

Internet in the Library – the Sky is Not Blue Comments on the Selected Library Problems When Offering Patrons Access to the Internet.

Błażej Feret

Main Library, Technical University of Łódź,
223 Wólczańska Street, 90-924 Łódź, Poland,
Blazej.Feret@bg.p.lodz.pl

Barbara Szczepańska

Polish Library Association – Commission for Electronic Publications
Lovells International Law Firm, Warsaw, Poland
Barbara.Szczepanska@lovells.com

Abstract:

In the past few years, libraries, including academic libraries, became not only a place in which users could find information supporting teaching and research, but also hubs for patron access to the Internet and its vast resources. However, the Internet is not a “good boy”, and the information easily found with search engines or peer-to-peer programs may be used for bad goals. Should academic libraries promote unrestricted access to the Internet for the sake of people’s right to open access to information, or should they rather restrict and filter the incoming information to that actually related to the subjects of studies? If information is to be restricted, then to what and how should it be restricted?

Another question is what is legal in the library and what is not? For example: is it legal to install and use peer-to-peer programs like eMule or Kazaa? Ninety-nine percent of the time they are used for downloading music, video and program files from other users. In most countries it is illegal to distribute music and movies in the form of electronic files, but the related legislation is in many aspects still not precise.

So what should library policy be towards the Internet access and use in the library?

Quite often the problems of misusing Internet tools extend from user to staff and pose the following question: what is allowed for library staff regarding the use of Internet and how deeply should the managers control the staff activities and content of their PC-s?

The paper will aim at describing the most important problems that libraries face when providing access to the Internet.

Keywords:

Internet, library, legal problems.

Introduction

For the past decade or so, libraries and library managers have been coping with the problem of electronic exchange of information and access to Internet on the premises of their libraries. What was, and probably by many still is considered a blessing for librarians, a wonderful information and communication tool and “a Sesame of knowledge” – the Internet, now brings at least as many problems as benefits. In the course of past years, librarians learned (or at least they have been trying to learn) how to use electronic information resources, not only those that for many years were considered credible, but also the as yet unknown ones. They learned how to be Web Cinderellas and to separate the valuable information available out there in the open Internet, from the remaining mass of information trash and dirt. And although they are aware that the ease of using tools like Google is illusive, they cannot refuse the demands of users (and authorities) to put computer workstations in libraries and let users play with the Internet. How could they resist these demands? Wouldn't it be throwing out a baby with the bathwater? After all, the Internet IS a great tool to distribute valuable information and most of us would probably have difficulties in day-to-day operations without it. So what's all this fuss about?

The problem is that we, especially in academic libraries, expect our patrons to use Internet tools for purposes related to the processes of education or research. But the truth is that even in the United States, where the culture of Internet use should be the strongest, a lot of “academic” online time is wasted for non-professional and non-educational purposes. According to the reports by Pew Internet & American Life Project [1], more than half of college students use Internet primarily for social communication and entertainment. Another report [2] says that the top five websites, where the traffic from college students was particularly high, were online music services, file sharing and chat servers. That is the case in the USA. So how about countries, where the Internet revolution has only begun? The percentage of inappropriate use of Internet in academic environments (including libraries) is certainly much bigger.

The question is whether academic libraries should control how their patrons use computers and restrict inappropriate use or, sticking to a position of providing unrestricted access to (whatever) knowledge, should they provide open, uncontrolled and unrestricted access to the Internet? What would be the implications of eventual limitations and restrictions? Would this generate unnecessary conflicts and disagreements? If so, what are the areas of potential conflicts and confrontations between users and librarians? Or even among librarians themselves?

Are we, library managers, ready to solve all these conflicts? Do we have appropriate policies? Do we know what is legal and what illegal in libraries?

In this paper, the authors are trying to select and describe the most common and at the same time the most ambiguous situations that occur in libraries and add some legal comments and observations. The paper does not pretend to be a comprehensive analysis of the problem. The intention of the authors was rather to turn the attention of library managers, especially in countries where the legislation does not follow reality and practice sufficiently quickly, to problems that at the first look may appear trivial, but may have serious legal consequences. The four selected areas, namely limits of Internet use by staff, peer-to-peer file sharing, access to adult content, and the position of libraries in the face of terrorism threats, are only examples of problems, which are stimulated by internet access in libraries and related, ambiguous legislation. The authors hope that the paper will alert

library directors to have a closer look at the services they provide and laws that may be linked to them.

Use of Internet Services by Library Staff

Although most confrontations, with Internet use in the background, occur between patrons and the library staff, there are also problems related to use of Internet services by the librarians themselves.

The expansion of computer use and the Internet made us dependent on services like e-mail and WWW. Many librarians use these services in daily work, sending e-mails and searching for information on the Web. Library directors expect that available Internet tools will be used exclusively for work-related purposes. However, it often happens that library staff make use of e-mail for entirely non-official purposes, like sending private messages, chain letters, funny pictures or jokes. Sometimes, they also use official tools for remunerative activities or just for pure fun. The question then is whether the employer is entitled in such cases to monitor the “electronic” activities of the employee and penalize or even fire the person, if he/she uses the official equipment or software inappropriately. What complicates the problem is the fact that private use of computers at work, unlike the use of copier, printer or telephone, does not generate extra costs for the company and is therefore much more acceptable.

