**PRIVACY IN THE “LIBRARY WITHOUT WALLS”:
LIBRARY PRACTICE IN AN AGE OF DIGITAL CONTENT**

Reply to:

Michael Khoo, Department of Communication, 270 UCB

University of Colorado, Boulder CO 80309-0270

michael.khoo@colorado.edu

INTRODUCTION

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.

Warren and Brandeis, 1890:193

The development of electronic computer and communication technologies has radically impacted library practice. Until recently, library holdings such as books, journals, newspapers, magazines, audio- and video-cassettes, and compact disks have traditionally been used by one person at a time. When made available in digital forms, however, these holdings can be accessible to multiple subscribers, in multiple places, at multiple times.

This emerging “library without walls” is often described as existing in a space free from the spatial and temporal constraints of bricks and mortar, a space in which patrons (provided they have computers and modems) can search catalogs and access electronic files without having physically to walk through a library’s doors. While offering advantages, these “libraries without walls” also raise a number of issues regarding the relationship between libraries and their patrons. This paper examines one of these issues, the implications for established norms of library patron privacy. In examining this issue, I will make the argument that new digital content technologies are throwing into question taken-for-granted definitions of privacy and that, unlike legal definitions of privacy that apply to people or property, the notion of what privacy means in relation to the provision of online content remains contested. The discussion will be structured around a case study, a review of the experience of the author with netLibrary, a digital content provider for the University of Colorado.

PRIVACY

The definition of privacy is temporally and culturally contingent (Moore 1998). In the United States, privacy rights are found not in the Constitution, the purpose of which is to set limits on government power, but in the Bill of Rights, the purpose of which is to limit the extent to which government can impose on individuals. While a number of legal definitions of privacy have been accumulated over time, no absolute, legal concept of privacy exists that can guide us as to whether a particular situation might or might not be construed as a violation of privacy.

Smith (2000) argues that any time we place private information into the public domain, it can potentially be intercepted. He therefore defines privacy as “[T]he desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves” (p. 6). He traces the manifestation of this desire through American history and through the development of various information transmission technologies such as postal services, the telegraph, and the telephone.

While these technologies transmitted information, they could also monitor it. Although there were legal (and moral) obligations upon the operators of information technologies to treat the channels they provided as private connections between sender and recipient, there were any number of occasions when these obligations were over-ridden or ignored by private and government agencies. Postal services, for example, benefited from the development of postage stamps and postage boxes (these made the act of posting a letter anonymous), as well as gummed envelopes (which made the contents of a letter anonymous), but letters remained susceptible to interception. Telegraph and telephone messages could be intercepted by the operators listening in on lines. Concerns over the integrity of these technologies quickly led to the development of cryptographic techniques by which messages could be encoded (see Standage 1998 for an account of this process with the telegraph).

The end of the nineteenth and the beginning of the twentieth centuries saw the introduction of a number of other new technologies—such as the camera and the high-speed printing press—that further changed

commonly defined notions of privacy. According to Lester (2001), “For the first time, spontaneous, unposed pictures could be taken, quickly printed in newspapers and books, and distributed widely, all without the subjects’ consent.” This unsettling possibility provoked an 1890 article by Samuel D. Warren and the future Supreme Court justice Louis D. Brandeis that is worth quoting at length here; it is surprising how apt their general argument is for conditions a century later. Writing against the contemporary newspaper practice of printing photographs of and unverified stories on individuals, the authors begin by stating,

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property . . . Later, there came a recognition of man’s spiritual nature, of his feelings and his intellect . . . now the right to life has come to mean the right to enjoy life,—the right to be let alone.

The fourth paragraph reads in part:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right “to be let alone.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons . . . [and] the evil of invasion of privacy by the newspapers.

The fifth paragraph reads in part:

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

(Warren and Brandeis, 1890:193)[\[1\]](#)

Warren’s and Brandeis’s article “broadened the legal conception of privacy to include not only the tangible but also the intangible realm” (Lester 2001). Definitions of privacy previously attached to home and personal property, fixed and specific points in society, were starting to become attached to the individual as he or she moved through society.

This analysis of the impact of new technologies on conceptions of personal privacy is instructive for understanding how computer and communication technologies are again challenging established definitions of privacy (Stefik 1997:197). One good example of an area where there is confusion surrounding the definition of privacy is in the debate surrounding the use of “cookies.” Cookies as they were originally developed were tools that helped web sites move beyond the function of providing information and towards the function of providing a service (see Appendix A for more detailed information). Web advertisers realised, however, that cookies could also be used to accumulate information about a user’s interactions with a site. For instance, advertising companies can place cookies on your hard drive if you visit a site on which they have placed an advertisement. If you then visit other sites that are monitored by the same company that originally set the first cookie, then the cookie that is already placed on your hard drive will let the advertising company know that you have also visited this second site and, often, a third and fourth site, and so on. In this way, correlative data collection can occur across a number of sites. This second use of cookies was not related to the desire to add functionality to a web site.

Although this use of cookies is not illegal and can be defeated by altering the user’s browser preferences (see Appendix A), it has generated some controversy. Cookie critics see it as an intrusion upon the privacy of the person upon whose hard drive cookies are placed, particularly in the case of those that provide details of a web user’s surfing patterns across a number of sites.[\[2\]](#) They point out that there is usually no way to tell, short of viewing web site HTML code and then figuring out where the advertisements originated from,

whether one advertising content provider might be collating all the little bits of personal information that the user supplied at all the separate and apparently unconnected web sites he/she visited.

I will illustrate these concerns with a “bricks-and-mortar” example. Suppose that in your local town, there is a video store. To become a member and rent videos, you have to fill out a form with your name, address, and telephone number. To rent DVDs, you have to leave a credit card number as a deposit. To enter promotional sweepstakes, you have to divulge some of your consumption habits (the model and year of the car you drive, how much you spent on your last vacation, and so on). On each form you fill in, there is some fine print that appears to guarantee that the information you provide will be kept private and confidential.

One day, however, somebody realises that the video company, instead of reinvesting its profits in new videos, has instead been spending them on a flashy company headquarters with a free cappuccino bar, pinball machines, a massage therapy room, and a climbing wall. Further, it turns out that the company has failed to anticipate new developments in the video rental market and that their expensive web-site, eVideos.com (“The new way to rent videos”), is poorly designed and losing a lot of money. Investors lose confidence, there is a cash-flow problem, and the company goes belly-up. As ex-rental videos are not worth that much, the company seems to possess little in the way of liquifiable assets apart from, that is, a large database of personal information that they have collected from customers like you, information they announce they will sell off to the highest bidder.

