User Authentication in the Public Area of Academic Libraries in North Carolina

Gillian (Jill) D. Ellern, Robin Hitch, and Mark A. Stoffan

ABSTRACT

The clash of principles between protecting privacy and protecting security can create an impasse between libraries, campus IT departments, and academic administration over authentication issues with the public area PCs in the library. This research takes an in-depth look at the state of authentication practices within a specific region (i.e., all the academic libraries in North Carolina) in an attempt to create a profile of those libraries that choose to authenticate or not. The researchers reviewed an extensive amount of data to identify the factors involved with this decision.

INTRODUCTION

Concerns surrounding usability, administration, and privacy with user authentication on public computers are not new issues for librarians. However, in recent years there has been increasing pressure on all types of libraries to require authentication of public computers for a variety of reasons. Since the 9/11 tragedy, there has been increasing legislation such as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and Communications Assistance for Law Enforcement Act (CALEA). In response, administrators and campus IT staff have become increasingly concerned about allowing open access anywhere on their campuses. Restrictive licensing agreements for specialized software and web resources are also making it necessary or attractive to limit access to particular academic subgroups and populations. Permitting access to secured campus storage from these computers can make it necessary for libraries to think about the necessity of authentication. And finally, the general state of the economy has increased the user traffic to libraries, sometimes making it necessary to control the use of limited computer resources. Authenticating can often make these changes easier to implement and can give the library more control over its IT environment.

That being said, authentication comes at a price for librarians. Authentication often creates ethical issues with regards to patron privacy, freedom of inquiry, increasing the complexity of using public area machines, and restricting the open access needs of public or guest users. Requiring a patron to log into a computer can make it possible for organizations outside the library's control

Gillian (Jill) D. Ellern (ellern@email.wcu.edu) is Systems Librarian, **Robin Hitch** (rhitch@email.wcu.edu) is Tech Support Analyst, and **Mark A. Stoffan** (mstoffan@email.wcu.edu) is Head, Digital, Access, and Technology Services, Western Carolina University, Cullowhee, North Carolina.

to collect, review and use data of a patron's searching habits or online behaviors. Issues associated with managing patron logins can also create barriers for access as well as being time consuming and frustrating for both the patron and the library staff.[1] While open, anonymous access does not completely protect against these issues, it can help to create an environment of free, private and open access similar to the longstanding situation with the book collection in most libraries.

The Hunter Library Experience

While working on the implementation of a new campus-wide pay-for-print solution in 2009, librarians from the Hunter Library at Western Carolina University began to feel pressured by the campus IT department to change its practice of allowing anonymous logins to all the computers in the public areas of the library. Concerns about authenticating users on library public area machines had been building between these two units for several years. The resulting clash of principles between protecting privacy and protecting security came to a head over this project.

The Hunter Library employees perceived that there needed to be more time for research and debate before implementing the preceded mandate. Initially, there was great resistance from campus IT staff to take the library's concerns into account, but eventually a compromise was worked out that allowed the library to retain anonymous logins on its public computers. The confrontation led library staff to investigate the practices of other libraries, particularly within the University of North Carolina (UNC) System of which it is a member. It seemed a logical development to extend the initial research into the authentication practices throughout the state of North Carolina.

The Problem

One of the first questions asked by Western Carolina's library administration of the systems department was what other libraries in the area were doing. In our case, the library director specifically asked how many of West Carolina's sister universities were authenticating and why. Anecdotally, during this process, it seemed that many other University of North Carolina System libraries reported being pressured to authenticate their public computers by organizations outside the library, most often the campus IT department.

When the librarians at the Hunter Library began looking at research to support their position, hard data and practical arguments that could be used to effectively argue their case against this change, helpful literature seemed to be lacking. Some items were found such as Carlson, writing in the *Chronicle of Higher Education*, who reported on the divide between access and security. He confirmed that other librarians also have ambivalent feelings about authentication issues but that there was also growing understanding in libraries about the potential vulnerability of networks or misuse of their resources.[2]

It seemed that the speed at which authenticating computers in the public areas of libraries was happening across the country had not really allowed the literature on the subject to quite catch up.

Those studies that existed such as *SPEC Kits* seem to address the issue from the perspective of larger research libraries or else did not systematically assess other specific groups of libraries.[3,4] There were questions in our minds about whether the current research that was found would describe the trends and unique situations of libraries located in rural areas or in other types of academic libraries. There seemed to be no current statewide or geographically defined analysis of authentication practices across various types of academic libraries in a specific state or region, nor were there any available studies creating a profile of libraries more likely to authenticate computers in their public areas. We questioned if the rural nature of our settings, our mission, or our geographic area in the South might reinforce or hurt our position with IT. Authentication status is not something that is mentioned in the ALA directory nor is this kind of information often given on a library's web site. We found that individuals usually need to call or visit the library directly if they want to know about a library's authentication practices.

During the initial investigation, the need for this kind of information to support the library's perspective became clear. This question led to the creation of this survey of authentication practices in a larger geographical area and across various kinds of academic libraries. The goals of this research were to determine some answers to the following questions:

- What is the current state of authentication practices in the public area of academic libraries in North Carolina?
- What factors caused these libraries to make the decisions that they did in regards to authentication?
- Could you predict whether an academic library would require users to authenticate?

LITERATURE REVIEW

A number of studies have discussed various other aspects of user authentication in libraries, including privacy and academic freedom concerns, guest access policies, differing views of privacy and access between library and campus IT departments, and legislation impacting library operations. All are potential factors impacting decisions on authentication of patron accessible computers located in the public areas of library.

Privacy and academic freedom about the use of a library's collection have long been major concerns for librarians even before information technology was introduced. The impact of 9/11 and the PATRIOT Act made the discussion of computers and network security, especially in the library environment much more entwined. Oblinger discussed online access concerns in the context of academic values, focusing on unique aspects of the academic mission. She discussed the results of an EDUCAUSE/Internet2 Computer and Network Security Task Force invitational workshop that established a common set of principles as a starting point for discussion: civility and community, academic and intellectual freedom, privacy and confidentiality, equity of access to resources, fairness, and ethics. All of these principles, she argues, are integral to the environment

of a university and concluded that security is a complex topic and that written, top-imposed policies alone will not adequately address all concerns.[5] While not directly addressing the issues of the library's public computer access in particular, she established a framework of values on how security issues relate to the university culture of freedom and openness.

Dixon in an article written for library administrators discussed privacy practices for libraries within the context of the library profession's ethical concerns. She highlights such documents as the *Code of Ethics of the American Library Association*[6], the Fair Information Practices adopted by the Organization for Economic Cooperation and Development[7], and the NISO *Best Practices for Designing Web Services in the Library Context*[8]. She also reviews a variety of ways that patron data may be misused or compromised. She stated that all the ways that patron data can be be stored or tracked by local networks, IT departments, or Internet service providers may not be fully understood by librarians. While most librarians ardently maintain the privacy of patron circulation records, she points out that similar usage data on online activities may be collected without the librarians or their patrons being aware. Dixon studied the current literature and maintained that libraries need to be closely involved in decisions about the collection and retention of patron usage data, especially when patron authentication and access is controlled by external agencies such as campus or city IT departments, because of a tendency for security to prevail over privacy and free inquiry.[9] This theme was of major importance to us in preparing the present study as it shows that we are not alone in these concerns.

Carter focused on the balance between security and privacy and suggested several possible scenarios for addressing both areas. He emphasized librarian values involving privacy and intellectual freedom, contrasting the librarian's focus on unrestricted access with the over-arching security concerns of computing professionals. He discussed several computer access policies in use at various institutions and possible approaches. These options include computer authentication (with associated privacy concerns), open access stations visually monitored from staffed desks, or routine purging of user logs at the end of each session. He also suggested librarians lobby state legislatures to have computer usage logs included in laws governing the confidentiality of library records.[10]

Still and Kassabian provided a good summary of Internet access issues as they affected academic libraries from legal and ethical perspectives. They suggested that librarians focus on public obligations, free speech and censorship, and potential for illegal activities occurring on library workstations. The issues highlighted in the article have increased in the 15 years since the article was written but it remains the best available overview.[11] The arguments put forth in this article proved relevant for us in understanding the multitude of viewpoints regarding authentication even before 9/11.