Let us briefly analyze the problem of the use of email service by library staff.

In the USA, the privacy of the Internet is regulated by Electronic Communications Privacy Act (ECPA) [3]. This act allows companies to monitor employees' emails when one of three provisions is met: one of the parties has given consent, there is a legitimate business reason or the company needs to protect itself. These conditions are interpreted by lawyers according to actual situation and needs. State laws (e.g. in California) are usually in favor of employee rights: to monitor, the employer must inform staff about the intention, and employees have to confirm in writing that they have been informed, and that they know the rules of Internet usage in the company.

In most of cases, American courts have ruled in favor of employers, recognizing their right to check the content of email being sent from official e-mail accounts, although there is a difference between “monitoring” and “filtering”, which may influence the line of judgment. Monitoring (auditing) is controlling email content after data transmission, while filtering (interception) is controlling content during the data transmission [4]. Several cases have upheld the right to check email after transmission (i.e. email auditing is legal), since this is viewed as no different than searching through a file in an employee's drawer. For instance, in a criminal case against a CIA employee charged with receiving inappropriate emails (United States v. Mark L. Simmons), the court ruled that the viewing of personal email did not violate federal wiretapping laws, since the email was not viewed while it was being transferred but read from the email inbox. Email filtering (interception) has not as clear status as email monitoring and it falls under above mentioned wiretapping laws. However, cases in the United States have shown that most forms of email interception are permitted if this is done in a reasonable way, and if the company has an appropriate email policy in place. The Library of Congress regulations state that using the Internet by employees is a privilege, but not a right, and that this privilege may be revoked at any time [5]. A good example is also the case of Smyth v. Pillsbury Company [6], in which the employee was fired for communicating unprofessional and threatening comments over the company's email system to a member of the sales staff. When the employee claimed that the

company had violated privacy laws, the court concluded that no reasonable person would consider the interception to be a highly offensive invasion of privacy, and that the company's interest in preventing inappropriate or unprofessional comments or illegal activity outweighed any privacy interest.

However, in several other cases related to use of company email services, rulings were different from the the ones described above. For example, in the case of Intel v. Ken Hamidi [7], Intel charged its former employee of “trespassing” on its IT systems to distribute thousands of emails, which criticized Intel’s former employer. After several appeals from the state court, the US Supreme Court ruled in favor of Hamidi, with argument that distributing email was not “trespassing”, but just “using” Intel’s email system to communicate with other employees.

In South Africa it is not enough to inform an employee about monitoring activities undertaken by an employer. The latter cannot legally dismiss an employee on account of misuse of company email systems, if the employee has not agreed and not signed a clause allowing the employer to monitor his email or telephone calls [8]. In turn, in 2003 Australian court has ruled that sending or receiving emails containing pornography may be reason for firing an employee, even if he/she has not been aware of company’s policy of using Internet.

In Europe, work on new legislation concerning the problem of using electronic mail in work environments is in progress in France and Germany. A new law in preparation in Germany is going to protect the privacy of employees regarding their email messages. The draft proposes that employers should be able to control official email messages only as to the nature of the email – whether it **is** or **is not** an official email, but not as to its content. Employers should inform employees about the company policy but would not be allowed to read the content of emails, especially private e-mails [9].

Polish Labor Law does not directly regulate matters related to the use of email and the Internet by employees. Monitoring email by employers, regardless of the legal status of this activity, raises many emotions and controversies. However, lack of appropriate regulations does not mean that it is not possible to judge legality of using company email for private purposes under Polish Law.

Labor Law in Poland obliges the employee to render the employer work services and to comply with the agreed time for work and with the internal work regulations. If so, the employee cannot use work time for activities other than those stated in the employment contract without permission of the employer. At the same time, computer hardware and software should be treated as work tools because the employer provides these tools not for the private purposes of the employee, but for company related work. Therefore, we can assume that using official email for private purposes is a clear violation of job duties, which are prescribed by the Labor Law and the internal regulations in the company. To prove that an employee has used official email for purposes not related to his/her work, an employer has to open and check the content of email letters. This poses a question if the employer is allowed to read employee’s emails without violating his/her privacy. However, authorization of the employer to control the company’s email system and content of emails results in Poland from regarding this system as a work tool, being owned by an employer. Email is stored on the employer-owned server. Electronic mail being sent by employees from the official, company email server contains a “stamp” telling from where the email has been sent. Using such email for private purposes is equivalent in a “paper” office to sending a private letter on the company’s letterhead. Thus, based on current Polish Law, if the employee uses company tools and breaks the law, actions of his/her employer

aiming to control such behavior cannot be regarded as violation of anyone's privacy.