This video store is somewhat like a company providing advertising content to different web sites. Each transaction with the video store (renting a video, entering sweepstakes, and so on) can be compared to visits to different web sites. While each transaction/visit involves your providing only a small piece of personal information, it is possible for one company to collate personal information about you—much as the video store starts to build a profile of your renting habits, income, and family—and to treat this data as an asset. For instance, in fall 2000, Toysmart, an online toy retailer partly owned by the Walt Disney Corporation, filed for Chapter 11 bankruptcy.^[3] It then emerged that Toysmart was considering selling its database of customer information to the highest “trustworthy” bidder. The Federal Trade Commission, opposing this action by Toysmart, for a while considered blocking the sale before finally allowing it to proceed under restricted conditions.^[4] Notably, these conditions did not include any obligation on the part of Toysmart’s creditors to either inform or obtain permission from Toysmart’s customers. In the end, the affair turned out to be a storm in a tea cup. The data failed to provoke the anticipated bidding frenzy: the highest offer had come from Disney itself (\$50,000) with the next highest offer being \$15,000 from a market-research firm in Maine.^[5] Nevertheless, Toysmart’s strategy was only one of a number of announcements by dot-coms (including boo.com and craftshop.com) that were similarly going belly-up.^[6]

Stories such as these inform many discussions of online privacy. The terms of the debate are, however, plastic and mobile. For instance, while a number of reports have found that online users are suspicious of cookies and the harvesting of user information,^[7] users at the same time display ambiguous attitudes about how they might be regulated. This lack of agreement on the desirability of cookies can be attributed at least partly to the effect that new technologies have on the definition of social ideals often thought to be stable and immutable—in this case, notions of privacy.

A CASE STUDY: netLibrary

The ambivalent status of privacy in cyberspace is illustrated in the following case study involving netLibrary’s use of cookies on its web site. The somewhat convoluted nature of the example, including the debate over what (if anything) netLibrary was doing wrong, is a good illustration of the more generally contested nature of the definition of privacy in cyberspace.

netLibrary, founded in 1998, is located in Boulder, Colorado. On its web site, netLibrary explains its mission as “combining the time-honored traditions of the library system with electronic publishing” in order to offer “an easy-to-use information and retrieval system for accessing the full text of reference, scholarly, and professional books.”^[8] After its beginning with an emphasis on academic texts,^[9] netLibrary acquired in May 1999 \$25 million in venture capital^[10] and subsequently moved into 100,000 square foot offices^[11] before securing a further \$72 million of funding in October 1999. It has expanded its purview to include

business oriented services such as custom collections development. Along the way, it has acquired from publishers the rights to a number of e-books and signed content-provision agreements with bricks-and-mortar libraries. (The netLibrary site has links to a series of netLibrary press releases that detail these activities[12] as well as to press articles written about netLibrary up until the end of 2000.[13])

The University of Colorado has access to a collection of e-books purchased from netLibrary, and a class I was taking recommended readings that were available in netLibrary. In October 2000, while working at home, I became frustrated with the slow download of netLibrary pages. By reading the download status bar at the bottom of the browser, I realised that each netLibrary page, especially the front page, consisted of a large number of buttons and other images that were being downloaded from different servers.[14] According to the status bar, the images on the netLibrary site were being served not by netLibrary but by another company, Akamai.[15]

Akamai serves a lot of images to many different web sites. Although these images often include advertisements targeted at personal profiles of the web surfer determined through the use of cookies, netLibrary's site contains no advertisements. One explanation for netLibrary's use of Akamai is that netLibrary envisages rapid growth in its user base and that, rather than constantly reconfiguring its own servers to meet demand, it has outsourced image serving to Akamai, who every so often sends them a bill for providing this service. As Akamai is a specialist in image serving, it provides a convenient scalable server solution for netLibrary's projected growth.

The netLibrary home page calls for a number of these Akamai images; and as I loaded netLibrary's home page, the name Akamai appeared time and time again in the status bar of my web browser. One particular line in the status bar, however, caught my attention. It was a one-time, brief reference to a company called focalink.com. If my home connection had not been so slow, I probably would not have noticed it.

The appearance of focalink.com in my browser status bar meant that the HTML script of the netLibrary home page was asking my web browser to retrieve an image from a third source (besides netLibrary and Akamai), a source called focalink.com. Wondering who focalink.com might be and what netLibrary might be using them for, I used my browser menu bar to view the HTML source code of the netLibrary front page. I then saved the code as a text file. Reading through the code, I found that netLibrary was serving one image—a Graphic Image File, or GIF—from focalink.com. Interestingly, the HTML code that achieved this was placed between the </BODY> and </HTML> tags at the end of the document and so the image, when fetched from the focalink server, would not appear on the netLibrary home page. Even if it had, it probably would not have been noticeable anyway; the image was only 1 pixel by 1 pixel in size, that is, smaller than a period in browser displays.

The particular code that fetched the image from focalink read as follows:

```
</BODY>
```

```
<IMG SRC="https://s2.focalink.com/SmartBanner/nph-graphic?20791.1-972861055866" height=1 width=1>
```

```
</HTML>
```

In this code, the letters IMG tell the browser to fetch an image. The subsequent letters, SRC, are known in HTML as an attribute, a part of the HTML code that can have a value. The value of the attribute in this particular case is the subsequent string of letters and numbers within the quotation marks, which tells the browser where to fetch the image from, i.e, from a directory on the servers of focalink.com.

Following this, the words "height" and "width" are further attributes that tell the browser, after it has retrieved the image, what size to display the image on the screen. The values of both attributes are 1, meaning that the image will be displayed 1 pixel by 1 pixel in size, that is, the smallest possible size that a browser will render an image on anyone's computer screen.

This piece of HTML code is, in essence, a request from my browser to focalink.com to send back to my

browser a small, meaningless image that is too small to see and that is not displayed in the web page anyway. These tiny images are known by various names, including 1 pixel GIFs (because they are GIFs that are 1 pixel by 1 pixel in size) and also as web bugs. Why would netLibrary and/or focalink.com want to send a web bug to my computer? One answer is that by sending the request for the web bug, my browser was also telling focalink.com where my browser (hence my computer) was located. When my browser asked for the image, it also had to provide a return address for the image to be sent back to my computer; as noted above in the case of cookies, it is like a kind of caller ID from my computer that tells the focalink.com server where the request came from (my computer) so that it can send back a 1x1 pixel image. Thus, when I loaded the netLibrary home page, the following things happened:

1. My browser received the HTML code for the page from netLibrary and started to display it on the screen;
2. The HTML code told my browser to fetch a series of images from Akamai—navigation buttons and so on—that were displayed in my browser window;
3. The HTML code told my browser to ask focalink.com to send a small, almost invisible image;
4. focalink.com sent the image back to my computer, and it was not displayed in my browser window.

After I had loaded the netLibrary home page, therefore, not only netLibrary and Akamai but also focalink.com knew where I was or at least where my computer was. But here is the interesting part:

5. Along with the image, focalink.com also sent back a cookie.

How did I know this? Well, being curious, I decided to view again the source code for the netLibrary home page. At the bottom, it now read:

```
</BODY>

<Script language="JavaScript">

var now = new Date();

document.write('<IMG SRC="https://s2.focalink.com/SmartBanner/nph-graphic?20791.1-' + now.getTime()
+ '" height=1 width=1>');

</Script>

<noscript>

<IMG SRC="https://s2.focalink.com/SmartBanner/nph-graphic?20791.1 Alt="Invisible
Dot" height=1 width=1>

</noscript>

</HTML>
```

The netLibrary home page had now downloaded from focalink.com a small piece of a programming language known as javascript. This was used to set a cookie on my hard drive that would answer to focalink.com. In other words, if I loaded any other site that contained advertising content served by focalink.com, focalink.com could (although not necessarily would) know that I had also been using netLibrary.