In the post-9/11 era, Essex discussed the USA-PATRIOT Act and its implications for libraries and patron privacy. Some of the 9/11 terrorists were reported to have made use of public library computers in the days before the attack. This has led to heighted concern about patron privacy

among librarians. Accurate assessment of its impact is difficult due to restrictions placed on libraries in even disclosing that they have been subjected to search.[12] While not directly addressing authentication, the article highlights privacy issues surrounding library records of all types.

One of the arguments in not requiring authentication in the public area is the use by unaffiliated users of academic libraries. This is especially true in rural areas where an academic library might be some of the best-funded, comprehensive and accessible resources in a geographical area. Even in urban areas, guest access by unaffiliated users is a growing issue for many academic libraries because of limited resources, software licensing problems and public access to campus infrastructure. While most institutions have traditionally offered basic library services to unaffiliated patrons, the online environment has raised new problems. Weber and Lawrence provided one of the best studies of these issues. Their work surveyed Association of Research Libraries (ARL) member libraries to determine the extent of mandatory logins to computer workstations and document how online access was provided to non-affiliated guest users. They concentrated their study questions on Federal and Canadian Depository libraries that must provide some type of access to online government information, with or without authentication. Less than half of respondents reported having any written policies governing open access on computers or guest access policies. Of the 61 responding libraries to the survey, 32 required that affiliated users authenticate, and of these libraries and 23 had a method for authenticating guest users.[13] This article, which was published just as this study was testing and evaluating the survey instrument, proved to be very useful as we worked with our questions in Qualtrics™ and dealt with the IRB requirements.

Courtney explored a half-century of changes in access policies for unaffiliated library users. Viewing the situation from somewhat early in the shift from print to electronic resources, she foresaw the potential for significantly reduced access to library resources for non-affiliated patrons. These barriers would be created by access policy issues with computing infrastructure and licensing limitations by database vendors. This is especially true if a library's licenses or policies did not specifically address use by unaffiliated users. She concluded that decisions about guest access to online library resources should be made by librarians and not be handed over to vendors or campus computing staff.[14] Our study began as a result of this very issue, i.e., an outside entity (campus IT) determining how access to library resources should be controlled, without input by librarians or library staff.

Courtney also surveyed 814 academic libraries to assess their policies for access by unaffiliated users. She focused on all library services including building access, reference assistance, and borrowing privileges in addition to online access. Many libraries were also cancelling print subscriptions in favor of online access and she questioned the impact this might have on use by unaffiliated users. While suggesting little correlation between decisions to cancel paper subscriptions and requiring authentication of computer workstations, she concluded that reduced

access by unaffiliated users would be an unintended consequence of this change.[15] This article proved valuable to us in framing our study, as it gave us some idea of what we might expect to find and provided some concepts to use when we formulated our survey.

Best-Nichols surveyed public use policies in 11 NC tax-supported academic libraries and asked similar questions to our own. This study was dated and didn't address computer resources, but some of the same issues were addressed.[16] Public use and authentication policies have the potential to impact one another and how the library responds.

Courtney called on librarians to conduct a carefully thought out discussion of user authentication because of the implications for public access and freedom of inquiry. While librarians are traditionally passionate at protecting patron privacy involving print resources, many are unaware of related concerns involving online authentication. She advocated for more education and open debate of the issues because of the potential gravity of leaving decision-making in the hands of database vendors or campus IT departments. Decisions regarding authentication and privacy impact library services and access, and therefore need to include input from librarians.[17] As this study included a summary of the reasons for authentication as provided by surveyed libraries, it also gave us another reference point to use when comparing our results and highlighted the intellectual freedom issues that were often missing or glossed over in other studies.

Barsun surveyed the Web sites of the 100 Association of Research Libraries to assess services to unaffiliated users in four areas: building access, circulation policies, interlibrary loan services, and access to online databases. 61 member libraries responded to requests for data. She explored the question of whether the policies governing these services would be found on a library's web site. She perceived a possible disparity between increasing demand for services generated by members of the public who are discovering a library's resources via online searching and the library's ability or willingness to serve outside users. While she did not address computer authentication issues directly, she did find that a significant percentage of academic library web sites were ambiguous about stating the availability of non-authenticated access to databases from onsite computers.[18] This ambiguity could possibly be related to vague usage agreements with database vendors that do not clearly state whether non-affiliated users may obtain onsite access to these resources. In "secret shopper" visits done as part of our own research, we saw a disparity between what was stated on a library's web site and the reality of access offered.

METHOD

It seemed appropriate to start this project with a regional focus. None of the studies available looked at authentication geographically. Because colleges and universities within a state are all subjected to the same economic, political and environmental factors, looking at the libraries might help provide some continuity for creating a relevant profile of current practices. North Carolina has a substantial number of academic libraries (114) with a wide variety of demographics. Historically, the state supports a strong educational system with one of the first public university

systems. Together with the 17 universities within University of North Carolina system, the state has 59 public community colleges, 36 private colleges and universities, and 3 religious institutions. Religious colleges are identified as those whose primary degree is in divinity or theology. (See Chart 1.)

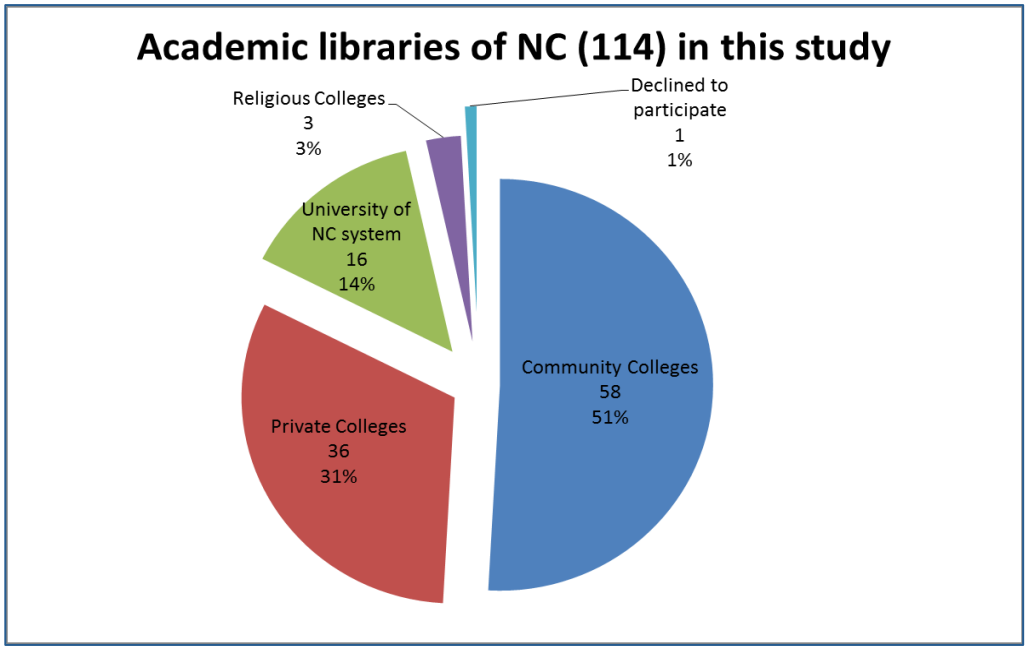


Chart 1. Survey participation by type of academic library.

Work had been started to identify the authentication practices of other UNC System libraries, so the researchers expanded the data to include the other academic libraries within the state. To create a list of the library's pertinent information for this investigation, the researchers used the *American Library Directory*[19], the NC State Library's online directories of libraries[20], and visited each library's web page to create a database. The researchers augmented each library's data to include information including the type of academic library (public, private, UNC System and religious), current contact information on personnel who might be able to answer questions on authentication policies and practices in that library, current number of books, institutional enrollment figures, and the name and population of the city or town in which the library was located. The library's responses to the survey were also tracked in the database with SPSS and Excel employed in evaluating the collected data.

