Next Library, **Conference, Aarhus 2011**.

Time: 20 June 11:00 - 12:30
Location: LAB 3 CONCERT HALL
Type: Interactive Session

Does Freedom of Information Exist in the Internet World?

Introduction

In this presentation I will focus on two issues: The consequences of electronic publishing for libraries and the freedom of information on the Internet.

In both cases we see a tendency that access to information is controlled by interests and forces outside of the libraries, and that the freedom to access information is endangered.

The main headlines of my presentation are

- Publishing and libraries
- Privatization of control
- Internet and data protection
- Internet and law enforcement

Publishing and libraries

Since the end of the 90'ties, scientific journals are primarily published in electronic formats and distributed in packages, compiled either by the publisher or by distributing agencies. We see the same development with books.

The distribution of mainstream products

It is convenient and reduces transactions costs subscribe to packages of journal articles or book databases. The problem however, is the same as with television: The supplier decides what is in the package, and he may not be interested in distributing infrequently used material. It fills up the database and does not give much revenue.

From Collections to Connections

Acquisitions are substituted by subscriptions. Libraries subscribe to an internet access-point at the publisher or distributor's database.

Libraries started a move from having collections to having connections. This move is not yet fully completed, as books are still primarily acquired in print. We also still have some printed journals. However, the end of this period is in sight. With the development of reading devices, we are approaching the end of the Gutenberg era.

In addition, we see libraries discarding printed material, which is available in electronic formats. The rationale of this development is twofold: Improved services and savings.

Improved services and savings

The search and retrieval facilities in full text databases are incomparably better than earlier bibliographic searches followed by time-consuming procedures for getting the material form the stacks or via inter library loans from other libraries. Now users have immediate access to full text databases 24/7 the whole year.

The transaction costs are minimised. 20 years ago, the journals department had a staff of 25 employees managing 8.000 foreign journals. Now four persons manage the subscriptions of 43.000 electronic journals.

This development is an immense improvement of services at reduced costs. However, there are no free meals.

Privatisation of control

The consequence of this move from collections to connections is that the supplier decides what is in the package, and he may not be interested in distributing infrequently used material. It fills up the database and does not give much revenue.
As to the content of the package, libraries will no longer be able to control the authenticity of the content or that content is not removed from the databases.

Neither will the library be able to control long-term preservation. This is so because the library no longer has physical control over the files.

It will also be difficult to control conditions for access and use, because use will depend on licence agreement, and the publisher can dictate the conditions and enforce them by installing TPMs (Technical Protections Measures).

Removed content

It is very difficult to detect whether content has been tampered with, but it happens regularly that content is removed from the databases. In many cases, the content will be available from another distributor, but sometimes it simply disappears.

It may also happen that an author regards an earlier work as a youthful aberration whose contents or quality do not meet his present standards. If the work is published in print, the author can do nothing about it. However, if it is published electronically in a database, the work may simply be removed or be substituted with a new edition.

Privatisation of the digital literal heritage

In most countries large-scale digitisation will require private entrepreneurs (e.g. Google), or public / private partnerships. To the extent that digitisation is done by private entrepreneurs, there will have to be room for cost recovery – also for material in the public domain. The consequence is that private entrepreneurs will be able to control conditions for access.

The truth of the matter is that except for a few countries there is not the political will to allocate the necessary funds. Therefore, we will see large-scale privatisation of our literal heritage.

Internet and data protektion

With the development of computerised processing of personal data and the possibility to make cross-searches in several databases at the same time, there has been increased awareness of the need to protect privacy, In the 1980ies, many countries introduced legislation in order to protect personal data.

Since then the development of the Internet, the World Wide Web, and very efficient search machines have increased the political sensitivity of the issue, and the need for even stricter data protection is often voiced.

Within the European Union the Directive 95/46/EC on the protection of personal data[1] presents some serious legal problems in respect to harvesting the internet. I can here only summarize the main problems.

The main problem consists in the extremely wide scope of the directive. This is illustrated by the definitions of 'personal data' and 'processing of personal data':

- 'Personal data' means any information relating to an identified or identifiable natural person ('data subject').

- 'Processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Rights of the data subject

The principal rules of the Directive are that

- The data subject should give his consent, and if the data are collected without the knowledge of the data subject, he should be informed, unless this is impossible in practice.
- The data subject has the right to access the data
- Inaccurate or incomplete data should be erased or rectified
- The processing of sensitive data is prohibited. Sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.
- Access to sensitive personal data may only be given for research or statistical purposes.