One question I found myself asking was “Who is focalink.com?” This was quite easy to answer. I typed the URL <http://www.focalink.com> into my browser and was swiftly redirected to the site of [adknowledge.com](#).^[16] Adknowledge is, in turn, a division of Engage,^[17] itself owned by a corporation called CMGI.^[18] Adknowledge is therefore part of a conglomerate of corporations, some of which specialise in generating consumer profiles from data derived from online ad campaigns, presumably collected through cookies placed on users’ hard drives.

I thought it might be interesting to see what other sites were making use of Adknowledge's services. A method for carrying out such a search has been outlined by Richard Smith of the Privacy Foundation (<http://www.privacyfoundation.org/>). The search method is based on the fact that the Altavista search engine can be asked to look for code strings within the HTML of a page. In this case, one can search for the address strings in IMG (image) tags served by Adknowledge. Smith recommends in the case of Adknowledge that the Altavista search string be as follows:

image:ads01.focalink.com/SmartBanner.

Such a search reveals that many sites make use of Adknowledge's services. Adknowledge appears to maintain a number of image servers, including ads01.focalink.com, ads02.focalink.com, etc. Although it is not clear whether all servers represented by the address ads+number.focalink.com are being used, a good many are:

Ads01.focalink.com/SmartBanner	70 results
Ads02.focalink.com/SmartBanner	6652 results
Ads03.focalink.com/SmartBanner	64 results
Ads04.focalink.com/SmartBanner	140 results.

These results indicate the number of pages that receive advertisements from an Adknowledge server. I found twenty-five Adknowledge servers, some serving thousands of different advertising images. In other words, Engage-Adknowledge is monitoring thousands of other web sites. It is thus possible (although I have no way of knowing whether or not this actually occurred) that the cookie that Adknowledge placed on my hard drive from the netLibrary home page would let Adknowledge know when I accessed any of these other sites. Adknowledge was thus able—possibly—to correlate my behaviour as a netLibrary registered subscriber to my visits to all other sites that are monitored by Adknowledge.

There is nothing unusual in Adknowledge placing cookies on users' hard drives. Paying a visit to any commercial sites will result in a number of such cookies being set. At the time when the data was being collected on the netLibrary site, however, netLibrary appeared to be promising its users, among whom were a number of public and university libraries, that it would *not* collect such information for third-party advertisers from netLibrary users without first informing its users.

This promise was made in netLibrary's privacy policy,^[19] which seems to assure users that netLibrary would not allow any personal information collected on the netLibrary site to be divulged to third parties. But what was netLibrary's privacy policy actually saying? It begins,

netLibrary, Inc. is committed to protecting user privacy online. We believe that strong electronic privacy is crucial for the ongoing success of the Internet. We also believe it is critical for us to adhere to the American Library Association's Code of Ethics. At netLibrary, we pledge to give you as much control as possible over your personal information. We will not disclose individually-identifiable information about you to any third party without your consent.

A key phrase here, both for netLibrary and the user, is "individually-identifiable information." Individually-identifiable information includes information that can be directly linked to individual users. In netLibrary's definition, cookies furnish only non-identifiable information, and netLibrary's Privacy Policy thus allows netLibrary to disclose non-personally identifiable information to third parties. The policy does not recognize, however, that cookie-derived, non-individually-identifiable information gathered from the netLibrary site by Adknowledge could be correlated with individually-identifiable information collected from other sites monitored by Adknowledge.

Note that netLibrary states that it "is critical for us to adhere to the American Library Association's Code of Ethics." A relevant clause in the ALA Code of Ethics states, however,

We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired *or transmitted*. [Emphasis added]

By not making a distinction between “individually-identifiable information” and other types of data-gathering, the ALA’s Code of Ethics would thus appear to offer more protection than netLibrary’s privacy policy.

netLibrary also states that it is “a licensee of the TRUSTe Privacy Program.” TRUSTe, a non-profit privacy organisation established in 1997 (see Appendix B), feels that online customers should be informed about whatever information is collected from them in interactions and that they will be attracted to sites that disclose this information. An important part of the TRUSTe programme is the “Trustmark,” a web site logo “awarded only to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures” (for details of the standards of privacy that TRUSTe requires for a site to receive the Trustmark, see Appendix B). TRUSTe’s Privacy Glossary draws less of a distinction between personally- and non-personally-identifiable information than does netLibrary’s Privacy Policy. TRUSTe gives the following definitions of various forms of collectable information:

Personally identifiable information.

Information that can be traced back to an individual user, e.g., your name, postal address, or e-mail address. Personal user preferences tracked by a Web site via a “cookie” (see definition above) are also considered personally identifiable when linked to other personally identifiable information provided by you online.

Aggregate information.

Information that may be collected by a Web site but is not personally identifiable to you. Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as none of these fields is linked to a user’s personal information, the data is considered aggregate.

Cookie.

A block of text placed in a file on your computer’s hard drive by a Web site you have visited. A cookie is used to identify you the next time you access the site. Cookies cannot identify an individual user specifically unless the cookie data is attached to personally identifiable information collected some other way, such as via an online registration form.

Although TRUSTe makes the distinction between non-personally identifiable and aggregate information that we find in the netLibrary Privacy Policy, TRUSTe recognises that information from cookies can be correlated with personally identifiable information obtained elsewhere on the Internet. TRUSTe errs, therefore, on the side of caution with regard to cookies and aggregate information, noting that it is possible for cookie technology to aggregate information in sufficient amounts for it to become personal. In a “Self Assessment Sheet” attached to their “Model License Agreement (v. 6.0),”^[20] the potential TRUSTe license applicant is asked the following questions:

II. Who is Collecting Information?

C. Third Party Ad Servers

- a. Do banner ads appear on the site? Yes No
- b. Does the site have a relationship with a third party ad server? Yes No
- c. If yes, explain who serves ad strings on the web site (e.g. Flycast, Doubleclick).

It seems, therefore, that, as a TRUSTe licensee, netLibrary should have at least made it clear that Adknowledge cookies were being placed on netLibrary users’ hard drives. Whether or not these cookies actually led to the aggregation of personal information is not strictly relevant. By using the TRUSTe Trustmark, netLibrary should have informed their users of the following:

- a) that they were serving images from a third-party server;
- b) that that third-party server was then also setting cookies on the user’s hard drive; and

c) that these cookies were not functioning to “maintain state” during the user’s netLibrary experience (as is claimed in netLibrary’s privacy policy) but rather that they were involved in some form of measurement of the user’s behaviour.