A Western Carolina Institution Review Board (IRB) "Request for Review of Human Subject Research" was submitted and approved using the following statement: "We want to know the authentication situation for all the college libraries in North Carolina." The researchers discovered quickly that the definition of "authentication" would have to be explained to the review board and many of the responding librarians that filled out the survey. The research goal was further simplified with the explanation of authentication as "how do patrons identify themselves to get

access to a computer in the public area of a library" because many librarians might not realize that what they do is "authentication".

During the approval phase, there was some question about whether the researchers needed formal approval because much of the information could be collected by just visiting the libraries in person. The researchers saw no risk of potentially disclosing confidential data. However, it was decided that it was better to go through the approval process, since the survey asked the librarians whether they were being required to authenticate by outside entities. There might also be a need to do some follow-up calls and there was a plan to do site visits to the local libraries in order test the data for accuracy.

The Qualtrics™ online survey system was used to create the survey and collect the responses. Contact information from the database was uploaded to the survey system with the IRB approved introductory letter to each library contact person along with a link to the survey. The introductory letter described the goals of the project and included an invitation to participate as well as refusal language as required by the IRB request. The same language was used in the follow up emails and phone calls.

The initial (16) surveys were administered to the UNC System libraries in October – December 2010 as a test of the delivery and collection system on Qualtrics™, with the rest of the libraries being sent the survey mid-December 2010.

In the spring of 2011, the researchers followed initial survey with a second letter and then with phone calls and emails. During the follow up calls, some librarians chose to answer the survey questions with the researcher filling it out over the phone. Most filled out the survey themselves. The final surveys were completed in April 2011. Because the status of authentication is volatile, this survey data and research represents a snapshot in time of their authentication practices between October 2010 and April 2011. The researchers did see changes happening over the course of the surveying process and made changes to any data collected in follow up contact in order to maintain the most current information about that library for the charts, graphs and presentations made from the data.

In Fall 2011, the researchers did a "secret shopper" type expedition to the nearest academic libraries by visiting in person as a guest user. The main purpose of these visits was to check the data, take pictures of the library public areas, get a firsthand experience with the variety of authentication practices, and talk to and thank the librarians that participated.

The Survey

The survey asked 36 different questions using a variety of pull down lists, check boxes and fill in the blank questions. Qualtrics™ allows for the survey to have seven branches, or skip logic, that asked further questions depending upon the answer given. These branches allowed the survey software to skip particular sections or ask for additional information depending on the answers

supplied. Some libraries, especially those that didn't authenticate or didn't know specific details, might be asked as little as 14 questions while others received all 36. The setup of computers in the public area of libraries can be quite variable, especially if the library differentiates between student-only and guest/public use only workstations. The survey questions were grouped into seven basic areas: Descriptive, Authentication, Student-only PCs, Guest/Public PCs, Wireless Access, Incident Reports, and Computer Activity Logs.

The full survey is included as Appendix A.

Initial Hypothesis

Given the experience at the Hunter Library, we expected the following factors might influence a decision to authenticate. Some of these basic assumptions did influence our selection of questions in the seven areas of the survey.

We expected to find:

- When the workstations were under the control of campus IT, authentication would usually be required
- When the workstations were under the control of the library, authentication would probably not be required
- That factors such as population, enrollment, and book volume would play a role in decisions to authenticate
- That librarians would not be aware of what user information was being logged whether or not authentication was required
- A library would have experienced incidents involving the computers in the public area that the library would have authentication
- That authentication increased from post- 9/11 factors and its legal interpretations to force libraries to authenticate

SURVEY QUESTIONS, RESPONSES, AND GENERAL FINDINGS

The data collected from this survey, especially from those libraries that did authenticate, produced over 200 data points for each library. Below are those that resulted in answers to questions posed at the outset that particularly looked at overall authentication practices. Further articles are planned to look at areas of inquiry with regards to other related practices in the public areas of academic libraries geographically.

There are 114 academic libraries in North Carolina. As a result of the follow up emails and phone calls, this research survey got an exceptional 99.1% response rate (113 out of 114). Once the

appropriate librarians were contacted and understood the scope and purpose of this study, they were very cooperative and willing to fill out the survey. Those who were contacted via phone mentioned that the original email was overlooked or lost. Only one library refused to participate in the study.

Individual library's demographics were collected in a database by using directory and online information. The data was matched with the survey data provided by the respondents to produce more in-depth analysis and create a profile of each library.

How many libraries in North Carolina are authenticating? (Chart 2)

The survey asked: "Is any type of authentication required or mandated for using any of the PCs in the library's public area?" 66% (or 75) of libraries answered yes that they required authentication to use the PCs. (See Chart 2.)

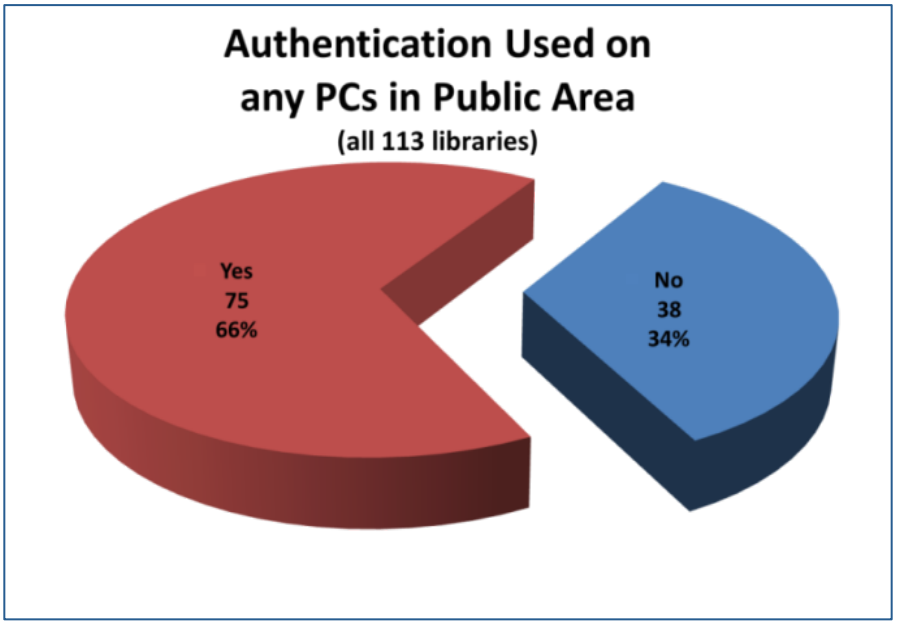


Chart 2.

Are some types of libraries more likely to authenticate? (Chart 3)

While each type of library had a different overall total as compared to the other types, Chart 3 shows how the percentages of authentication hold for each type. Three out of the four types of libraries authenticate more often. Of the 58 community college libraries, 60% (or 35) of them require users to authenticate. Seventy-eight percent (78%) of the 36 private colleges libraries authenticate and 11 of the 16 (or 69%) UNC System libraries authenticate. Only the religious college libraries more often don't require users to authenticate (1 of the 3 or 33%), although this is a very small population in the survey. However, percentagewise, community colleges are more likely to not require users to authenticate then private college libraries (40% vs. 22%) and the UNC System libraries, that are public institutions, fall in the middle at 31%.