Polish courts have only begun to investigate cases related to the use of electronic media. However, in 1997, the Polish Supreme Court ruled that using company telephones for private purposes is a violation of job duties [10]. Moreover, this can be even regarded as a strong violation and be a reason for dismissal. By analogy, such a ruling may be applied to cases of private use of official email. Currently, in several dismissal cases of employees who have been accused of misusing official email systems, Polish courts ruled in favor of employers, recognizing that they have had right to fire the person.

The problem of inappropriate use of the Internet by staff in Polish libraries is still underestimated. The general practice in libraries is that the use of workstations with access to email and the Internet is not controlled and not monitored. In case of workstations used by a single person, managers are usually too tolerant and too restrained to interfere in someone's computer work content. When computer is used by several people, the problem is even more difficult – who did what, and when? A result is that sending and receiving private emails or searching the Internet to find answers to non work-related questions and problems, is regarded as normal, as long as it does not influence regular job activities and efficiency. It is usually left to the employee's sense of duty to decide if and how much of work time is spent on private activities. In turn, library staff with high self-esteem would certainly regard any control and monitoring activities as offensive and inappropriate in an institution such as a library. Unfortunately, the quality of library employees degrades and being exposed to attractions of electronic media, staff should be at least partly controlled.

According to a 2001 survey, 42% of US employers monitored their employees' emails but only 60% actually had an adequate written policy in place [11]. In many companies, also in Poland, employers regulate the use of office equipment with special instructions, but they usually do not say anything about monitoring staff activities. However, if employers monitor activities and emails without warning, they are arguably infringing on an individual's privacy and therefore susceptible to workplace privacy lawsuits. Also, library directors should protect themselves and their institutions in both ways: against the inappropriate use of Internet by staff by monitoring their activities, and against claims of violating the individual's privacy. The only way to do this is implementing an email and monitoring policy and communicate it to the employees. The rules should be included in the library's work rules or, if that is not possible, in a separate document provided for the staff. Such procedures permit the avoidance of many misunderstandings and problems, especially in case of a court trial. Without the described measures, the library and every other entity providing their employees with email and Internet access may face serious legal threats.

Peer to Peer file downloading

One of the students' favorite activities on library computers is downloading images, music, video or software with the use of peer-to-peer (P2P) programs like Kazaa, Morpheus, BearShare or other. All these programs are successors of Napster, which has been banned by the San Francisco District Court in 2001. But while Napster was distributing mp3 files centrally and could be "centrally" closed, peer-to-peer networks do not use centralized servers and closing down such networks with a single order or ruling is not possible, because nobody but the owner of the individual computer providing content is – if at all – violating law. It means also that programs and protocols for file sharing are legal. What may be

illegal in certain countries is mainly distributing (not possessing) copyrighted intellectual property, especially for profit.

Librarians are not very happy about using peer-to-peer programs on Internet workstations in libraries for two basic reasons: one, because very often they are not sure whether downloading whatever files one can with the use of this kind of program is legal; two, because downloads are usually completely unrelated to study and research. Because of these arguments, libraries usually forbid installing and using peer-to-peer programs by internal regulations. Breaking these rules has consequences like the refusal of right to use Internet workstation in the library, at least for some time, or other. But do we have the right to forbid peer-to-peer? What if students want to share documents or other, perhaps copyrighted but widely distributable manuals of software? What if, using Kazaa, someone wants to benefit from legal files, like we did some time ago with ftp storage servers? Another thing is that sharing music and video files, which in many countries is being regarded as computer piracy, IS NOT everywhere in fact piracy and illegal. Therefore, when we make decisions on forbidding peer-to-peer programs, we must have a set of serious arguments at hand. Otherwise, libraries may be accused of limiting access to information.

Another thing is that stopping determined students from using peer-to-peer programs in libraries, where Internet lines are very good and guarantee fast downloads, is very difficult. Even if forbidden by internal regulations, peer-to-peer programs are easily available on the Internet and easily downloadable and installable. Traditional watching of screens in computer labs to control who is doing what (unless done remotely), does not very often reveal those breaking the rules, not to mention internet workstations in open areas of the library, which remain beyond visual control. Also, a range of other, more automated tools like refreshing hard disks after each user session and limiting session times does not bring satisfying results in limiting unwanted activities.

So maybe we shouldn't control at all the use of Internet workstations by students. Perhaps we should secure our public workstations against permanent changes of configuration and let people play with them while limiting the time of a single session. If an appropriate notice is displayed and on a workstation during login (Internet policy), the responsibility for an eventual breach of copyright law is the user's, nor the library's. But even then, we should be aware of what IS in fact the current law regarding peer-to-peer downloading music and video in many countries, the same way as we are aware of any copyright violations regarding printed material.

At the beginning of March, 2004, the European Parliament adopted a Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights [12]. The directive states that the main enforcement measures need to be applied only with respect to acts committed on a commercial scale. These are acts carried out for direct or indirect economic or commercial advantage. This would normally exclude acts done by final consumers acting in good faith. Private individuals who download music or films for their personal use would not be targeted in the light of the project. If this project is accepted by the European Union Council, libraries in the EU will have the problem of installing peer-to-peer programs solved for some time. If so, librarians would then sigh with relief: they will not be charged with abetting crime.