Curious about the relationship between TRUSTe policy, TRUSTe practice, and the practices of netLibrary (a TRUSTe licensee), I e-mailed TRUSTe in November 2000 regarding TRUSTe’s policy towards web bugs. Within a couple of days, TRUSTe spokesperson David Steer (TRUSTe’s Director of Communications) replied, in part, as follows:

Clearly, one pixel GIFs (aka Web bugs) throw a new wrinkle in the privacy

conversation. At this point, TRUSTe is only beginning to examine their use and the implications to the legal agreement each Web site signs as a pre-requisite to joining our program. You may want to take a look at the research The Privacy Foundation is doing in this area—I believe its site is located at www.privacyfoundation.org.

Also in November, the web bug and the javascript that set the cookie answering to Adknowledge disappeared from netLibrary’s site. I contacted netLibrary to find out what had been going on, but the contact e-mail address provided in netLibrary’s Privacy Policy (privacy@netlibrary.org) did not appear to be the responsibility of any particular person in the organization and certainly not the responsibility of anyone who had read the privacy policy. My initial inquiries regarding netLibrary’s use of third-party cookies were dealt with by someone who assured me, without a trace of irony, that information about this practice was netLibrary’s private property and therefore none of my business. It was only after persistent e-mailing that I was able to reach someone at netLibrary—Paul Smith, netLibrary Executive Vice President—who was willing to address my concerns and who eventually arranged a meeting at netLibrary to discuss these issues in person.

Discussion

The disjuncture between netLibrary’s stated privacy policy towards its patrons and netLibrary’s actual practices (at least during the time I observed the Adknowledge web bug and cookie in fall 2000) opens an interesting space for a discussion of the impact of new technologies on the conceptualisation of privacy and how this relates to contemporary library practice. This discussion is important because the trust that the public places in libraries is predicated at least in part on the perception that libraries are open and (publicly) accountable institutions. In this section, it is argued that as libraries increasingly act as portals to a vast array of digital resources, both trust and accountability are becoming increasingly harder to locate, with potential detrimental effects for libraries.

If not illegal, netLibrary’s behaviour seemed, to this author at least, to be unethical. This was also the reaction of other people I presented the story to—including students in a computer science graduate seminar discussing online privacy and administrators at the University of Colorado’s Norlin Library—even if people were hard-pressed to define exactly what the unethical component of netLibrary’s behaviour was. Further, while some were concerned, others pointed out that similar monitoring behaviour is carried out by other organisations, such as supermarkets that issue loyalty cards. This difference of opinion regarding whether web bugs are or are not a problem is reflected in wider public debates on the same issue (see for instance a debate in the online discussion board *Slashdot* in January 2001 [21]).

In a meeting with Paul Smith and Roger Greene of netLibrary, the definition of online privacy seemed (to me) to be similarly ambivalent. For instance, I was told that netLibrary licenses e-books to both individuals and corporations and to public and university libraries and, thus, pursues appropriate marketing and revenue strategies for each sector. The use of third-party cookies was therefore presented as part of netLibrary’s overall financial strategy that public library users might encounter although presumably the promises of netLibrary’s Privacy Policy applied both to “traditional” and “commercial” subscribers. However, it must be remembered that both sectors are being sent to the *same* netLibrary home page. To make a comparison with “bricks-and-mortar” institutions, the netLibrary home page functions both as a large bookstore and as a public library. While, in the real world, both bookstores and public libraries can ask patrons to provide personal information in exchange for services (in the case of the bookstore to receive discounts and in the case of the public library to borrow books), in the real world it is also possible to tell when you are walking into a bookstore and when you are walking into a public library and to make some judgment as to whether or not

you wish to provide such information. In the case of the netLibrary home page, however, this distinction was not so clear.

Among both netLibrary users and netLibrary, there seemed, therefore, to be some lack of precision in the definitions of privacy being discussed. On the one hand, the netLibrary users I spoke with were worried that something was wrong with netLibrary's use of cookies but were hard-pressed to define exactly what this might be. On the other hand, netLibrary itself seemed to think that it was doing things correctly but was also interested in ways it could do them better. It was especially interested in understanding the varying perceptions of online privacy that it might encounter among various clients and in building trust among these clients. Were, for instance, users in the academy more likely to be concerned over third-party cookies than were private subscribers?

The unresolved nature of these concerns has relevance for libraries and librarians who have the opportunity to contribute to the debate and to the future definition of online privacy, especially in the case of libraries. Librarians already have a professional concern for patron privacy, as is evident in the International Federation of Library Associations and Institutions web site,[\[22\]](#) which archives a number of codes of ethics of library associations around the world (see Appendix C). A review of these codes of ethics, as well as those of the American[\[23\]](#) and British library associations,[\[24\]](#) reveals definitions of privacy and confidentiality that range from the duty of librarians to "[P]rotect the privacy and dignity of library users and staff" (Canadian Library Association) to far lengthier definitions (see for instance the provisions of the Japanese and Portuguese library associations).

While concerned with library patron privacy, none of these codes mentions the issues raised in this paper of the use of third-party cookies by external digital-content providers. While this might be attributed to the novelty of the problem, even where codes are being updated to take account of electronic communication technologies—as can be seen for instance in the range of online draft documents provided by the American Library Association's Office for Intellectual Freedom[\[25\]](#)—such cookies still do not appear to be mentioned. Thus, while the ALA/OIF's "Draft Principles for the Networked World" clearly articulates privacy principles that could apply to these cookies—

PRIVACY: The freedom to choose the degree to which personal information is monitored, collected, disclosed, and distributed.

Principles:

1. Privacy is a right of all people and must be protected in the networked world.
2. The rights of anonymity and privacy while retrieving and communicating information must be protected as an essential element of intellectual freedom.
3. The long-established principles of Fair Information Practices must be at the core of privacy policies in the networked world.
4. Users have the right to be fully informed about privacy policies and principles in the networked world.
5. Library patron confidentiality must be protected by law and policy[\[26\]](#)—

third-party cookies are not mentioned, perhaps because there seems to be an underlying assumption that these are principles that apply to libraries and not to the third-party vendors with whom they contract.

The debate regarding the nature and definition of online privacy is thus open and fluid and does not yet seem to have reached closure. While library associations worldwide may have policies that guarantee (or aspire to guarantee) the confidentiality of their own patron records, these policies can be less effective, or even ineffective, when the same patron uses that library's web site to access externally provided content to which that bricks-and-mortar library has a subscription. In the case of bricks-and-mortar libraries, it is assumed that user records will not be removed beyond the physical walls of the library, or indeed beyond the administrative space within which they are required. In the case of libraries with network connections to external content providers, however, the connections themselves ensure that any information provided by a user who clicks on a link to an external content provider may be transferred anywhere else on the Internet and for any purpose.

Lessig (1999) analyses this situation in terms of the relationship of “legal code” to “computer code.” Computer code, Lessig argues, challenges many areas of legal code; and to respond to these challenges, a re-structuring of both legal and computer code is called for. However, while this re-structuring should ideally be performed in the public sphere, much of it is currently being carried out piecemeal through political lobbying. Lessig argues that, consequently, we stand a real chance of losing rights in cyberspace that we take for granted in the real world.