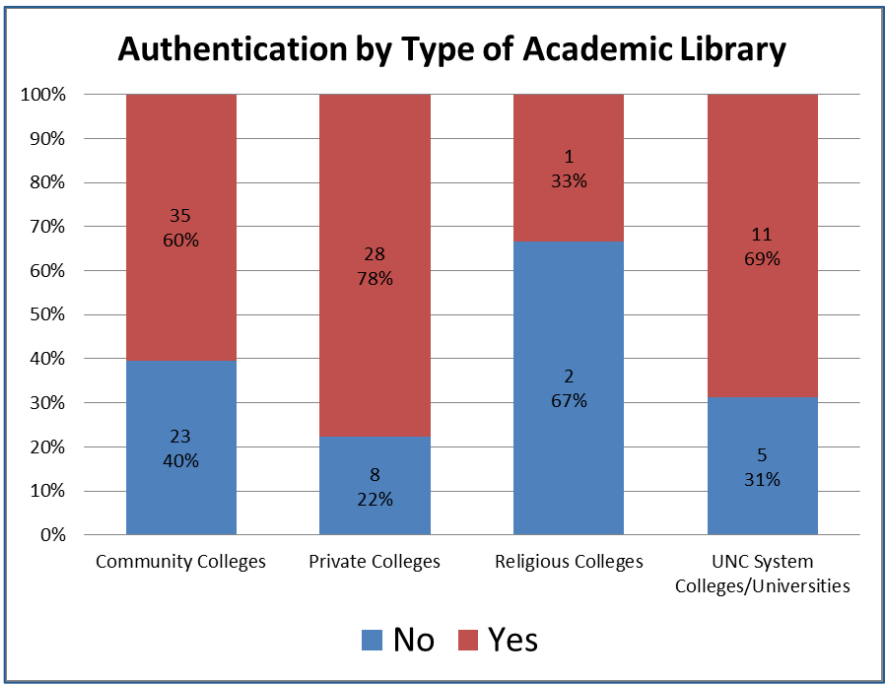


Chart 3.

How many academic libraries were required to authenticate PCs in their public areas? (Chart 4)

Of the 75 libraries that required patrons to authenticate, when asked if "they were required to use this authentication", 59 (52%) replied "yes". Putting these data points together shows that 16 (or 14%) of the libraries authenticate even though they were not required to do so. Some clues about why this was were asked in the next question and during the follow up phone calls.

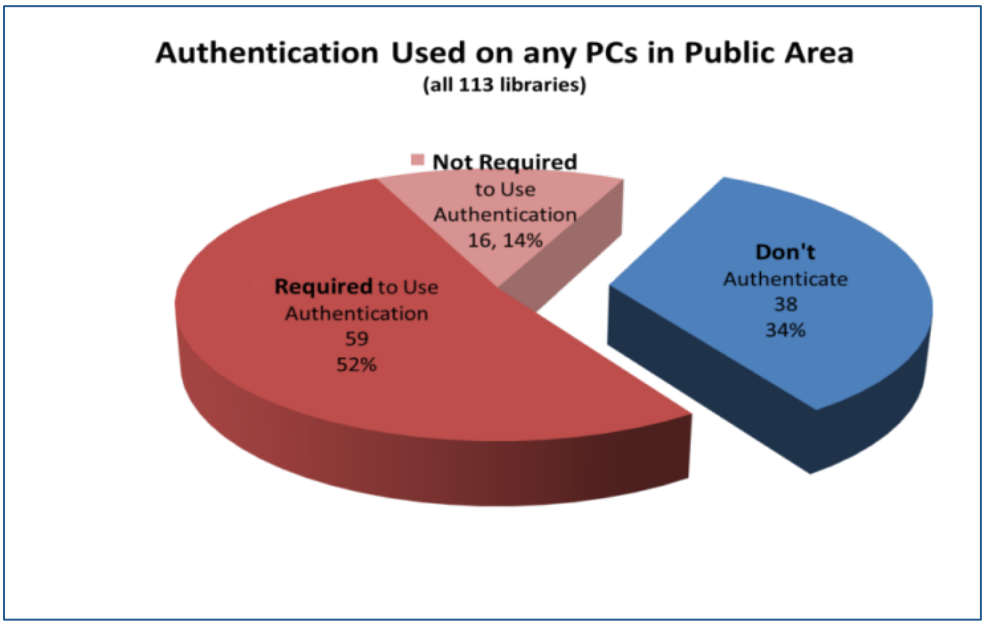


Chart 4.

Why was Authentication Used?

Libraries were asked, "Do you know the reasons why authentication is being used?" If they answered "prevent misuse of resources" or "control the public's use of these PCs" then an additional question was asked, "What led the library to control the use of PCs?" This option had two check boxes ("inability of students to use the resources due to overuse by the public" and "computer abuse") and a third box to allow free text entry. A library could check more than one box.

Of those 75 libraries that authenticated, 60% (or 45) checked "prevent misuse of resources" and 48% (or 36) cited "controlling the public's use of these PCs" as the reasons for authenticating.

In normalizing the data from the two questions and the free text field, Table 1 combines all answers to illustrate the number and percentages of each.

Top Reasons Why Authentication is Used or What Lead to Its Use to Control
(75 Authenticating Libraries)

Reasons	Number	Percentage of those that Authenticate
Prevent Missuse of Resources	45	60%
Inability of Students to Use the Resources Due to Overuse by the Public	24	32%
Computer Abuse	22	29%
Mandate by Parent Institution or Group	14	19%
Printing	11	15%
Access Control	10	13%
Statistics	8	11%
Control Underage Use	2	3%

Table 1.

In the course of the follow up calls with those libraries that answered the survey over the phone, further insight was provided. One librarian said that their IT department told them "authentication was the law and they had to do it". Another answered that they were "on the bus line and so the public used their resources more than they expected and so they had to".

To get a better understanding of the scope and variety of these answers, here are some examples of the reasons cited in the free text space: "all IT's idea to do this" "Best practices", "Caution", "Concerned they would be used for the wrong reasons", "Control", "We found them misusing computer resources (porn, including child porn)", "Control over college students searching of inappropriate websites, such as porn/explicit sites", "Disruption", "Ease of distributing

applications", "Fear of abuse on the part of legal", "Legal issues regarding internet access", "Making students accountable", "Monitor use", "Policy", "Security of campus network", "Security of machines after issues were raised at a conference", and "Time".

Who required that the libraries authenticate? (Chart 5)

The survey asked, "What organization or group required or mandated the library to use authentication?" Respondents were allowed to choose more than one of the 5 boxes. These choices included "the library itself," "IT or some unit within IT," "college or university administration," "other" (with a text box to explain), and "not sure". The results of this question are shown in Chart 5. The survey revealed that the decision was solely the library's choice 25% of the time, (or 28 libraries) 22% of the time the library was mandated or required to authenticate by IT or some unit within IT (or 25 libraries) and 4% of the time a library's college or university administration required or mandated authentication (or 4 libraries). Collaborative decisions in 14 libraries involved more than one organization. Of the 39 libraries that were involved with the authentication decision (28 that made the decision by themselves and 11 that were part of a collaborative decision), 55% (or 16) authenticated even though they were not required to do it.

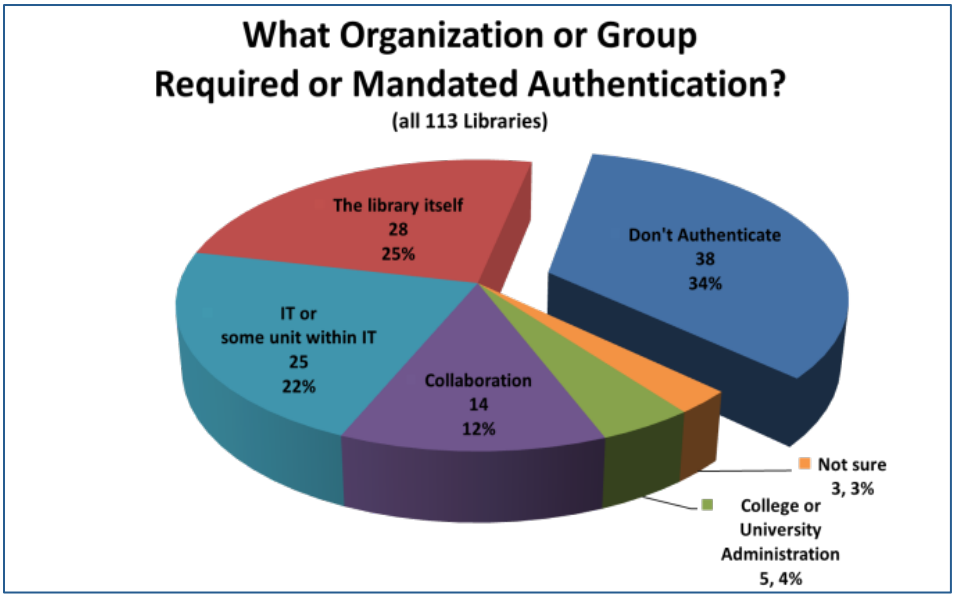


Chart 5.

