Surveillance, data protection and libraries in Europe and the US-notes on an empirical data case study on surveillance and Greek academic libraries

Maria Bottis

1. Academic libraries: values and surveillance issues

Surveillance especially of libraries is a rather unexplored surveillance theme. Especially in the academic environment, rigid surveillance for security reasons is not usually considered a priority in libraries. On the contrary, librarians have been trained to recognize that a library is a place where users enjoy the right to privacy, the right to read anonymously, freedom of research and freedom of information (ALA 1939; Greek Librarian Code of Ethics). Thomas Jefferson indicatively wrote "there are rights which it is useless to surrender to the government and which governments have yet always been found to invade. These are the rights of thinking and publishing our thoughts by speaking or writing . . . the right of personal freedom' (CCLE undated). The US Supreme Court has recognized the right to be free from state inquiry into the contents of one's library (*Stanley v. Georgia,* 1969); the First Amendment of the US Constitution protects the people's right to read and receive ideas anonymously.

Privacy in the library is, therefore, a presupposition of intellectual freedom to read and write and expressing thoughts freely. And libraries have a vital role in the articulation and defence of the fundamental right to intellectual freedom which is stated in Art. of the Universal Declaration of Human Rights (Byrne 2000). In this sense, privacy in a library is, if not an intrinsic, at least a functional value. Library and information scientists now have a greater potential of collecting and storing personal data and need to be vigilant in guarding public trust (Sturges et al., 2003). Besides, confidentiality is the hallmark of the traditional professions, such as law or medicine and information disseminators are in an analogous position with lawyers in this sense (Hauptman, 1982).

On the other hand, security of materials and information in a library is quite essential (Ramana, 2007). Patrons have been reported to steal material, usually related to quite common themes such as psychology and sports, but also, ironically, to law enforcement and criminal justice (Holleman, 2008). Patrons do not only steal books but also mutilate library items (Burrows & Cooper, 1992, Foster,

1995). Libraries, whoever, appear not to strongly penalize offenders (Holleman, 2008), reminding us the Chinese proverb that 'to steal a book is an elegant offense' (Alford, 1997). It is also reported that students see book theft as 'an academic crime' and not a real crime (Johnson, 1981). Book theft and material mutilation is not the only issue though; vandalisms in a library also happen (Lincoln, 1989). Library vandalism can be classified as acquisitive, tactical, ideological, vindictive, play and malicious vandalism (Hart, 2009). In Greece, the most important event occurred in 2010, when the whole of the Library for International and Foreign Law of the University of Athens was totally destroyed by fire in the center of Athens. The offenders were never caught.

2. The European Data Protection Directive 95/46/1997

Protection of privacy in the European Community is very strict. Article 8 of the European Convention of Human Rights provides that 'everyone has the right to respect for his private or family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right such as 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'. The European Court of Human Rights has interpreted this provision on the protection of privacy many times in the past.

Especially on personal data protection, the European Community has implemented 'the privacy Directive', the Directive on the protection of personal data (Fromholz, 2000). The Directive formed a mechanism for the protection of personal data which is not only punitive (protection after the violation of the protection of personal data) but also preventive, as it obliges all member states to institute a formal authority whose task is especially to oversee the implementation of the Directive. The Directive also encompasses administrative, penal and civil sanctions for the violation of personal data. More importantly, the Directive regulates all uses of personal data in any kind of 'environment', that is in both the public and private sector, by any legal and/or natural person for any reason. The very meaning of personal data, that is any kind of data which can be related to a physical person (any information relating to an identified or identifiable natural person ("data subject") is, perhaps unsuccessfully, very wide (Viola de Azevedo Cunha, 2012).

In the same line, the regulation of the 'processing' of personal data uses a very wide concept of what processing is. Processing is the 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;" (art. 2 b of the Directive). The list is not exhaustive, so in effect, processing is any kind of act in relation to personal data and as held by the European Court of Human Rights in the *Bodil Lindqvist* case (ECJ, 2001), the upload of personal data in the internet is data processing, demanding authorization (for example, consent by the data subject).

Therefore in Europe, any kind of surveillance in libraries is also regulated by the data protection Directive 95/46/EC, which provides, *inter alia*, for the confidentiality of library records and internet searches, email correspondence and social network contacts. Every member state of the EU has incorporated the Data Protection Directive and special statues usually regulate data protection in every member state.