In the case of privacy, Lessig casts the debate in terms of a distinction between monitoring and searching. The parts of your daily life that can be monitored consist of those parts that can be observed by others (for instance, walking down a street), while the searchable parts consist of the trail of artifacts—writings, voice mail, etc.—that you leave behind you. “What,” asks Lessig, “are the constraints in real space on others’ ability to monitor and search, and how do those constraints change as we move to cyberspace?” (143–144). One answer that he supplies is that cyberspace and digital technology have permitted the development of monitoring behaviour to the point where, as a practice, it becomes more akin to searching. The collection of data from many different points (for instance, with cookies) and the subsequent storing and correlation of that data can produce personal profiles that would be difficult to achieve through physical monitoring on the street but that might be achievable by searching someone’s room.

While in the realm of computer code, monitoring has become more like searching; in the realm of legal code, monitoring is still treated as monitoring, no matter how efficient it becomes. One of Lessig’s solutions to this problem is to advocate a strategy of notice and choice: “companies will inform consumers about how data will be used and not use it for any other purpose” (159).

Is a provision of such choice enough, however? Lessig sees such agreements as cumbersome; and as he suggests and as we have seen, unless the requirement is a legal one, there is nothing to prevent companies from adopting the quasi-legal standards of self-regulatory bodies that have no legal means of enforcement. Research into the adoption of complex technologies suggests that part of the problem here lies with the unfamiliar nature of new technologies. When people are faced with an unfamiliar technology that bears a resemblance to a familiar one, they can apply their understanding of the familiar technology to the unfamiliar one. While library patrons and staff often assume they know how on-line content provision works, if the model they hold of such content is couched more in terms of the bricks-and-mortar library with which they are familiar, they can transfer the trust they associate with bricks-and-mortar institutions onto online institutions, whether this trust is warranted or not. This trust is in turn open to potential abuse as unforeseen consequences of digital technologies make themselves apparent.

Research into the social adoption of complex technological artifacts suggests that one solution to this problem of misinterpretation lies in the use of “boundary objects” that can mediate the conceptual boundaries between old and new technologies, that function (for example) to explain old technologies in terms of new ones. Boundary objects can include institutional roles, journals, professional associations, and policy statements such as the codes of ethics of various library associations.^[27] Considered as boundary objects, these codes (for example) represent objects that can serve as foci of discussion. Revision of these codes could, therefore, serve as the first step towards discussions over the implications of the “library without walls” for library patrons. This should, however, only be the first step towards an informed and reasoned debate that would raise awareness both within and without the library community regarding the implications of the constant introduction of new technologies. While it might be objected that the public is not interested in these issues, it is argued here that this is only the case insofar as nothing untoward happens. What is at stake here is not “just” the public’s data but also the public’s perception of libraries as trustworthy public institutions. It would take only one (or several) well-publicised examples of identity abuse to undermine trust already damaged (in some eyes at least) by related public library/Internet-based debates of “filtering” versus “censoring” Internet content for their patrons. On a broader level, by bringing these debates into the open, librarians also have an opportunity to contribute to wider public

discourses concerning the relationships between new technologies, public freedoms, and civil society.

Conclusion

We can see how, over the years, notions of privacy have evolved along with technology. In Smith's history of privacy in the United States, privacy is a "moving target," subject to developments in social and cultural attitudes. Smith and Lessig both point out that it is periods of rapid technological change that throw definitions of privacy into relief and demand that they be discussed and negotiated.

In the context of libraries, I have argued that this issue is important for several reasons. Traditional "bricks and mortar" libraries, at least in the form of public libraries and state university libraries, have deserved reputations as impartial providers of informational resources for the public. Many provide other services that underline their role as community institutions, such as meeting places and notice boards, newspapers, Internet access, etc. (although in university libraries general public access to some of these services can be restricted). While libraries like these are generally trusted by the public, I have suggested that this trust is under potential threat. Expanding into an area that lacks widespread understanding, let alone legislation based on such understanding, providers of digital content can engage in practices that would be deemed inappropriate in many bricks-and-mortar libraries. The very novelty of digital content affords, however, opportunities for concerned librarians to discuss its implications and to draw up guidelines and best practices for working in such arenas (for instance, by expanding the code of ethics to specifically embrace digital technology and by pushing wider and more general discussion of these concerns). Such an opportunity requires, however, an informed historical, social, and technological understanding and discussion of the relevant issues.

Epilogue

In October 2001 and after raising \$109 million in three years, netLibrary sought Chapter 11 bankruptcy.[28] NetLibrary's assets are to be acquired and administrated by OCLC.[29] As of the time of writing (March 2002), netLibrary's bankruptcy appears to be part of a wider context of lean times for the e-book industry with a number of ventures also going under.[30]

Acknowledgements

Many thanks to Gabe Johnson (Department of Computer Science, University of Colorado) for interpreting and commenting on the Javascript. Also, my grateful thanks to Paul Smith (netLibrary) and Roger Greene (Metatext) for finding the time to arrange a personal meeting to address the issues raised in this paper.

References

Agre, Philip, and Marc Rotenberg (eds). 1997. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press.

American Library Association. 2000. *History of the Code of Ethics*.

<http://www.ala.org/alaorg/oif/historyofcode.html> (viewed November 2001)

Cheskin Research. 2000. *Trust in the Wired Americas*. Redwood Shores, CA: Cheskin Research.

<http://www.cheskin.com/think/studies/trust2.html> (viewed November 2001)

Clarke, Roger. 1996-2000. *Reference List: Surveys of Privacy Attitudes*.

<http://www.anu.edu.au/people/Roger.Clarke/DV/Surveys.html> (viewed November 2001)

Cranor, Lorrie Faith, Joseph Reagle, and Mark S. Ackerman. 1999. *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*. AT&T Labs-Research Technical Report TR 99.4.3.

<http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm> (viewed November 2001)

Fox, Susannah. 2000. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. The Pew Internet and American Life Project/Pew Charitable Trust.

<http://www.pewinternet.org/reports/toc.asp?Report=19> (viewed November 2001)

Lessig, Lawrence. 1999. Code and Other Laws of Cyberspace. New York: Basic Books.

Lester, Toby. 2001. The Reinvention of Privacy. The Atlantic Monthly, March 2001.

<http://www.theatlantic.com/issues/2001/03/lester.htm> (viewed November 2001)

Moore, Barrington. 1998. Privacy. Studies in Social and Cultural History. Armonk, NY: M. E. Sharpe, Inc.

Okamura, K., Fujimoto, M., Orlikowski, W., Yates, J. 1994. Helping CSCW Applications Succeed: The Role of Mediators in the Context of Use. ACM CSCW (1994), 55-65.

Orlikowski, W., and Gash, C. 1994. Technological Frames: Making Sense of Information Technology in Organizations. ACM Transactions on Information Systems, 12 (April 1994), 174-207.

Privacy Foundation

<http://www.privacyfoundation.org/> (viewed November 2001)

Slashdot. 2001. Fox Says Web Bugs = Virus Risk.