What type of authentication is used?

Authentication in libraries can take many forms. The most common method for those libraries that authenticate was by using centralized or networked systems. Almost sixty percent of the libraries used some form of this identified access (Tables 2 and 3) with one library using some other independent system. Twenty-five percent (or 19) of libraries that authenticate still use some form of paper sign-in sheets and 21% (or 16) use pre-set or temporary logins or guest cards. Fifteen percent (or 11) use PC based sign-in or scheduling software and 8% (or 6) use the library

system in some form for authentication. A few libraries indicated that they bypass their authentication systems for guests by either having staff log guests in or disabling the system on selected PCs. We saw this during the "secret shopper" visits as well.

What Form of Authentication Do You Use?
(75 Authenticating Libraries)

Forms of Authentication	Number	Percentage of those that Authenticate
Centralized or networked authentication	44	59%
Manual paper sign-in sheets	19	25%
Preset or Temporary Authorization Logins or Guest Cards Handed Out	16	21%
Individual PC based sign-in or scheduling software	11	15%
Use the Library system in some form	6	8%
Staff Log Guests In	2	3%
Independent authentication systems	1	1%
Auto log into guests accounts at select PCs	1	1%

Table 2.

Do the forms of authentication used in libraries allow for user privacy?

When asked how they handle user privacy in authentication, of the 75 libraries that authenticate, 67% (or 50) use a form of authentication that can identify the user. In other words, most users do not have privacy when using public computers in an academic library because they are required to use some form of centralized or networked authentication. The options in Table 3 were presented to the respondents as possible forms of privacy methods. Thirty-five percent (or 26) libraries indicated that they provide some form of privacy for their patrons. Anonymous access accounted for 28% (or 21) of the libraries.

Handle User Privacy of Authentication?
(75 Authenticating Libraries)

Privacy method	Number	Percentage of those that Authenticate
Identified access (none)	50	67%
Anonymous access (each session is anonymous with repeat users not identified)	21	28%
Pseudonymous access with demographic identification (characteristics of users determined but not actually identified)	2	3%
Identified access (but not guest login - anonymous)	1	1%
Pseudonymous access (repeat users identified but not the identity of a particular user)	1	1%
Pseudonymous access (repeat users identified but not the identity of a particular user) for guest	1	1%

Table 3.

Are librarians aware of the computer logging activity going on in the public area? (Table 4)

All the 113 respondents were asked two questions about the computer logging activities of their libraries: "Do you know what computer activity logs are kept" and "Do you know how long computer activity logs are kept". The second question was only asked if "unsure" was not checked. Besides "unsure", responses on the survey included "Authentication logs (who logged in)", "Browsing history (kept on PC after reboot)", "Browsing history (kept in centralized log files)", "Scheduling logs (manual or software)", "Software use logs" and "Other". The respondents could select more than one answer. However, over half (52%) of the respondents were unsure if the library kept any computer logs at all. Authentication logs of who logged in were the most common, but those were kept in only 25% of the total libraries surveyed. A high percentage of libraries kept some kind of logs but most respondents were unsure how long those records were kept. Of the various types of logs, respondents that use scheduling software were the most familiar with the length of time software logs were kept. In one case, a respondent mentioned that the manual sign-in sheets were never thrown out and that they had retained them for years.

What Kind and For How Long Computer Logs are Kept

(All 113 Libraries)

Computer Activity Logs	Number	Of total libraries	Don't know how long data is kept (unsure)
Unsure	59	52%	100%
Authentication logs (who logged in)	28	25%	60%
None	21	19%	--
Browsing history (kept in centralized log files)	14	12%	86%
Scheduling logs (manual or software)	10	9%	70%
Browsing history (kept on PC after reboot)	7	6%	57%
Software use logs	6	5%	33%
Library system	4	4%	75%
Other	2	2%	--

Table 4. Log retention.

Are past incidents factors in authenticating?

Only three libraries reported breaches of privacy and all those libraries reported using authentication.

Of the 75 libraries that do authenticate (Chart 6, 3 bars on the right), 36 reported that they did have improper use of the PCs while 29 of the libraries reported that did not and 10 did not know. Of the 38 libraries that do not authenticate (Chart 6, 3 bars on the left), 23 reported that they had no improper use of the PCs while 13 stated that they did and 2 did not know. The overall known reports of improper use in the survey are higher when the library does authenticate and is lower when the library doesn't authenticate.

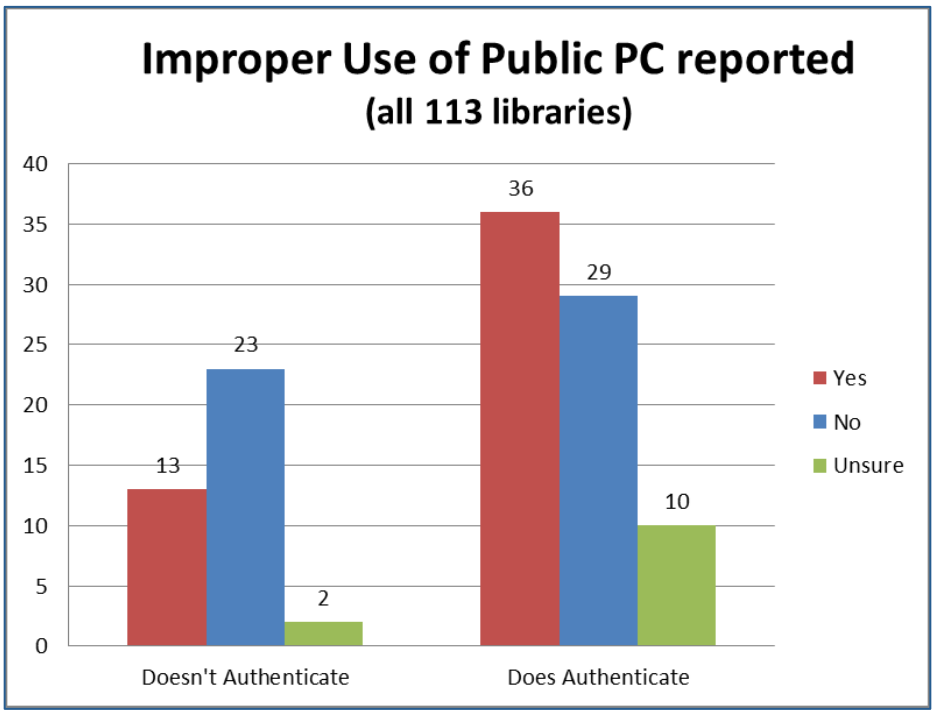


Chart 6.

When did libraries begin authenticating in their public areas?

Of the 75 libraries that authenticate, only one implemented this more than ten years prior to the survey. 51 (or 67%) of the responding libraries began authenticating between 3 and 10 years ago. 10 libraries implemented authentication in the year before the survey. This is consistent with the growth of security concerns in the post 9/11 decade. (Chart 7)

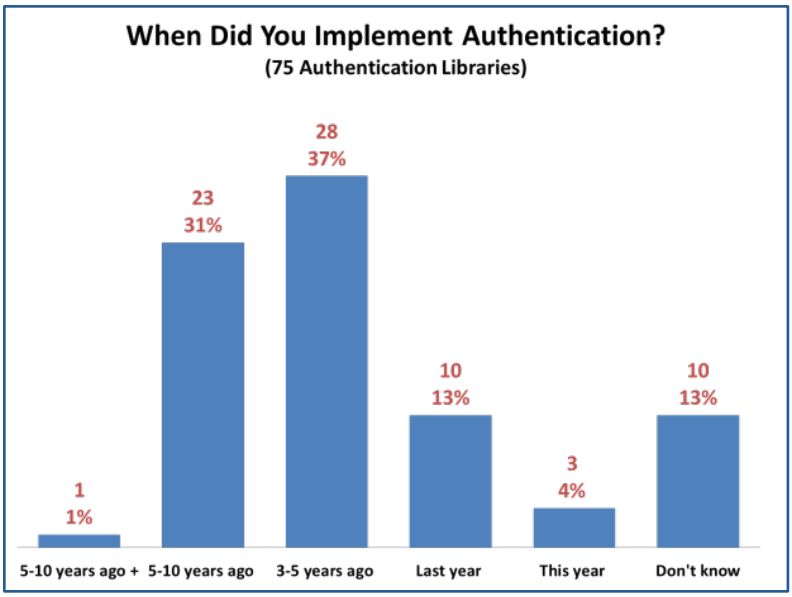


Chart 7.