As the Directive dictates, all personal data shall be processed fairly and lawfully, shall not be processed unless certain conditions are met, shall be obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose. Also, data collected and processed shall be adequate, relevant and not excessive, shall be accurate and where necessary up to date; data shall be kept for no longer than necessary, protected by appropriate security and shall not be transferred without adequate protection. Also, data shall be processed in accordance with the data subject rights under the Act. The data subject has the right to be told that the data is being processed, to see the information that is being held about her and to correct the data if it is wrong. Also, data shall be held in a secure place, e.g., in locked filing cabinets or in secure IT databases and data shall be held and disposed of securely. Unauthorised access to records should be prevented.

Exceptions to data protection under the Directive of course exist and they apply in library settings. One of these exceptions relates to the investigation of crime and other important public policy objectives. Surveillance cameras can be installed in a library legally, after obtaining a license from each member state's Data Protection Authority and for the sole purpose of protecting the library's premises from theft, vandalism and other crimes. The group of national data protection authorities (called group of Article 29) specified in a 2004 opinion that the member states should evaluate surveillance systems so that an over-proliferation or image-acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms, which would make them massively identifiable in a number of public and private places; also, it noted that video surveillance techniques should be evaluated, in

order to prevent the development of software applications based both on facial recognition and forecasting of the imaged human behavior from leading inconsiderately to dynamic-preventive surveillance (Lim, 2010).

Surveillance in the European libraries, therefore, is strictly regulated and the right to read anonymously, the right to users' privacy, the right to informational determination (rights which have acquired constitutional dimension in many EU states) are carefully observed. In a library, data about readers should never be revealed to third parties (friends, parents, landlords, police e.tc.), either deliberately or accidentally (SCONUL, 2000). Simultaneously, CCTV is used for surveillance purposes in many libraries in Europe. For example, a CCTV system is used in all British libraries, comprising cameras installed in strategic locations (The British Library 2008); the Library Board considers that the use of CCTV in the library is a necessary, proportionate and suitable tool to help reduce crime, protect staff and the public and to assist with maintaining the security of the Library's assets (The British Library, 2008). When third parties request access to CCTV personal data, the library's system's manager is responsible to verify the legitimacy and accuracy of the request. The police, statutory authorities with the powers to prosecute, solicitors, plaintiffs in civil proceedings, accused persons or defendants in criminal proceedings are amongst the parties who can request access to CCTV personal data in a library and this access depends upon showing adequate grounds for disclosure of this data (providing evidence in criminal procedures or in civil proceedings or tribunals, prevention of crime, investigation or detection of crime, identification of witnesses) (The British Library, 2008).

3. The US approach: foundations, the PATRIOT ACT and library surveillance

Privacy protection in the US is different from the European regime. The US has opted for a piecemeal approach, otherwise called a 'sectoral' approach: the American lawmaker preferred to regulate the protection of privacy in specific sectors, 'step-by-step', and not implementing a rule applicable in every domain and situation. We could also note that the American lawmaker has mostly regulated *after* a privacy violation signaled the need to regulate: for example, the Video Privacy Protection Act of 1988 (Public Law 100-618) was a legislative reaction to the revelation that Judge Robert Bork had rented adult videos from a video store and this information was later on, when he applied for office with the Supreme Court, conveniently publicized at that time to defeat his nomination (Williams, 2012).

On the other hand, the right to privacy, nowhere to appear as such in the American Constitution, has gained constitutional dimension starting in 1965 with *Gris-*

wold v. Connecticut (1965) and again, in 1973, with *Roe v. Wade* (1973). States like California have incorporated a right to privacy in their own constitutions.

In the private law field, the four privacy torts recognized by the common law (appropriation of name or likeness, intrusion of solitude and seclusion, public disclosure of private facts, false light) usually occupy a small part of a tort law handbook (Glannon, 2010). Scholars and judges do not seem to give any particular weight to such torts of privacy violations (Prosser et al., 2010). A possible explanation for this attitude could be that under American law in general, freedom of speech is considered as one of the most important tenets of the system and strict/wide privacy protection of a citizen's informational, at least, determination would not be in line with this, as could be supported, supremacy.

Under the FBI Library Awareness Program, the FBI attempted to engage American librarians to spy on their patrons and report people who seem like they belong to a country 'hostile' to the United States (Foerstel, 1991). Almost twenty years later, in a study by CILIP in 2008, it was also noted that librarians were asked to report what a Muslin patron was reading (CILIP, 2008).

In the US, ever since the adoption of the PATRIOT ACT in 2001, surveillance in the American libraries has been formally instituted. The PATRIOT ACT (Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001) came as a respose to the terrorist attacks in the States of September 9/11, 2001.