<http://www.slashdot.org/articles/01/01/04/1543202.shtml> (viewed November 2001)

Smith, Robert Ellis. 2000. Ben Franklin's Web Site. Privacy and Curiosity from Plymouth Rock to the Internet. Providence, RI: The Privacy Journal.

Standage, Tom. 1998. The Victorian Internet. New York, NY: Walker.

Star, S., and Griesmer, J. 1989. Institutional Ecology, "Translations" and Boundary Objects. Social Studies of Science 19 (1989) 387-420.

Stefik, Mark. 1999. The Internet Edge. Cambridge, MA: MIT Press.

Warren, S. D., and Brandeis, L. D.. 1890. The Right to Privacy. Harvard Law Review IV(5, December 15, 1890):193. Available at a number of places on the WWW, including: http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html (viewed November 2001)

Weedman, Judith. 1998. The Structure of Incentive: Design and Client Roles in Application-Oriented Research. Science, Technology, and Human Values 23(3) (1998) 315-345.

Appendix A: Cookies

Cookies are small pieces of computer code originally designed to maintain what web designers call "state" across a number of web pages. Maintaining state is important in sites that require the user to move from page to page while preserving some kind of personal profile.^[31] The reasons for maintaining a personal profile are varied. You might be shopping at an on-line retailer, in which case cookies can keep track of your purchases on different pages. If you frequent a news site, that site might remember your zip code so that every time you log on you are presented with local news and weather.

A cookie typically consists of a line of data in a file that is stored on your hard drive. In my own case, I have a Macintosh computer, and I use Netscape as my browser. On my computer, the cookie file can be found by going to my hard-drive folder Hard Drive and then System > Preferences > Netscape *f*. In the 'Netscape *f*' folder there is a file named "MagicCookie" that can be read as a text file. If I open this file on my Mac, I see a header that says,

Netscape HTTP Cookie File

http://www.netscape.com/newsref/std/cookie_spec.html

This is a generated file! Do not edit.

The first line in the header tells what this file is (a cookie file). The second line usefully contains an address that links to a page on Netscape's web site that describes the operation of cookies. The address is there presumably to satisfy the curiosity of those who have decided to rummage around in their Netscape folders to look at their cookie files. The third line is a warning to anyone who has done such rummaging that he/she should proceed no further. You can ignore this warning and delete whatever lines in the cookie file you wish; this is one way to get rid of cookies from your hard drive. You might find, however, that user "profiles" you have established at sites you frequently use will no longer work. The # in front of each of these three lines tells your computer to ignore these lines and not to treat them as cookies.

This header is followed by a list of cookies that look like this:

.amazon.com TRUE / FALSE 2082787401

x-mainr4aFOlZOz1UeNYOb8cH9ymZOHoE2pgYU.

Each cookie consists of an address—in this case, .amazon.com—and a series of letters and/or numbers. If, as you are surfing the Web, you type a URL into your browser that matches any of the addresses in your cookie file—in this case, amazon.com—when your browser subsequently sends the request to the site for the page you want to view, it also sends the cookie identification number (along with details such as the Internet address of your computer and the browser and operating system you are using). If the site you are contacting recognises this ID number, it can then retrieve any information regarding your user profile that is stored on the server—for instance, your log-in name and password, local news preferences, etc. When you receive the web page back, it will then be customised to this profile. In this way, cookies function as a sort of caller ID that lets the web site know who you are when you contact it.

Browsers allow the user to turn off cookies (although this might reduce the functionality of some web sites). In Netscape 4.0 for Macintosh, follow this path: Edit > Preferences > Advanced, and press the button that says "Accept only cookies."

Appendix B: TRUSTe[32]

TRUSTe is a non-profit privacy organisation that evolved out of a panel at Esther Dyson's PC Forum in 1996 that discussed the nature of trust on the Web. Chair of the Electronic Frontier Foundation (EFF),[33] Dyson set up a body that in June 1997 became TRUSTe.[34] Agreement was reached early "on two cornerstone principles that would govern the TRUSTe program: 1. Users have a right to informed consent; and 2. No single privacy principle is adequate for all situations." [35]

TRUSTe's mission was to make the rapidly expanding World Wide Web a place consumers could trust. It felt that consumers had a right to be informed about whatever information was being collected from them in web interactions and that online retailers would benefit from consumers being attracted to sites they knew operated with ethical privacy policies. Trust would be an integral part in successfully expanding the Web, with an emphasis not on preventing the collection of data but on providing the consumer with information regarding how that data was collected and used.

Several approaches were tried. Dyson noted in an early e-mail that

TRUSTe is *not* based on the premise that info will be collected. It is based on the premise of notification *whether* info will be collected, and allowing the customer to walk away if she/he does not like the options offered. There are *three* overall options, the first of which is "no data collected." The second is "data collected only for our use," although AOL (*Not* a TRUSTe supporter) has certainly muddled that concept recently! And the third is "data collected. . . ." with further disclosure.[36]

This three-tiered approach was abandoned as too complex; and in an effort to encourage widespread uptake of TRUSTe's principles, a more identifiable "one brand" approach to privacy was adopted.[37] On its current

web site, TRUSTe—motto: “Building a Web you can believe in”—states,

As an Internet user, you have a right to expect online privacy and the responsibility to exercise choice over how your personal information is collected, used, and shared by Web sites. The TRUSTe program was designed expressly to ensure that your privacy is protected through open disclosure and to empower you to make informed choices.[\[38\]](#)

An essential part of the TRUSTe programme is the TRUSTe “trustmark,”

an online branded seal displayed by member Web sites. The trustmark is awarded only to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures. Privacy principles embody fair information practices approved by the U.S. Department of Commerce, Federal Trade Commission, and prominent industry-represented organizations and associations. The principles include:

- Adoption and implementation of a privacy policy that takes into account consumer anxiety over sharing personal information online.
- Notice and disclosure of information collection and use practices.
- Choice and consent, giving users the opportunity to exercise control over their information.
- Data security and quality and access measures to help protect the security and accuracy of personally identifiable information.

While TRUSTe has a comprehensive privacy policy, it has also come in for some criticism, especially from privacy advocates who claim that as an industry-funded regulatory body, it lacks sanction. In a number of cases where the privacy policies of corporations displaying the TRUSTe mark have been found to be less than adequate, TRUSTe has been accused of failing to follow through, for instance by revoking a corporation’s TRUSTe license (examples include heavily visited sites like Microsoft[\[39\]](#) and Real Networks[\[40\]](#)). Perhaps the most embarrassing time for TRUSTe was when it was realised that, counter to its own privacy policy, TRUSTe was itself loading web bugs from a third-party server, that of TheCounter.com,[\[41\]](#) onto its web site. While TRUSTe justified this use of web bugs by saying that they were a way of outsourcing web site traffic measurement, the incident also generated bad publicity for TRUSTe.[\[42\]](#)

How fair are these criticisms of TRUSTe? The privacy watchdog group that exposed TRUSTe’s use of web bugs on its own site, Interhack,[\[43\]](#) accepted that TRUSTe’s use of web bugs was benign and probably born of ignorance. More generally, with regard to accusations that TRUSTe is toothless when it comes to censuring the corporations it is supposed to monitor, it appears that one of TRUSTe’s problems is that it is attempting to act as a regulatory body without any statutory powers. Instead, TRUSTe relies on achieving corporate compliance with its objectives by hoping that its reputation amongst consumers as a defender of privacy will attract additional users to sites with the TRUSTe Trustmark. Conversely, in order to attract consumer trust, TRUSTe has to show that it is capable of addressing consumers’ privacy concerns, for instance with regard to persuading corporations with web sites to provide meaningful privacy policies. It is a delicate balancing act that, in the absence of any legal reference points, is proving tricky to maintain.