DISCUSSION

Since the introduction of computer technology to libraries, library staff and patrons have used different levels of authentication depending upon the application. While remote access to commercial services such as OCLC cataloging subsystems or vendor databases have always used some form of authorization, usually username and password, it has never been necessary or desirable for public access to the library's catalog system to have any kind of authorization requirements. Most of the collections within an academic library have traditionally been housed in open access stacks where anyone can freely access material on the shelves. Printed indexes and other tools that provide in-depth access to these collections have traditionally been open as well. Today, most libraries still make their library catalog and even some bibliographic discovery tools open access and available over the web. This practice naturally extended to computer technology and other electronic reference tools until libraries began connecting them to the campus and public networks.

The principle of free and open access to the materials and resources of the library, within the library walls, has been a fundamental characteristic of most public and academic libraries. There is an ethical commitment of librarians to a user's privacy and confidentiality that has deep roots based in the First and Fourth Amendment of the US Constitution, state laws, and the Code of Ethics of the ALA. Article II of the ALA Code 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." Traditionally, library staff do not identify patrons that walk through the door; they don't ask for identification when answering questions at the reference desk nor do they identify patrons reading a book or magazine in the public areas of a library. Schneider has empathized that librarians have always valued user privacy and have been instrumental in the passing of many state's library privacy laws.[23] Usually, it is only when materials are checked out to a patron that a user's affiliation or authorization even gets questioned directly. Frequently patrons can make use of materials within the library building with no record of what was accessed. We are seeing these traditional principles of open access to materials as they transition to electronic formats. It is becoming more common for patrons to have to authenticate before they can use what was once openly available. The data collected from this survey confirms this trend with 66% of the libraries using some form of authentication in their public area.

The widespread use of personally identifiable information is making it more difficult for librarians to protect the privacy and confidentiality of library users. Although the writing was on the wall that some choices would have to be made with regards to privacy before 911, no easy answer to the problem had yet been identified. Librarians themselves are often uncertain about what information is collected and stored as evidenced by our data (Chart 6). As more information becomes available only electronically, because computers in the public areas are now used for much more than just accessing library catalog functions, it is becoming difficult to uphold the code of ethics and protect the privacy of users.

Using authentication can also make it more difficult to use technology in the library. In order to authenticate, users may be required to start or restart a computer and/or, log into or out of the computer. This can take time to do as well as require the user to remember to log off the computer when finished. Users often have difficulty keeping track of their user information and may require increased assistance (Table 5).

Authentication Issues seen on Student Only PCs
(of 32 libraries that Differentiate Between Student Only and Guest/Public Use PCs)

Authentication Issues	Number	Percentage of those that Authenticate
Users forgetting to log out of a sessions (94% require students to log out)	28	88%
ID management issues from the user (ie, like forgetting passwords)	18	56%
ID management issues from the network (i.e., updating changes in timely fashion)	6	19%
Timing out issues (only 31% use timeouts)	6	19%
Authentication system become not available	7	22%

Table 5.

Library staff or scheduling software can be required to help library guests obtain access to computer equipment. North Carolina, like other states, does have laws governing the confidentiality of library records. Librarians have long dealt with this situation by keeping as little data as possible. For example, many library circulation systems do not store data beyond the current checkout. Access logs that detail what resources a particular user has accessed would seem to fall under this legislation, although the wording in the law is vague.

Information technology departments, legal counsel, and administrators, on the other hand, are often less concerned about privacy and intellectual freedom issues. More often their focus is on security, limiting access to those users affiliated with the institution, and monitoring use. Being ready and able to provide data in response to subpoenas and court orders is often a priority. At Western Carolina University, illicit use of an unauthenticated computer in the student center led to an investigation by campus and county law enforcement. This case is still used as justification for needing to authenticate and monitor campus computer use even though the incident occurred many years ago. Being able to track an individual's online activity is believed to increase security by ensuring adherence to institutional policies. Authentication with individually assigned login credentials permits online activity to be traced to that specific account whose owner can then be held accountable for the activity performed. Librarian's responses to the survey indicate that these issues play a role in a library's decisions to authenticate as seen in the free text responses in Table 6.

Tracking use through IP address, individual login, and transaction logs allows scrutinizing of users in case of illegal or illicit use of computer resources. In many cases, this action is justified as being required by auditors or law enforcement agencies, though information regarding this is scarce. The authors of this article are not aware of any laws or auditing requirements in North Carolina that require detailed tracking of library computer use.

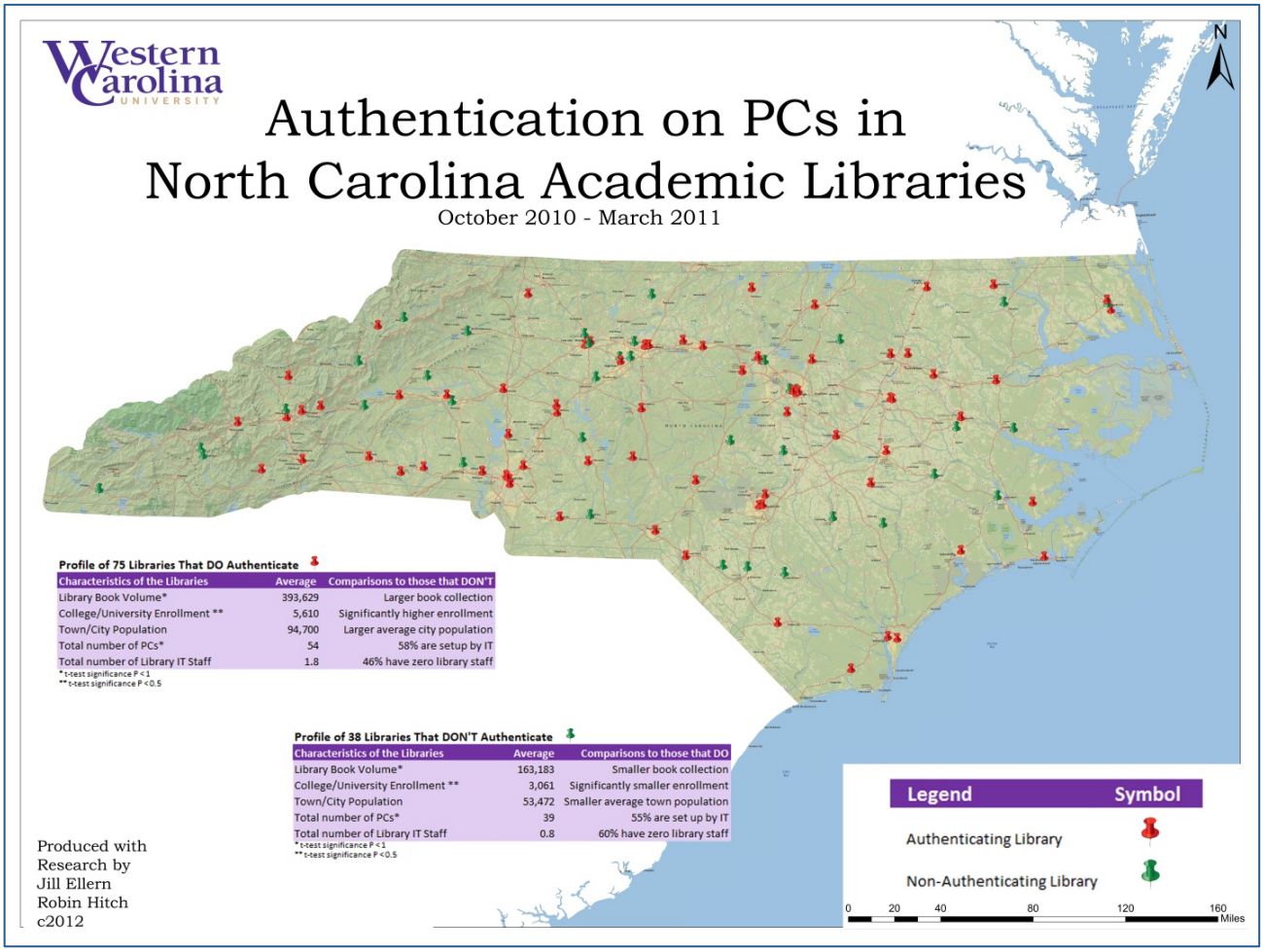
Some libraries indicated that IT departments were concerned about security of networks and/or computers. Security can be undermined when generic accounts are used or when no authentication is required. By using individual logins, users can be restricted to specific network resources and can be monitored. When multiple computers use the same account for logging in or when the login credentials are posted on each computer, it can compromise security because use cannot be tracked to a specific user. In some libraries, these security issues have trumped librarian's concerns about intellectual freedom and privacy.