Of course, there are exceptions to this, and the Directive has a long list. It even allows Member States, for reasons of substantial public interest, to lay down exceptions in addition

[1] 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 data. (Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31 ff.)

to those laid down in the directive, either by national law or by decision of the supervisory authority. In such cases certain procedures have to be followed.

Sensitive information

Everybody who has been surfing the internet knows that the internet contains lots of personal information, and that a substantial proportion of this information is sensitive.

Therefore the mere collection of the data, the harvesting of the internet, requires that it is recognized to be of substantial public interest and that a special permission is granted either by national law or by the supervisory authority.

Access

According to the directive personal data may only be accessed for research purposes and only after permission by the supervisory authority.

The consequence of this is that as long as we have not separated (sensitive) personal information from other types of information, the whole internet archive must be regarded as "sensitive". Therefore, in principle, any access requires the permission by the supervisory authority.

Digital retro conversion

The Directive on the protection of personal data is very complicated and it may be implemented differently in Member States. The Nordic countries have a tradition of rather strict protection of personal data. However, the lesson we learnt from this was, that the Directive will probably apply also for personal data created in the process of digital retro conversion of printed material, e.g. newspapers, periodicals and books.

Internet and law enforcement

The enforcement of copyright on the internet has been considered difficult. The illegal data are often placed on servers outside the jurisdiction of the country and is therefore out of reach. However, recently users in Denmark were met by the following screen (see figure next page) when trying to link to Pirate Bay.

STOP - Adgang hindret

Ved Københavns fogedrets kendelse af 25. oktober 2006(allofmp3.com), 15. august 2007(mp3sparks.com) og 29. januar 2008(thepiratebay.org) er Tele2 A/S (en del af Telenor) blevet pålagt at hindre vores kunders adgang til www.allofmp3.com, www.mp3sparks.com og www.thepiratebay.org.

Fogedretskendelsen i de 3 nævnte sager kan i sin helhed hentes her:

Fogedrets kendelse AllofMP3
Fogedrets kendelse MP3Sparks
Fogedrets kendelse thepiratebay.org
Østre Landsrets stadfæstelse thepiratebay.org

Tele2 A/S har ikke foretaget nogen registrering af din adgang til denne side.

Instead of trying to seize the illegal copies, rights holders succeeded in getting an injunction ordering the telecommunication companies to block access to the service provider. As there are only a few telecommunication companies in Denmark this is a relatively simple operation.

The problem is that such steps may not only block for access to illegal data or services, but also for third parties legal activities. However, a third party who might be affected by the court order has no say in the court's dealings with the injunction. That is only an issue between the rights holder and the telecommunication company. Undesirable consequences for third parties are not considered by the court. Neither is the service provider, whose presumed illegal activities are blocked, part of the court's hearings.[2] That happens only afterwards, at the justification proceedings.

Virtual Schengen Border

A Virtual Schengen Border is contemplated by the *Law Enforcement Working Party*. This Working Party was unknown to me, but a quick search on the internet revealed that LEWP (Law Enforcement Working Party) is a working Group within the domain 'Justice and Home Affairs' of the Council of the European Union. According the Belgian Federal Police's homepage "The importance of the LEWP working group in the decision-making process within the Justice and Home Affairs Council of the EU can hardly be overestimated."[3]

In the minutes from a meeting held the 17th of February, we can read under the heading of "Cybercrime"

"The Presidency of the LEWP presented its intention to propose concrete measures towards creating a single secure European cyberspace with a certain "virtual Schengen border" and "virtual access points" whereby the Internet Service Providers (ISP) would block illicit contents on the basis of the EU "black-list". Delegations were also informed that a conference on cyber-crime would be held in Budapest on 12-13 April 2011." [4]

If these proposals are implemented it may well prove to be the most serious attack on the freedom of information in European history after WW2.

Harald von Hielmcrone

State and University Library
Aarhus

[2] Clement Salung Petersen, "Netværksoperatørernes rolle i bekæmpelsen af ophavsretskrænkelser", NIR, 2009 nr. 1 s. 32

[3] http://police-eu2010.be/mu-eu2010/en/working-groups/police-cooperation-working-party/wg-law-enforcement-party/

[4] OUTCOME OF PROCEEDINGS of: Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party, on: 17 February 2011, Subject: Summary of discussions. Brussels, 3 March 201, 7181/11, ENFOPOL 44, ENFOCUSTOM 13