But for the time being, the situation is not that clear. The number of peer-to-peer networks is growing, and research has shown that the largest user class consists of

students operating from within university computer networks including libraries [13]. RIAA – Recording Industry Association of America – the organization to protect intellectual property rights in American music industry, consequently undertakes actions to limit peer-to-peer sharing of licensed music material. In the last months, they sued next group of over 500, P2P networks users.

The actions of RIAA did not gain a wide approval of American courts. The courts ruled that P2P network operators cannot be sentenced for illegal copying of files by users of the network [14]. In addition, recently a New Jersey woman, one of the hundreds of people accused of copyright infringement by the RIAA, has countersued the big record companies, charging them with extortion and violations of the federal antiracketeering act! The woman's attorneys claim that by suing file-swappers for copyright infringement, and then offering to settle instead of pursuing a case in which liability could reach into the hundreds of thousands of dollars, the RIAA is violating the same laws that are more typically applied to gangsters and organized crime [15]. It is also ironical that RIAA itself has been using third-party software for tracking P2P traffic, infringing two patents owned by Altnet, partner of Sharman Networks – operator of Kazaa [16]. These developments limit RIAA activities very much and statistics show that after a temporary breakdown in swapping files caused by closing Napster, swapping has again start to climb.

American libraries have also taken a stand against the P2P limiting actions by RIAA and other organizations. The Association of Research Libraries, the American Association of Law Libraries, the Medical Library Association and the Special Libraries Association have formed a coalition for P2P networks (Amicus). In September 2003, they have been joined by the American Library Association in the efforts to support P2P network operators in several cases. "Amicus" have issued a common brief, supporting file-sharing companies Grokster and Morpheus in their defense against a copyright-infringement suit brought against them by MGM Studios and 27 other entertainment companies [17]. However, "We are not supporting the wrongful sharing of copyrighted materials," emphasized ALA Executive Director Keith Michael Fiels September 24, 2003 in an e-mail to the ALA Council discussion list. Rather, he explained, the library associations are seeking to uphold the principle that "free speech and the public interest are best served by rules that allow new and innovative mediums of communication to develop and flourish."

In Poland, there are also organization protecting intellectual property rights (ZAIKS, SWAP, ZPAV, STOART) which, like RIAA, may undertake actions against individuals who illegally distribute music files on the Internet. According to one of the ZPAV expert Jan Baldyga: "Basing on current Polish law it is possible to conduct legal, penal and civil actions against persons, who multiply music recordings on their computers and using Internet and P2P networks, without consent of respective music labels. Such responsibility may also be extended to Internet providers. Also, basing on mutual international agreements, ZPAV may act on behalf of foreign producers. Restricting actions of this kind have already started and will be intensified" [18]. As a result, 10-20 WWW and FTP services are closed each month.

Antipirate Coalition by ZPAV, FOTA and BSA started an awareness campaign on the legality of P2P services. In the first stage, more than 600 companies and almost 100 academic institutions were targeted. Antipirate Coalition was distributing a free copy of GASP – a program to make an inventory of software and other

resources. It allows one to remove useless (from the Antipirate Coalition point of view) files from the company computers.

On the other hand, ZAIKS does support activities of RIAA and Antipirate Coalition. According to Anna Zakrzewska-Biczuk of ZAIKS, RIAA policy does not produce the expected results and does not meet the expectations and needs of music fans. Accordingly, ZAIKS despite its legal rights, does not conduct any actions against P2P users.

From the technical point of view, it is possible to track down every Internet user, so P2P users can no longer feel completely anonymous and safe. Sharing a large number of files and access to a certain computer by large number of external users can be easily watched by an Internet service provider. Providers might be legally obliged by authorities to reveal the names of such users, especially if there is a suspicion that he/she acts illegally. Potential evidence found on computer disks and logs of user activity provided by the ISP would certainly be enough to begin an inquiry.

In addition, Polish libraries may face legal problems based on the Law on Liability of Collective Subjects for Acts Prohibited under Punishment [19], which states that if a person, as a result of neglect by institution's management, violates certain laws (also: infringing intellectual property rights), the institution is a subject to a financial penalty.

How may library managers and libraries protect themselves against the legal consequences of improper behavior of their users? The only reasonable policy for today, in countries where legislation is not clear, is to introduce clauses in by-laws, prohibiting the use of P2P services. Regulations must also include the declaration that the library closely cooperates with organizations enforcing intellectual property rights, that all computer activities are logged (and logging must really be done), and that in case of any legal problems the responsibility is the user's, not the library's. It would be the best to have users acknowledge with their signature that they have read the rules and accept them.

Another method of limiting unwanted activity is to set up a packet filter on incoming IP routers. If the activity in question uses a specific IP port (as is in case of chat or P2P), the packets may be filtered out. This solution requires appropriate technical conditions and knowledge.

For these in Europe, let us hope that the UE directive under debate will be introduced and that libraries will have clear interpretation what is legal regarding P2P usage and what is not.