Creating a profile as a result of these findings

Given the number of characteristics collected about each library, it was assumed there were some factors gathered that might influence a decision to authenticate and allow for the possibility to create a profile for prediction. The data was collected from libraries within a fixed geographic region. The externally collected and survey data was coded, put into SPSS™ and a number of statistical tests were performed to find what factors might be statistically significant. To further the geographical analysis of the data, the data was also put into ARCView™ to produce a map of North Carolina with the libraries given different colored pins for those academic libraries that authenticated vs. non-authenticated to see if there were any pattern to the choice. (Map 1)

To more completely explore the possible role that geographic information might play in the decision to authenticate, the population of the city or town the institution was located in, enrollment, book volume, number of PCs and total number of library IT staff (scaled variables) as well as ordinal variables such as "who controlled the setup of the PCs", "do you differentiate between student and public PCs", and "known incidents of privacy and misuse", were also integrated into the analysis. The data collected could not predict whether an academic library would authenticate or not using logistical regression techniques, although those that differentiate between student and public PCs did have a higher probability. Based on all our collected data and mapping, it is impossible to predict with any significance whether or not an academic library would authenticate.

So the short answer statistically is no. Using all of the data collected, a statistically significant profile could not be created, however there are general tendencies identified that the data was able to suggest.



Map 1.

For those libraries that do authenticate, the average book volume is almost 400,000, the enrollment around 5,600, the city population where the institution is located is 94,000, the total number of PCs in the public area is 54, and the average number of library IT staff is 1.8.

For those libraries that do not authenticate, the average book volume is about 163,000, enrollment around 3,000, the population is 53,000, the average number of PCs in the public area is about 39 and the average number of library IT staff is 0.8.

Libraries that authenticate tend to have statistically significant differences in book volume, the number of PCs in the public area, which has a t-test value of $P<1$. Student enrollment was the most statistically significant factor in those that authenticated, with a t-test value of $P<0.5$. Libraries that authenticate had many more students, more books and a larger number of PCs in their public areas then libraries that didn't authenticate.

Those libraries that didn't authenticate tended to be in smaller towns, more often their PCs in the public areas were setup by non-library IT staff, and had fewer library IT staff. Sixty percent (60%) of the libraries that don't authenticate had zero library IT staff.

While it was assumed at the outset of this research that the responsible campus department for the setup of the workstations (the library or IT) in the public area would be a factor in whether authentication was used in the library, the data does not support this assumption statistically.

Ethical questions about authentication as a result of these findings

There are a variety of reasons why a library might choose to authenticate despite the ethical issues associated with it. The protection and management of IT resources or the mission of the institution are two likely scenarios. A library, especially one with lots of use by unaffiliated users or guests, might chose to authenticate regardless of concerns in order to make sure its own users have preference to the PCs in the public area of their library. A private institution may choose to authenticate in order to limit access by any members of the general public. Of those 75 libraries that authenticate, 81% cited concerns about controlling use, overuse and misuse. This study also found that in 25% of the total academic libraries, the library itself decided to authenticate without influence from external groups. This was a higher percentage than was expected. Given librarian's professional concerns about intellectual freedom and privacy, we were very surprised that so many libraries choose to authenticate on their own.

We suspected that many librarians might not have a full understanding of the privacy issues created when requiring individual logins. Based on this assumption, we expected that many of the librarians would not be fully aware of what user tracking data was being kept. Examples include network authentication, tracking cookies, web browser history, and user sign-in sheets. The study found that librarians are often unsure of what data is being logged with 51 (or 45%) of 113 libraries reporting this. Only 19% reported knowing with certainly that no tracking data was kept. Of those that did know that tracking data was being kept, most had no idea how long this data was retained.

CONCLUSION

This study found that 66% (or 75) of the 113 surveyed North Carolina academic libraries required some form of user authentication on their public computers. The researchers reviewed an extensive amount of data to identify the factors involved with this decision. These factors included individual demographics, such as city population, book volume, type of academic library, and enrollment. It was anticipated that by looking a large pool of academic libraries within a specific region, a profile might emerge that would predict which libraries would chose to authenticate. Even with comprehensive data about the 75 libraries that authenticated, a profile of a "typical" authenticated library could not be developed. The data did show two factors of any statistical significance (enrollment and book volume) in determining a library's decision to authenticate. However, the decision to authenticate could not be predicted. Each library's decision to authenticate seems to be based on the unique situation of that library.

We expected to find that most libraries would authenticate due to pressure from external sources, such as campus IT departments, administrators, or in response to incidents involving the

computers in the public area. This study found that only 39% (or 44) libraries surveyed authenticated due to these factors so our assumption was incorrect. Surprisingly, we found that 25% (or 28) libraries did choose to authenticate on their own. The need to control the use of their limited resources seemed to have precedence over any other factors including user privacy. We did expect to see a rise in the number of libraries that authenticated in the aftermath of 9/11. This we found to be true. Looking at the prior research that define an actual percentage of authentications in academic libraries, no matter how limited in scope, (for example, just the ARL libraries, responding libraries, etc.), there does seem to be a strong trend for academic libraries to authenticate.

Our results, with 75% of academic libraries having authentication, support the conclusion that there is a continued trend of authentication that has steadily expanded over the past decade. This has happened in spite of librarian's traditional philosophy on access and academic freedom. Libraries are seemingly relinquishing their ethical stance or have other priorities that make authentication an attractive solution to controlling use of limited or licensed resources. Our survey results show that many librarians may not fully understand the privacy risks inherent in authentication. Slightly over half (52%) of the libraries reported that they did not know if any computer or network log files were being kept nor for how long they are kept.

The issues surrounding academic freedom, access to information, and privacy in the face of security concerns continue to effect library users. Academic libraries in smaller communities are often the only nearby source of scholarly materials. Traditionally these resources have been made available to community members, high school students, and others who require materials beyond the scope of the resources of the public or school library. As pointed out, restrictive authentication policies may hamper the ability of these groups to access the information they need. However, the data showed very little consistency to support this idea with respect to authentication in small towns and communities throughout the state.

Some of the surveyed academic libraries made a strong statement that they are not authenticating in their public area computers and have every intention of continuing this practice. These libraries are now in a distinct minority and we expect their position will continually be challenged. For example, at Western Carolina University, we continue to employ open computers in the public areas of the library but are regularly pressed by our campus IT department to implement authentication. We have so far been successful in resisting this pressure because of the commitment of our dean and librarians to preserving the privacy of our patrons.

