arguments for and against this

30 Ibid.
31 Gutenberg Project, (Last accessed 02 July 2008), from http://www.gutenberg.org/wiki/Main_Page
32 See http://www.makezine.com/blog/archive/2006/08/sony_responds_to_our_sony_read.html
proposition and the recommendation by the Government – which is against a levy system – have been raised, some of which were set out in the preceding pages. Finally, this paper questioned issues such as legality of P2P file-sharing and mobile-reader devices as a possible format-shifting device which has not been addressed in the Gowers Review.

In view of these arguments, the author submits that the real issue lies in the form of private copying and the format to which it is copied. In other words, the sole use of an Apple iPod player is to listen to music; Apple regulates these devices with the use of digital rights management systems; and sharing music directly from an iPod is not possible. Therefore, it is submitted that a tax on such a device is not substantiated. On the contrary the act of copying music/videos to a computer enables the user to share that music with millions of other users as is also the case with downloading music from the Internet. In such a case, placing a tax on a desk top computer or laptop computer is seen to be more viable and possibly more acceptable. However, where private copying applies to format-shifting and where that particular format, does not allow the sharing of music but is limited to an individual’s use, then a tax on such a device can certainly be questioned.

Furthermore, the Gowers Review recommends that the private copying should be limited to ‘format shifting’ (i.e. transferring a work from CD to an MP3 player or from a video tape to a DVD), rather than simply allowing any copies to be made for private purposes. The exception also applies only to personal or private use and the owner would not be permitted to sell, loan or give away the copy or share it more widely. Multiple copying would also not be allowed. The exception also allows one copy per ‘format’, provided that the transfer between formats is preceded by an intermediate step.

However, what is less clear is the types of work to which format-shifting applies for purposes of private copy. The UK IPO addresses this question, but does not answer it. As Nick Rose in his article points out, there are three choices presented; (1) apply the exception solely to sound recordings and films (on the basis that these are the types of works most suited and most regularly “format-shifted”); (2) apply the exception to all categories of works; and (3) tailor different exceptions to different categories of works.33

It is also interesting to note that Australia went through a similar amendment to their copyright laws when on October 19, 2006, the Australian government introduced the Copyright Amendment Bill 2006 in to the Federal House of Representatives (the lower house of Parliament).34 Amongst other things, the Bill contained a format-shifting exception in the new section 109A of the Act. In accordance with this exception, format-shifting of copyright works will not infringe copyright laws if:

1. The owner of a non-infringing sound recording, literary work or photograph makes a copy (called a main copy) of the sound recording for his or her own private and domestic use;
2. The copy made by the owner is in a different format to the original from which it is made;
3. The recording from which the copy is made was not created by downloading a digital broadcast of a radio broadcast or similar program from the internet (e.g. recording of a podcast); and
4. The owner has not and is not making more than one copy of the recording in the selected format.35

Although UK is as yet in the Consultation process and is quite away from drafting such a format-shifting provision for purposes of private copying, it is useful to look to Australian legislation, particularly in relation to clarity. The Australian provision is clear in the type of work which the

33 See op. cit., Rose N., n. 6 p. 76.
34 Australian Copyright Amendment Act is now in force and received Royal Assent on 11 December 2006.
format-shifting would apply to; clearly prohibits activities such as P2P file-sharing and further makes it clear that whilst format-shifting of podcasts is legal, the recording of broadcasts such as podcasts, if downloaded from the internet, however will be illegal. In looking to the future in relation to domestic legislation, UK can learn valuable lessons from Australia.

A private copying and format shifting exception is to be hailed as a development in the law, in keeping up with technological developments.36 It appears to be the next logical step in the development of copyright law, in maintaining the all-important balance between the right holder and user/consumer. As UK moves towards this latest development, more clarity is needed in relation to the provision and particularly in relation to the compensation system: whether it be a levy or not. If not, copyright law in the UK will be a legal minefield.

7. References


36 Greiger C., The answer to the machine should not be the machine: safeguarding the private copy exception in the digital environment [2008] 30(4) European Intellectual Property Review pp. 121-129.
INDEX OF AUTHORS

Barczewski Maciej .............................................. 93
Czychowski Christian ......................................... 49
Derclaye Estelle ................................................. 137
Dietrich Yann ..................................................... 85
Dimmich Agata .................................................. 21
Gaster Jens .......................................................... 13
Guibault Lucie .................................................... 75
Henrion Benjamin ............................................. 133
Herr Robin Elizabeth ....................................... 211
Jakob Georg ..................................................... 115
Kasprzycki Dariusz ........................................... 61
Koščík Michal ................................................... 101
Mendis Dinusha ................................................ 219
Moritz Hans-Werner .......................................... 69
Müller Benoît ................................................... 59, 99
Nordemann Jan ................................................... 49
Ożegalska-Trybalska Justyna ............................. 107
Piesiewicz Grażyna ........................................... 57
Pilch Hartmut .................................................... 115
Polčák Radim .................................................... 199
Rauber Andreas ................................................ 171
Rauhofer Judith .................................................. 195
Remmert-Fontes Ricardo Cristof ........................ 209
Saarenpää Ahti ................................................... 181
Schlötter Richard .............................................. 135
Schweighofer Erich .......................................... 171
Sowinski Mikolaj ............................................... 207
Wiebe Andreas .................................................. 19, 29
Wimberger Knut ................................................ 125