Adult content

The great debate on pornography on the Internet has also reached libraries. When Internet workstations are widely available in libraries, directors and staff are concerned about possibility of easy access to web sites with pornographic content. How then should libraries and librarians behave? Should they limit access to the Internet by installing filtering software or, supporting the idea of unrestricted access to knowledge, should they allow users to browse all, even the darkest parts of the Internet universe?

American authorities have been demanding public debate on access to adult content for a long time. Claims for legislation that public libraries should block the access to pornographic content increased upon discovering that library patrons, including minors, regularly search the Internet for pornography and expose others to pornographic images by leaving them displayed on Internet terminals or printed

at library printers. As a result, the US Congress enacted the Children's Internet Protection Act (CIPA), which prevents public libraries from receiving federal assistance for Internet access unless they install software to block obscene or pornographic images and to prevent minors from accessing material harmful to them [20].

ALA representatives together with several libraries, patrons, Web site publishers, and related parties, sued the Government, challenging the constitutionality of CIPA's filtering provisions. "Ruling that CIPA is generally unconstitutional and enjoining the Government from withholding federal assistance for failure to comply with CIPA, the District Court held, *inter alia*, that Congress had exceeded its authority under the Spending Clause because any public library that complies with CIPA's conditions will necessarily violate the First Amendment; that the CIPA filtering software constitutes a content-based restriction on access to a public forum that is subject to strict scrutiny; and that, although the Government has a compelling interest in preventing the dissemination of obscenity, child pornography, or material harmful to minors, the use of software filters is not narrowly tailored to further that interest" [21]. Similarly, few years earlier, in 1997, Mainstream Loudoun organization sued Loudoun County Public Library (Virginia) for installing blocking software on library computers with the access to Internet, and thus violating the First Amendment. The court decided that the library had no obligations to provide Internet access to its users, but if it did, it had no rights to install blocking software [22].

However, in June, 2003, Supreme Court of the United States reversed the previous judgment of District Court for the Eastern District of Pennsylvania on CIPA being unconstitutional, and held that CIPA is **not** unconstitutional. CIPA became law, despite protests of ALA representatives, who expressed concern that filtering pornography may also block access to many non-pornography services, because filtering mechanisms are based on simple keywords [23]. The Supreme Court ruling is consistent with the expectations and demands of many religious organizations, which insisted on such regulation [24]. However, it should be stressed once again that this ruling was the completely opposite of the ruling of the lower court in Philadelphia, which was mentioned above.

These examples show that problem of legality of access to pornography and other harmful material in libraries does exist not only on the international level, but also on national levels, where completely inconsistent interpretations do occur even in different courts of the same country.

Further legislation on distributing pornography include also the CAN-SPAM Act [25], according to which all email containing pornography must be specially marked to enable filter it out, but no decision was made about the form of this marking. The latest regulation of the Federal Trade Commission [26] adopts the rule that starting May 19th, email spam which contains sexually explicit material must include the warning "SEXUALLY-EXPLICIT".

In Europe, in the years 1999-2003, European Union ran a program called "Safer Internet". The main goal of the program was to promote safe Internet through subsidizing actions against illegal and harmful content on the Internet [27]. Libraries have participated in the "Safer Internet" program via a separate sub-project "Safer Internet for Knowing and Living (SIFKaL) [28]. The main goal of SIFKaL was to orient the process of education and to inform, to advise and to provide ideas about a safer way to use the Internet. It was directed to all social agents involved in the education of the European citizens, including parents, teachers, local authorities and librarians. Furthermore, it was also directed to

people who have not had much experience with the Internet in their ordinary life. Librarians' role in promoting safe Internet has been formulated in the following way: "Librarians, in a complementary position to the other target groups, are placed between parents, teachers and local authorities. With the emergence of the 'hybrid library', libraries become more concerned regarding where to get information and where to participate in cultural activities and performances and where to interact with others engaging in those activities". Safer Internet program will be continued in 2005-2008 as "Safer Internet Plus" [29] under auspices of the European Commission. In March, 2004, Erkki Liikanen, European Commissioner for Enterprise and Information Society, proposed spending 50 million Euros in the next four years for creating a system that would enable children to use the Internet safely. The program would include financing hotlines, filtering software and actions to raise awareness. "Children have right to use Internet freely, for learning, entertainment or social contacts, but they must be protected from exploitation and deception by adults", said Mr. Liikanen. The program will include equally the public and private sectors and will be directed mainly against child pornography, racism and other harmful content. The program will also employ spam filters.

However, none of the European projects and programs intended to provide new legislation. Instead, they have all played a great role in raising awareness of librarians and users concerning safer Internet [30].

In Poland, more and more libraries face the problem of users opening and browsing web pages with offensive content. Unfortunately, Polish law on libraries does not regulate whether or not, and when to use blocking software in libraries. Even the Polish Library Association has not yet prepared guidelines for libraries, concerning this problem. Also, it seems that Polish courts have not considered cases of this kind. So the guide for preparing internal procedures in Polish libraries should just be common sense. However, it should be noted that watching pornography is not a crime in Poland and libraries, which decide to allow adults to do so, are not breaking the law.