Under sections 215 and 216 of the PATRIOT ACT, the FBI can have access and seize any library tangible thing (records, books, documents e.tc.) that could be useful to an investigation of terrorist or intelligence activities, tap library computers and obtain access to all users' internet searches and emails without a warrant. Key provisions of Section 215 include allowing the FBI to apply for warrants from the Foreign Intelligence Surveillance Act Court (FISC) to retrieve library usage records to assist in terrorism and intelligence investigations (Reid 2009). The FBI is not obliged to prove probable cause, only state that it has "reasonable grounds" to suspect that library records are related to an investigation. FISC search warrants override state and local privacy laws and they contain a "gag order" prohibiting a library from notifying users under suspicion, the press, or anyone else that an investigation is underway. A 2009 report from the US Justice Department to Congress states that only one of 2.000 FBI applications for a warrant in 2008 alone was rejected (Zetter, 2009). This means, necessarily, that appropriate oversight of the granting of these warrants cannot be proven with any certainty. Section 505 also, of the PATRIOT ACT authorizes the FBI to ask for a National Security Letter, by which a library is obliged to grant access to usage records.

American courts have denied the constitutionality of these sections. For example, in *Doe v. Holder* (2010), a lower court ruled that the Natioal Security Letter upon an internet service provider, under the PATRIOT ACT violated the First Amendment. In *Library Connection v. Gonzales* (ACLU 2006), a federal court similarly held that a National Security Letter filed with a library consortium also violated the First Amendment of the American Constitution). However, it is evident that the strong opposition of the American Library Association, the American Civil Liberties Union and other orgnizations (Ramasastry, 2006) should not only help in the judicial resolution of these disputes, but aim at the general clarification of the legality, or not, of the PATRIOT ACT surveillance of libraries sections 215 and 216. Twice so far the legislation surpassed the sunset provisions it included (in 2005 and in 2009) despite severe efforts to to contrary (Reid 2009).

For more than a decade, all efforts of the American Library Association and the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (Reid, 2009) amongst other organizations, to block the application of the law and annul it have constantly failed. The discussion will be repeated in 2015, when the new sunset date for these sections is set. In the meantime, resistance to PATRIOT ACT by American libraries has reached the point where, for example, the King County Library System decided to remove all security cameras, after the police demanded, without furnishing a court order, the tape of a video from a crime in the parking lot outside the library filmed by the cameras, (Gilmore, 2011).

In this case, a homeless suspect had assaulted an elderly library patron in the library's parking lot and was quickly arrested after the police took hold of the taped event by the library camera (Nichols, 2011). The police, though, had to argue with library officials who had refused to surrender the tape without a warrant (Wilkinson, 2011). Actually, cameras were installed in all libraries of the King County, beginning in 2006 and the yearly cost to maintain them comes up to 30.000 dollars. Surveillance cameras were installed both inside and outside the buildings, after specific requests by the librarians themselves, who faced petty crimes, vandalism and graffiti in and out of the libraries. The decision was justified as protection of intellectual freedom as too important to merit a possible adversarial relationship with the police every time the police would ask the tapes for crime detection and prevention (Gilmore, 2011). But it was certainly not met with universal acceptance (Nichols, 2011). The advice of the American Library Association on the issue of cameras and police investigation is rather straightforward: "when a library considers installing surveillance equipment, the administrative necessity of doing so must be weighed against the fact that most of the activity being recorded is innocent and harmless ... and if the library decides surveillance is necessary, it is essential for the library to develop and enforce strong

policies protecting patron privacy and confidentiality appropriate to managing the equipment, including routine destruction of the tapes in the briefest amount of time possible, or as soon as permitted by law" (ALA undated).

In any case, intensified federal monitoring of public libraries is, as it seems, in fact taking place across the US. A Department of Justice report on surveillance activities for 2010 revealed a dramatic increase in surveillance of Americans between 2009 and 2010, whereas the PATRIOT ACT section 215 orders were four times more than those ones in 2009 and the nuber of people surveilled with National Security Letters more than double in comparison to 2009 as the FBI requested 24,287 National Security Letters on 14,212 people (Zaluski, 2011).

4. A survey in Greek academic libraries on surveillance

The questionnaire was divided into two parts. The first part addressed the extent to which libraries opt for creating a page or profile in a social networking site, for what reasons, and whether any problems were encountered in using it.

Out of 40 libraries, 18 replied. Among these, only five answered that they actually have a page/profile in a social networking site, i.e. Facebook. One library mentioned that they would promptly create a Facebook page and a Twitter profile page. One more stated that it was their intention to create a profile on a social networking site. One library created a Facebook page only for a specific purpose.