Appendix C: Definitions of privacy and confidentiality in various National Library Associations' Codes of Ethics [\[44\]](#)

Australia

Must protect each user's right to privacy with respect to information sought or received and materials consulted

Canada

[P]rotect the privacy and dignity of library users and staff

Hong Kong

Library and information personnel should respect a client's privacy and the confidentiality of the library-client relationship.

Croatia

The librarian has the right and obligation to protect the privacy of all users of information and library resources, both during and after the provision of a service in response to a query.

Estonia

We acknowledge each person's and every social group's rights to privacy and confidentiality with respect to information, and we protect intellectual property rights. We follow the laws, agreements and standards applying to our professional work.

Israel

The librarian does not disclose the information which a user has requested or received, and does not report the sources to which the user referred and the material he borrowed and/or circulated.

The librarian ensures that the user community of the library under his/her care will be aware of his/her duty to maintain professional confidentiality concerning the services rendered to users.

Italy

The librarian guarantees the confidentiality of the user, of the information he requested or received and of the information sources used.

In carrying out his professional duties, the librarian should not place himself in a position of conflict of interest and shall not use the information and resources available to him by virtue of his position for his personal interest.

Jamaica

The librarian should respect the confidentiality of any information revealed by the user in the course of research.

Japan

A Librarian should respect the confidentiality of each library user. In order to assure people's freedom to read, a Librarian should respect the privacy of each library user, and should not divulge his/her name or details of books or other library materials used to third parties, and should resist all pressures to do so except as required under due process of law . . . This duty is carried out by all the staff members, both professional and non-professional, and both full-time and part-time.

Lithuania

A librarian respects a right of a user to privacy and does not distribute confidential information.

Malaysia

Must protect the library user's right to privacy and confidentiality with respect to information sought or received, and materials consulted or borrowed.

Netherlands

The librarian safeguards, within current law, the privacy of users at all times.

Portugal

Privacy of Users of Information Services

Privacy is important in its own right. Information professionals in Portugal recognise the importance and singularity of each of the users of their services and thus respect their privacy as a right.

Information professionals in Portugal assume the following responsibilities as their own:

1. To use personal data only for the purposes for which they were collected.
2. To consider the following data as private: records of reading materials, loans, bibliographical consultations and any data that may identify the users of their services and their activities.
3. Not to publish data of a private nature, observing the security requirements to ensure that these data are not intercepted.
4. To guarantee that records kept on paper or in computerised form are not left in places where they can be easily accessed or read by other users.
5. To take every precaution to ensure that the manipulation of and access to computerised records are only undertaken by authorised members of their services.
6. To guarantee that data on the reading habits or bibliographical interests of the users of their services are collected for the normal functioning thereof and that it is only possible to use these data for research or statistical purposes.
7. Not to inform any user of their services about the work undertaken by another user.
8. To consider any request for information that seeks to violate the privacy of a user as being improper and abusive.
9. If pressurised [sic] for any reason into providing information of a private nature, information professionals may only do so with the prior written permission of the users who made this information available to them.

Information professionals in Portugal consider that it is their duty to respect Article 12 of the Universal Declaration of Human Rights:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Slovenia

A Librarian should protect a user's privacy as regards personal data, searched items and information.

Sweden

The librarian shall treat library users with respect and good judgement: impartially and equally. The individual's right to privacy shall be safeguarded, both as regards personal situation and information acquired and as regards materials borrowed.

Ukraine

[W]e protect the right of library users to the confidentiality of information and provide confidentiality of library and informational services.

United Kingdom

(i) Members must not divulge or permit to be divulged any materials, information or administrative record (in manual or electronic form) which has been entrusted to them in confidence, to any third party nor use such information without the prior consent of the client for any purpose other than that for which it was first obtained. This duty to the client continues after the relationship of librarian and client ceases.

(ii) Members are absolved from the duty set out in sub-paragraph (i) above in so far as is required by law and in so far as it is necessary to answer accusations before the Disciplinary Committee.

United States

We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.

[1] For a detailed discussion and historical contextualisation of Warren and Brandeis, see Smith (2000:121-).

[2] See for example the discussion in the World Wide Web Consortium's guide to cookies available at: <http://www.w3.org/Security/Faq/wwwsf7.html#Q66> (viewed November 2001)

[3] Robert Conlin and Mary Hillebrand, *Disney's Buena Vista Acquires Stake in Toysmart.com*. E-Commerce Times, August 25, 1999. Available at:

<http://www.ecommercetimes.com/news/articles/990825-6.shtml> (viewed November 2001)

Keith Regan and Nora Macaluso, *Disney Pulls Plug on Toysmart.com*. E-Commerce Times, May 23, 2000. Available at:

<http://www.ecommercetimes.com/news/articles2000/000523-4.shtml> (viewed November 2001)

[4] Federal Trade Commission, *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*. Available at:

<http://www.ftc.gov/opa/2000/07/toysmart2.htm> (viewed November 2001)

See also:

Chet Dembeck, *FTC to Block Toysmart Data Sale*. E-Commerce Times, July 10, 2000.

<http://www.ecommercetimes.com/news/articles2000/000710-6.shtml> (viewed November 2001)

Paul Greenberg, *Toysmart Flap Triggers Privacy Bill*. E-Commerce Times, July 13, 2000.

<http://www.ecommercetimes.com/news/articles2000/000713-4.shtml> (viewed November 2001)

FTC, Toysmart.com settle. CNNfn, July 21, 2000. <http://cnnfn.com/2000/07/21/companies/toysmart/>

Lori Enos and Elizabeth Blakey, *Toysmart Will Not Sell Customer Names . . . For Now*. E-Commerce Times,

July 28, 2000. <http://www.ecommercetimes.com/mews/articles2000/000728-2.shtml> (viewed November 2001)

[5] Jill Morneau, *Judge Blocks Toysmart's Plan To Sell Customer List*. TechWeb News, August 18, 2000. Available at:

<http://www.techweb.com/wire/story/TWB20000818S0011> (viewed November 2001)

[6] Greg Sandoval, *Failed Dot-Coms May be Selling Your Private Information*. CNET News, June 29, 2000. Available at:

<http://news.cnet.com/news/0-1007-202-2176430.html> (viewed November 2001)

[7] Examples of surveys of Internet user attitudes to privacy include Cranor *et al.*, 1999; Fox, 2000; Cheskin Research 2000. Clarke 1996-2000 has a list of links to a number of surveys on online privacy.