In public libraries, the situation regarding the rationale for providing access to pornography is rather clear (i.e. a library should not be interested in why a patron eventually wants to browse pornography) and library has to be prepared to provide this access to adult persons. In academic libraries, this is less obvious. Even if allowed by law, should a university library provide similar access? If in medical or general universities one could, in the end, find a pseudo-scientific excuse, such an access should be hardly explainable in libraries of technical universities. What are then the solutions for technical university libraries?

To avoid using library computers to access pornography, libraries may either introduce appropriate, exclusion paragraphs in the usage rules for Internet workstations or install filtering software. Libraries in the USA usually install filtering software and inform users about this. In such cases, information to the effect that users may ask that the filtering software be disabled if they want to have unrestricted access to Internet, should be clearly visible. Another option is to install "unfiltered" workstations in a chosen, separate location in the library.

In Poland, most libraries place adequate information in the library rules. A statement that it is forbidden to use the library workstations to browse pages with offending or pornography content is included in the library regulations, but usually without clear description how this ban will be enforced.

In the Polish literature of the problem, authors also stress a viewpoint that on the Internet, access to pornographic material requires a special actions by the user:

entering a keyword in the search engine or typing the direct address to known website [31]. If so, displaying pages containing harmful material, is not the effect of neglect by librarians, but the result of intentional activity of the user, for which the library cannot be held responsible.

Terrorism

Libraries were always guardians of freedom, especially intellectual freedom as defined in the United Nations' Universal Declaration of Human Rights: "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*" [32]. In 1999, IFLA adopted a Statement on Libraries and Intellectual Freedom, in which it appeals to libraries to respect and promote intellectual freedom, unrestricted access to information and expression, and users' right to privacy [33]. And with this tradition in mind, one of authors' colleagues, a director of an academic library in Poland, has been visited by an officer from the Agency for Internal Security (FBI equivalent in Poland) and asked to think about the possible tracking of library users, who express interest in terrorism, dangerous chemical substances, bombs, etc. This visit raised a question, where the dividing line is between users' right to privacy and the rights of authorities to access library files, which contain personal data, preferences etc. Are we, library directors, obliged to collect and store data about users, and to provide them to appropriate authorities, violating the Declaration of Human Rights and IFLA directives? Do we have to acquiesce in the demands of a single officer coming to the library? Should we contact the university authorities?

These questions probably would not be asked if it were not for September 11. But in the post-9/11 era, more and more security services investigate more and more cases, collect more and more data on suspected individuals. This activity has also affected libraries, and it is an important fact that preparing for September 11, terrorists used libraries as hubs of the network, and Internet as a communication medium [34]. This is the basic reason to include terrorism as one of the important topics related to providing Internet access to library patrons.

Obviously, it was the US legislation, which reacted promptly for the new needs. In October, 2001, the US Congress passed a bill "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act", known as the Patriot Act [35]. The act gave the FBI new powers to investigate terrorism, including the ability to look at library records and computer hard drives to see what books patrons have checked out, what Web pages they have visited, and where they have sent e-mails. Librarians, who refuse to cooperate may be arrested and charged with obstructing the work of FBI. In addition, cooperating librarian may not inform anyone that the FBI was asking the questions, including the patron being investigated.

The Patriot Act started a great public debate in the US (and in the rest of the World) on the right to privacy, powers of the FBI, and also on the real intentions of President Bush. Many organizations, including the American Civil Liberties Union, Electronic Privacy Information Center or Campaign for Readers Privacy [36] started campaigns against the Patriot Act. A part of the library community in the USA also came out against the new law, expressing their attitude on different occasions [37]. They have been recalling readers' right to privacy and basic rules of intellectual freedom. Several libraries keep resisting the Patriot Act by removing users' data from library computers and files as soon as they are not required [38]. Another method of legal resistance against the Act is raising the

awareness of users about the consequences of the Patriot Act, as is being done by Jassamyn West [39]. These are not isolated examples. Soon after September 11, in October 2001 IFLA/FAIFE Committee prepared a statement on Terrorism, the Internet and Free Access to Information, in which it gives a strong support to maintaining patrons' privacy and anonymity [40]. However, all these statements and actions do not change the fact that FBI has the powers to confiscate computer equipment for investigation if necessary, as happened in Delray Beach, Florida [41].

In the European Union there are no special directives regarding the threat of terrorism, which would be directed to, or applied strictly to libraries. However, after September 11, almost all European countries prepared new laws or regulations, which entitle security services to access electronic information in computer networks [42]. Even if the legislation does not directly mention libraries, the new powers of special services are usually extensive enough to include data being processed in libraries.

In Poland, the body which is approved to investigate cases of threat of terrorism is the Agency for National Security (ABW). In the legislation on ABW, there is a statement that local administration, state and public institutions are obliged to cooperate with ABW and to help the Agency in fulfilling its tasks [43]. Since libraries are public institutions, they are obliged by law to assist ABW officers, and consequently library directors have to provide all requested information.