All libraries noted that their users considered the creation of such a website positively. The main reasons for the creation of a website included: firstly, interactive communication with library users; secondly, library presentation in a popular social network; and thirdly, facilitation of communicating with librarians and other libraries. The assessment of whether such targets were actually attained was rather moderate. Five libraries replied 'fairly'. One said 'a little'. There were no replies on any malicious comments made by Facebook page users.

Subsequently the survey dealt with whether libraries permit access to social networking sites through their PCs and whether they inform their users on the benefits and risks related to the use thereof. According to the replies given, 4/5 of the libraries permit access to social networking sites through the PCs of both their personnel and their users. Two of them replied that they did not permit access of students; one explained that they did not have sufficient equipment to serve all users. In one case, users reacted; in the other, they did not. Another library replied that they did not permit access of neither their personnel nor their users because such pages were considered to be unsuitable for an academic facility and that they were used too much by their personnel. That is why only limited reac-

tions were noted by their personnel. One library permits access of its personnel, whereas some reactions were expressed by its users.

Even though libraries do permit access of their users (12 out of 18), most of them did not consider it necessary to provide information on the operation of such networks (e.g. risks related to their privacy protection or benefits arising from their use). Only 5 out of 18 libraries replied that they considered such information to be necessary.

Unfortunately, from so small a sample, no safe conclusions can be drawn. Nevertheless, on the basis of the results mentioned above, we could say that approximately 1/3 of the survey-participating libraries already have or are about to have an account in a social networking site. The second conclusion is that most libraries permit access to social networking sites through their open access PCs, but they do not provide any relevant information on the potential of holding that kind of information or the risks related to their users' privacy.

The second part involved whether libraries opt for security cameras and closed circuit TVs or anti-theft devices or RFID systems, why and whether they have encountered any problems from their usage.

Out of forty (40) libraries, eighteen (18) answered, eleven (11) of which answered that they have anti-theft devices in place. Three (3) answered that they have anti-theft devices and RFID systems. Two (2) answered that they have anti-theft devices and security cameras and two (2) that they do not have any protection system at all. When asked why that system was the most appropriate, only libraries with anti-theft devices and security cameras answered that they best help them to protect their premises.

Only five (5) answered the question on how long their security systems have been installed. They reported more than five years. Other questions involved only two (2) libraries the directors of which have chosen security cameras as their means of protection. Specifically: at which points of their library were the cameras installed? How were their readers informed on the use of such systems? Who administers the information collected by the cameras? Whether they had any reactions from users regarding the use of cameras and how they dealt with them. Whether there were any instances when they decommissioned the systems and what were the reasons that led them to such a decision. Finally, to what extent did cameras' installation attained their original targets?

Unfortunately, such a small sample may not easily lead to the drawing of safe conclusions. Nevertheless, based on the findings mentioned above, we can safely say that the majority of the libraries questioned have protection systems in place at a rate of 90%.

5. Conclusions

Detailed principles and laws regulate surveillance in academic libraries in Greece. The Data Protection Directive fully applies to data processed by libraries, data on book lending and data from surveillance cameras as well. Academic libraries in Greece also have started to participate in social networking sites, receiving a positive reaction from library users. Although risks of participation in social networking sites are widely known, libraries did not select to notify users on these dangers. A fair number of libraries have installed anti-theft devices, most probably for more than five years. The sample unfortunately was small and does not allow for absolutely secure conclusions. From the answers, overall, to the survey and the comments we received, we can conclude that, although Greek librarians do see safety as a library policy goal and assume a positive attitude towards surveillance systems, they generally treasure the protection of users' privacy, under the laws and their ethical commands. Also, they do not stress the importance of surveillance in academic settings in comparison to the dedication of librarians to the values of intellectual freedom and freedom of information. Greek libraries, lastly, do promote the use of social networking services for the benefits of their users.