[8] http://www.netlibrary.com/aboutus_index_info.asp (viewed November 2001)

[9] Vincent Kiernan, *An Ambitious Plan to Sell Electronic Books*. The Chronicle of Higher Education, April 16, 1999. Available at:

<http://chronicle.com/free/v45/i32/32a02901.htm> (viewed November 2001)

[10] Kris Hudson, *NetLibrary Secures Financing*. Boulder Daily Camera, May 25, 1999. Available at:

<http://www.bouldernews.com/business/25bnet.html> (viewed November 2001)

[11] Carly Schulaka, *NetLibrary to Hire Hundreds*. Boulder Daily Camera, July 20, 1999. Available at:

<http://www.bouldernews.com/business/20bnet.html> (viewed November 2001)

[12] http://www.netlibrary.com/aboutus_index_info_pressreleases.asp (viewed November 2001)

[13] <http://www.netlibrary.com/articles.asp> (viewed November 2001)

[14] A button is a graphic image on a web page that when clicked usually takes the user to another page. The image that is clicked could just be a small circle or square; it can also be a larger image containing some text such as "Click Here." Note that such images are *images* of text rather than text themselves. They are composed in imaging editing software and cannot be cut and pasted from the web browser window into a text document. As these images can be tailor-made for each web site, many sites use them although the same functionality can be achieved through the use of faster loading text links.

[15] <http://www.akamai.com>

[16] <http://www.engage.com/adknowledge/> (viewed November 2001)

[17] <http://www.Engage.com/> (viewed November 2001)

[18] <http://www.cmgi.com/> (viewed November 2001)

[19] http://www.netLibrary.com/help/privacy_statement.asp (viewed November 2001)

[20] The license agreement and self assessment sheet have since been updated to version 6.1, but the relevant part of the self assessment sheet quoted here is essentially the same. See:

http://www.truste.org/webpublishers/pub_selfassessmenttest.html (viewed November 2001)

http://www.truste.org/webpublishers/truste_license_agreement_6_1.htm (viewed November 2001)

[21] Slashdot, *Fox Says Web Bugs = Virus Risk*. Slashdot, January 4, 2001. Available at:

<http://www.slashdot.org/articles/01/01/04/1543202.shtml> (viewed November 2001)

[22] <http://www.faiife.dk/ethics/codes.htm> (viewed November 2001)

[23] American Library Association: <http://www.ala.org/alaorg/oif/ethics.html> (viewed November 2001)

[24] The Library Association, U.K.: <http://www.la-hq.org.uk/directory/about/conduct.html> (viewed November 2001)

[25] <http://www.ala.org/oitp/> (viewed November 2001)

[26] <http://www.ala.org/oitp/pubdraft.pdf> (viewed November 2001)

[27] See for example the case studies discussed by Okamura et al 1994; Orlikowski and Gash, 1994; Star and Griesmer 1989; Weedman 1998.

[28] Hane, Paula. *NetLibrary in Discussions with Potential Buyers*. Information Today, October 22, 2001. <http://www.infotoday.com/newsbreaks/nb011022-1.htm> (viewed November 2001)

[29] OCLC. *OCLC makes offer to purchase assets of netLibrary*. OCLC, November 15, 2001. <http://www.oclc.org/oclc/press/20011115.shtm> (viewed November 2001)

Hane, Paula. *OCLC completes netLibrary Acquisition, Raises e-Book Fees*. Information Today, February 11, 2002. <http://www.infotoday.com/newsbreaks/nb020211-2.htm> (viewed November 2001)

[30] Gibbons, Susan. *Ebook obituaries in abundance*. Librarian's Ebook Newsletter, Volume 2, Number 2, December 2001. <http://www.lib.rochester.edu/main/ebooks/newsletter2-2/obit.htm> (viewed November 2001)

[31] For an early technical specification for cookies, see 'Netscape.Support Documentation, Persistent Client State HTTP Cookies,' available at:

http://www.netscape.com/newsref/std/cookie_spec.html (viewed November 2001)

[32] For more background information, see TRUSTe's "Online Privacy Resource Book" (TRUSTe 2000). Available at:

http://www.truste.org/about/truste/about_truste_book_intro.html (viewed November 2001)

[33] <http://www.eff.org/> (viewed November 2001)

[34] <http://www.truste.org/> (viewed November 2001)

[35] http://www.truste.org/about/about_truste.html (viewed November 2001)

[36] <http://www.anu.edu.au/mail-archives/link/link9708/0084.html> (viewed November 2001)

[37] <http://news.cnet.com/news/0-1005-202-322221.html> (viewed November 2001)

[38] http://www.truste.org/users/users_how.html (viewed November 2001)

[39] Tim Clark, *Truste Asked to Probe Microsoft*. CNET News.com, March 16, 1999. <http://news.cnet.com/news/0-1007-200-340001.html> (viewed November 2001)

Tim Clark, *Truste Clears Microsoft on Technicality*. CNET News.com, March 22, 1999. <http://news.cnet.com/news/0-1005-200-340253.html> (viewed November 2001)

[40] Robert Lemos, *Can You Trust TRUSTe?* ZDNN, November 2, 1999. <http://www.zdnet.com/filters/prINTERfriendly/0,6061,2387000-2,00.html> (viewed November 2001)

Declan McCullagh, *Is TRUSTe Trustworthy?* Wired News, November 5, 1999. <http://www.wired.com/news/politics/0,1283,32329,00.html> (viewed November 2001)

D. Ian Hopper, *Can TRUSTe Protect Users?* CNN.com, November 9, 1999. <http://www.cnn.com/TECH/computing/9911/09/real.truste/> (viewed November 2001)

[41] <http://www.thecounter.com/> (viewed November 2001)

[42] George A. Chidi, Jr., *TRUSTe Learns Privacy Lesson the Hard Way*. IDG.net, August 25, 2000. http://www.idg.net/ic_230886_1794_9-10000.html (viewed November 2001)

George A. Chidi, Jr., *TrustE Breaks Privacy Rule*. IDG.net, August 25, 2000. <http://www.idg.net/idgns/2000/08/25/TrustEAccusedOfBreakingOwnPrivacy.shtml> (viewed November 2001)

George A. Chidi, Jr., *Is TRUSTe Trustworthy?* PCWorld.com, August 25, 2000. <http://www.pcworld.com/resource/printable/article/0,aid,18228,00.asp> (viewed November 2001)

Keith Regan, *TRUSTe Stung by Own Privacy Gaffe*. E-Commerce Times, August 25, 2000. <http://www.ecommercetimes.com/news/articles2000/000825-3.shtml> (viewed November 2001)

Linda Rosencrance, *Truste Accused of Violating its Own Privacy Policy*. Computerworld.com, August 25, 2000.

http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO49059-,00.html (viewed November 2001)

[43] <http://www.interhack.org/> (viewed November 2001)

[44] <http://www.faiife.dk/ethics/codes.htm> (viewed November 2001)