Unfortunately, in the age of international terrorism, the borderline between freedom of a single human being, and attempts by governments to protect it will be increasingly ill-defined. Libraries will have to continue their mission without guarantees that they are able to ensure privacy and intellectual freedom to their users.

For these, who would like to act according to the letter of law, let us quote Judy Matthews and Richard Wiggins, who in their paper on the Internet after September 11, wrote [44]:

Whose decision is it to call the police when a librarian feels she or he has encountered possible terrorist uses of a library? If a library insists that all staff members go through the director before calling police, what happens when a librarian decides to make the call without approval? What constitutes evidence that a patron is a terrorist? If a teenaged patron is obsessed with information on anthrax or bomb making, can a concerned librarian turn that patron in to the police? Will state laws providing patron confidentiality remain on the books, but ignored? What district attorney or attorney general will prosecute a well-meaning librarian "helping in the war on terrorism?" Will the government's desire for information on terrorists be limited to specific searches of known targets of investigations, or will the government pursue digital dragnets, asking to surreptitiously examine circulation records, Web site usage logs, and search engine logs? How will libraries and the profession respond to such requests?

After the attacks, a number of government agencies removed from their Web sites information on sensitive topics, such as the locations of U.S. nuclear and hazardous chemical facilities. In some cases, agencies asked libraries to remove related materials, whether print or CD-ROM, from their physical holdings. Librarians are accustomed to building and maintaining their collections based on the information needs of their

patrons, not the mandates of government agencies. How will libraries and librarians respond to these new government edicts? What will the effects be on the citizenry's ability (and duty) to remain informed?

Summary and conclusions

Providing access to Internet for library staff and patrons implies substantial changes in internal library regulations. This fact is becoming increasingly accepted by library directors. However, there are still many libraries that do not have consistent and published policy on Internet use for patrons and staff. Most of Polish libraries have not even started works on such a coherent policy. The main reason for this fact is that the fast pace of technology and legal changes force library managers to categorize the emerging problems as more or less important, with current acquisition and circulation problems always on top or the priority list. Such a flood of small and big problems arising in libraries every day does not allow for systematic “patching” of holes in security and services. Problems are being solved as they arise, without earlier discussions and preparation for them. In many libraries certain parts of the organization and workflow remain unchanged for years, despite changes in patrons’ expectations, behavior and personal culture. Unfortunately, very often there are more important problems than internet rules to occupy minds of library managers...

The good news is that many libraries do have partial solutions in the form of statements in library regulations, specifying rules of Internet use by patrons, with special stress put on students. The rules are usually more restrictive than they should be, and they release libraries from any legal responsibility for patron failure to comply with the law when using the tools provided by library. Such a high level of restrictions, which naturally limits users’ freedom to access Internet information resources, lets library directors to sleep peacefully, but often it does not allow them to give clear answers to a patron to the question “why I can’t do this on a library computer, if I need it to my work or personal development?”.

Changing the library environment, including legislation, requires that library directors pay special attention to the legal aspects of providing services to users. This should not be a low priority task, but rather a continuous activity, the goal of which should be to protect the library against any legal action from patrons and library staff.

Acknowledgements:

The authors want to thank Prof. Richard E. Quandt of Princeton University and The Andrew W. Mellon Foundation, for his help in preparation of this text.

References:

All references to Internet websites accessed on the EU Accession Day, May 1st, 2004.

1. The Internet Goes to College. How students are living in the future with today’s technology. Steve Jones et al., Pew Internet and American Life, September 15, 2002. <http://www.pewinternet.org/reports/toc.asp?Report=71>
2. Pew Internet & American Life Project Data memo from: Lee Rainie, Director of Pew Internet & American Life Project, Max Kalehoff, Senior Manager comScore Networks and Dan Hess, Vice President comScore Networks. September 2002 <http://www.pewinternet.org/reports/toc.asp?Report=73>
3. Electronic Communications Privacy Act (ECPA) <http://www4.law.cornell.edu/uscode/18/p1ch119.html>
4. Mike Spykerman: Is email monitoring legal? <http://www.policypatrol.com/docs/email-monitoring-article.pdf>