References

ALA Code of Ethics, 1939, available at http://www.ala.org

Alford W., (1997), To steal a book is an elegant offense: intellectual property law in Chinese civilization, Stanford University Press

American Civil Liberties Union, Librarians' NSL Challenge, May 26, 2006 available at http://www.aclu.org/national-security/librarians-nsl-challenge

Burrows, J. and Cooper, D., (1992), Theft and loss from UK libraries: a national survey. Home Office Police Research Group, London: HMSO

Byrne A., (2000), Promoting intellectual freedom globally through libraries: the role of IFLA, Libri vol. 50, pp. 57-65

Center for Cognitive Liberty and Ethics, The readers' rights project, http://www.cognitiveliberty.org/readers_rights/stmnt.htm (undated)

CILIP Survey on Police Surveillance and Libraries, (2008), available in http://www.cilip.org.uk

Doe v. Gonzales, 386 F. Supp. 2d 66 2005 US Dist. LEXIS 1943

Doe v. Holder, S.D.N.Y. 04 Civ. 2614, 2010

European Court of Human Rights (2001), *Bodil Lindqvist* Case C 101-01

Foerstel H., (1991), Surveillance in the stacks: The FBI's Library Awareness Program (Contributions in Political Science), Greenwood Press

Foster C., (1996), Determining losses in academic libraries and the benefits of theft detection systems. Journal of Librarianship and Information Science, 28(2): 93–103

Fromholz J., (2000), The European Union Data Privacy Directive, 15 Berkeley Tech. L.J. 471, 472

Gilmore S., (2011), King County Library System is removing its security cameras, The Seattle Times, May 24, 2011, available at http://seattletimes.nwsource.com/html/localnews/2015138444_library25m.html

Glannon J., (2010), The law of torts, examples and explanations, 4th ed., Aspen Publishers

Griswold v. Connecticut, 381 U.S. 479, 1965

Hart S., (undated), Vandalism in libraries: causes, common occurrences and prevention strategies. Available at http://capping.slis.ualberta.Ca/Cap05/Sandy/capping.htm

Hauptman R., (1982), Five assaults on our integrity, in Ethics and Reference Service, Katz B. & Farley R. (eds)

Holleman P., (1983), Report on Surveillance Issues in Community College Libraries Community and Junior College Libraries, 1:4, pp. 49-55

Johnson, E.S., (1981), Research methods in criminology and criminal justice, Englewood Cliffs: Prentice Hall

Librarian's Code of Ethics (Greek), available in http://www.eebep.gr/files/doc_ethics/pdf

Lim L., (2010), The legal framework of video surveillance in Europe, in Citizens, Cities and Urban surveillance, Towards a democratic and responsible use of CCTV, European Forum for Urban Security

Lincoln, A.J., (1989), Vandalism: causes, consequence and prevention, Library and Archival Security 9:3/4: 37- 61

Nichols R., (2011), Officials urge library to reconsider removal of surveillance cameras, available at http://www.waterlandblog.com/2011/05/20/officials-urge-library-system-to-reconsider-removal-of-surveillance-cameras/

Prosser W. et al., (2010), Cases and Materials on Torts, 12th ed., Univeristy Casebook Series, Foundation Press

Ramana Y., (2007), Security in libraries need surveillance and biometrics, 5th International CALIBER, Panjab University, paper available at http://www.inf.libnet.ac.in/dxml/bitstream/handle/1944/1927/498-507.pdf

Reid M., (2009), The PATRIOT ACT and academic libraries, an overview, College & Research Libraries News, 646-650

Roe v. Wade, 410 U.S. 113 (1973)

SCONIL, Data protection issues: checklists for libraries, http://www.sconul.ac.uk/about_sconul/groups/access/tf_access/papers/dpa_checklist.doc

Stanley v. Georgia, 394 U.S. 557 (1969)

Stuges P. et al. (2003), User privacy in the digital library environment: an investigation of policies and preparedness, Library Management 24 (1/2) pp. 44-50

The British Library (2008), Code of Practice for the Operation of Closed Circuit Television System

Viola de Azevedo Cunha M. (2012), Review of the Data Protection Directive: is there need (and room) for a new concept for personal data? In Gutwirth S., Leenes R., De Hert P. & Poullet Y., eds., European Data Protection: in good health? Springer

Wilkinson E., (2011), King county libraries remove security cameras, The Seattle Times, May 13, 2011, available at http://www.king5.com/news/cities/seattle/King-County-libraries-remove-security-cameras-122476239.html

Williams G., (2012), The Video Privacy Protection Act – Winding up, not down, Government politics and privacy, February 6, 2012, available at http://sixestate.com/the-video-privacy-protection-act-winding-up-not-down/

Zalusky P., (2011), ALA Council continues opposition to use of Section 215 of Patriot Act and use of National Security Letters to violate reader privacy, available at http://www.americanlibrariesmagazine.org/print/7949

Zetter K., (2009), FBI use of PATRIOT ACT increased dramatically in 2008, available at http://www.wired.com/threatlevel/2009/05/fbi-use-of-patriot-act-increased-dramatically-in-2008