5. Internet Policies of the Library of Congress
<http://www.loc.gov/loc/webstyle/inetpol.html>
6. Michael A. Smyth v. The Pillsbury Company, C.A. NO. 95-5712, United States State District Court for the Eastern District of Pennsylvania,
<http://www.complaw.com/lawlibrary/smyth.txt>
7. <http://www.intelhamidi.com/> ; <http://cyber.law.harvard.edu/openlaw/intelvhmami/>
8. Internet a Prawo - archiwum wydarzeń, vol.44
http://www.vagla.pl/prawo_044.htm
9. Justyna Kurek: Prywatność korzystania z internetu pracowników w Niemczech.
http://www.vagla.pl/skrypts/ prywatnosc_pracownicza_niemcy.htm
10. I PKN 93/97 Orzecznictwo Sądu Najwyższego. Izba Pracy 1998/7/208
11. NUA Internet Surveys: Net and email monitoring now standard (June 2001)
http://www.nua.com/surveys/index.cgi?f=VS&art_id=905356827&rel=true
12. Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the **enforcement of intellectual property rights**.
http://www.db.europarl.eu.int/oeil/oeil_ViewDNL.ProcViewCTX?lang=2&procid=6837&HighlightType=1&Highlight_Text=intellectual{ _SPACE_ }property
13. Data from RIAA web pages
<http://www.riaa.org/>
14. Policja wkacza do siedziby operatora KaZaA, Internet Standard, February 2nd, 2004
<http://www.internetstandard.com.pl/news/63555.html>
15. RIAA sued under gang laws. CNet news.com, February, 2004
<http://news.com.com/2100-1027-5161209.html>
16. Kazaa Strikes Back at Hollywood, labels. CNet news.com, January 2003
http://news.com.com/2100-1023_3-982344.html
17. ALA Files Amicus Brief Supporting P2P Technology. American Libraries Online. September 2003.
<http://www.ala.org/ala/alonline/currentnews/newsarchive/2003/september2003/alafilesamicus.htm>
18. Pozwy dla Polaków: nie tylko RIAA. <http://www.idg.pl/news/62732.html>
19. Dziennik Ustaw RP, no 197, .p. 1661. November, 2002.
20. The Children's Internet Protection Act
<http://www.ala.org/ala/washoff/WOissues/civilliberties/washcipa/cipa.htm>
21. Supreme Court of the United States, Syllabus, United States et al. v. American Library Association, Inc., et al. Appeal from the United States District Court for the Eastern District of Pennsylvania, No. 02-361. Argued March 5, 2003. Decided June 23, 2003.
<http://www.onlinepolicy.org/action/20030623.ussupremecourt.cipalibrarydecision.02-361.pdf>
22. Mainstream Loudoun: Internet Policy Lawsuit.
<http://www.loudoun.net/mainstream/Library/Internet.htm>;
Mainstream Loudoun v. Loudoun County Library (Blocking Software Case)
<http://techlawjournal.com/courts/loudon/default.htm>.
23. cf. ref. 21
24. Jeanette Allis Bastian: Filtering the Internet in American Public Libraries: sliding Down the Slippery Slope. First Monday, Vol.2 No.10 - October 6th. 1997
http://www.firstmonday.org/issues/issue2_10/bastian/index.html
25. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)
<http://www.spamlaws.com/federal/108s877.html>
26. FTC Adopts Rule That Requires Notice That Spam Contains Sexually-Explicit Material: <http://www.ftc.gov/opa/2004/04/adultlabel.htm>
27. <http://www.saferinternet.org>.
For 2005-2008 the European Commission prepares a program titled „Safer Internet Plus”: <http://europa.eu.int/iap>

28. Safer Internet for Knowing and Living
<http://www.sifkal.org/>
29. <http://www.safer-internet.net/>
30. Making the Internet Educational in Libraries
<http://www.saferinternet.org/downloads/Libraries-doc.pdf>
31. Warylewski J., Pornografia w Internecie – wybrane zagadnienia karnoprawne, Prokuratura i Prawo 2002, nr 4, s. 53-54
32. The Universal Declaration of Human Rights
<http://www.un.org/Overview/rights.html>
33. IFLA Statement on Libraries and Intellectual Freedom
<http://www.ifla.org/faife/policy/iflastat/iflastat.htm>
34. FBI Targets Library Computers in Terrorism Investigation American Libraries online news. American Libraries Online. September, 2001.
<http://www.ala.org/ala/online/currentnews/newsarchive/2001/september2001/fbitargetslibrary.htm>
35. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.
<http://www.aclu.org/Files/OpenFile.cfm?id=12250>
36. ACLU: <http://www.aclu.org/>
EPIC: <http://www.epic.org/>
Readers Privacy: <http://www.readerprivacy.com/>
37. Resolution Reaffirming the Principles of Intellectual Freedom in the Aftermath of Terrorist Attacks
http://www.ala.org/Template.cfm?Section=IF_Resolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=32463;
Resolution on the USA Patriot Act and related measures that infringe on the rights of library users
<http://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/alaresolution.htm>.
38. Rebel Librarians Go On A Tear
<http://www.cbsnews.com/stories/2003/05/28/national/main555885.shtml>
39. Jonathan Crowhurst : Librarians and The War On Terror
<http://www.freepint.com/issues/040304.htm#feature>,
<http://www.librarian.net/technicality.html>
40. Terrorism, the Internet and Free Access to Information
http://www.ifla.org/faife/news/ifla_statement_on_terrorism.htm
41. Daniel de Vise: Terror hunt may end privacy at the library
<http://www.miami.com/mld/miamiherald/news/3979136.htm>;
42. Stuart Hamilton: September 11th, the Internet and the effects on information provision in Libraries. <http://www.ifla.org/IV/ifla68/papers/156-079e.pdf>
43. Dziennik Ustaw RP. 2002.74.676 (U) Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu art. 10
44. Judy Matthews, Richard Wiggins: Libraries, The Internet and September 11. First Monday, December 2001.
http://www.firstmonday.org/issues/issue6_12/matthews/index.html