FURTHER STUDIES

As a follow-up to this study, we plan to contact the 35 libraries that did not authenticate to determine if they now require authentication or have plans to do so. Based on responses to this survey, we expect that many librarians are unaware of the degree to which authentication can undermine patron privacy. We suggest an in-depth study be conducted to determine the degree of

understanding among librarians about potential privacy issues with authentication in the context of their longstanding professional position on academic freedom and patron confidentiality.

APPENDIX A.

Survey questions

1. Select the library you represent:

2. Which library or library building are you reporting on?

- Main Library or the only library on campus
- Medical library
- Special library
- Other

3. How many total PCs do you have in your library public area for the building you are reporting on?

4. How many Library IT or Library Systems staff does the library have?

5. Does the Library's IT/Systems staff control the setup of these PCs in the library public area?

- Yes
- Shared with IT (Campus Computing Center)
- IT (Campus Computing Center)
- No (please specify who does control the setup of these PCs)

Authentication

6. Is any type of authentication required or mandated to use any of the PCs in the library's public area?

7. Were you required to use this authentication on any of the PCs in the library's public area?

8. What organization or group required or mandated the library to use authentication on PC's in the library public area?

- The library itself
- IT or some unit within IT
- Other (please explain)
- Not sure
- College/University administration

9. Do you know the reason's authentication is being used?

- Mandated by parent institution or group
- Prevent misuse of resources
- Other (please specify)
- Control the public's use of these PCs

10. What lead the library to control the use of PCs?

- Inability of students to use the resource due to overuse by the public
- Computer abuse
- Other (please specify)

11. How are the users informed about the authentication policy?

- Screen saver
- Web page
- Login or sign on screen
- Training session or other presentation
- Other (please specify)

12. What form of authentication do you use?

- Manual paper sign-in sheets
- Individual PC based sign-in or scheduling software
- Centralized or networked authentication such as Active Directory, Novell, or ERS (Enterprise Resource Planning) system with a college/university wide identifier
- Pre-set or temporary authorization logins or guest cards handed out (please specify the length of time this is good for)
- Other (please specify)

13. How does the library handle user privacy of authentication?

- Anonymous access (each session is anonymous with repeat users not identified)
- Anonymous access (each session is anonymous with repeat users not identified)
- Identified access
- Pseudonymous access with demographic identification (characteristics of users determined but not actual identified)
- Pseudonymous access (repeat users identified but not the identity of a particular user)

14. When did you implement authentication of the PCs in the library public area?

- This year
- Last year
- 3-5 years ago
- 5-10 years ago
- Don't know

Student only PCs

15. Do you differentiate between Student Only PCs and Guest/Public Use PCs in the library public area?

17. How many PCs are designated for Student Only PCs in the library's public area?

18. Do you require authentication to access Student Only PCs in the library's public area?

19. What does authentication provide on a Student Only PC once an affiliated person logs in?

- Access to specialized software
- Access to storage space
- Printing
- Internet access
- Other (please specify)

20. Once done with an authenticated session on a Student Only PC, how is authentication on a PC removed?

- User is required to log out
- User is timed out
- Other (please specify)

21 What authentication issue have you seen in your library with Student Only PCs?

- ID management issues from the user (e.g., like forgetting passwords)
- ID management issues from the network (e.g., updating changes in timely fashion)
- Timing out issues
- Authentication system become not available
- Other (please specify)

Guest/Public PCs

22. How many PCs are designated for guest or public use in the library's public area?

23. Describe the location of these Guest/Public Use PCs.

- Line-of-sight to library service desk
- All In one general area
- Scattered throughout the library
- Other (please specify)
- In several groups around the library

24. Do you require authentication to access guest/public use PCs in the library's public area?

25. What does authentication allow for guest or the public that log in?

- Limited software
- Control, limit or block web sites that can be accessed
- Limited or different charge for printing
- Timed or scheduled access
- Internet access
- Other (please specify)
- Control, limit or block access to library resources (such as databases or other subscription based services)

26. Are there different type of PCs in your library area? Check those that apply.

- All PCs are the same
- Some have different type of software (like Browser Only)
- Some have time or scheduling limitation
- Some have printing limitations
- Some have specialized equipment attached (like scanners, microfiche readers, etc.)
- Some control, limit or block web sites that can be accessed
- Some control, limit or block access to library resources (such as database or other subscription based services)
- Other (please specify)

Wireless access

27. Do you have wireless access in your library public area?

28. Do you require authentication to your wireless access in the library public area?

29. Does the library have its own wireless policies different from the campus's policy?

30. What methods are used to give guests or the public access to your wireless access? Check those that apply.

- No access to guest or general public
- Paperwork and/or signature required before access given

- Limited access by time
- Open access
- Limited access by resource (such as Internet access only)
- Other

Incident Reports

31. Has your library had any known incidents of breach of privacy that you know about?

32. Has your library had any incidents of improper use of public PCs (such as cyber stalking, child pornography, terrorism, etc.?)

33. Have these incidents required investigation or digital forensics work to be done?

34. Who handled the work of investigation?

- Library IT or Library Systems staff
- IT or Campus Computing Center
- Campus Police
- Other Law Enforcement
- Unsure
- Other (please specify)

Computer Activity Logs

35. Do you know what computer activity logs are kept? (if unsure, end, if not ask)

- Authentication logs (who logged in)
- Browsing history (kept on PC after reboot)
- Browsing history (kept in centralized log files)
- Scheduling logs (manual or software)
- Software use logs
- None
- Unsure
- Other (please specify)

36 Do you know how long computer activity logs are kept?

- 24 hours or less
- Week
- Month
- Year
- Unknown

REFERENCES

1. Pam Dixon, "Ethical Risks and Best Practices," *Journal Of Library Administration* 47, no. 3/4 (May 2008): 157.

2. Scott Carlson, “To Use That Library Computer, Please Identify Yourself,” *Chronicle of Higher Education*, June 25, 2004, A39.

3. Lori Driscoll, *Library Public Access Workstation Authentication*, SPEC Kit 277 (Washington, D.C.: Association of Research Libraries, 2003).

4. Martin Cook and Mark Shelton, *Managing Public Computing*, SPEC Kit 302 (Washington, D.C.: Association of Research Libraries, 2007).

5. Diana Oblinger, “IT Security and Academic Values,” in *Computer and Network Security in Higher Education*, ed. Mark Luker and Rodney Petersen (Jossey-Bass, 2003): 1-13.

6. Code of Ethics of the American Library Association, http://www.ala.org/advocacy/proethics/codeofethics/codeethics

7. Fair Information Practices adopted by the Organization for Economic Cooperation and Development, http://www.oecd.org/sti/security-privacy

8. ”NISO Best Practices for Designing Web Services in the Library Context,” NISO RP-2006-01 (Bethesda, MD: National Information Standards Organization, 2006)

9. Dixon, “Ethical Issues Implicit in Library Authentication and Access Management.”

10. Howard Carter, "Misuse of Library Public Access Computers: Balancing Privacy, Accountability, and Security," *Journal Of Library Administration* 36, no. 4 (April 2002): 29-48.

11. Julie Still and Vibiana Kassabian, "The Mole's Dilemma: Ethical Aspects of Public Internet Access in Academic Libraries," *Internet Reference Services Quarterly* 4, no. 3 (January 1, 1999): 7-22.

12. Don Essex, "Opposing the USA Patriot Act: The Best Alternative for American Librarians," *Public Libraries* 43, no. 6 (November 2004): 331-340.

13. Lynne Weber and Peg Lawrence, "Authentication and Access: Accommodating Public Users in an Academic World." *Information Technology & Libraries* 29, no. 3(September 2010): 128-140.

14. Nancy Courtney, "Barbarians at the Gates: A Half-Century of Unaffiliated Users in Academic Libraries," *Journal of Academic Librarianship* 27, no. 6 (November 2001): 473.

15. Nancy Courtney, "Unaffiliated Users’ Access to Academic Libraries: A Survey," *The Journal Of Academic Librarianship* 29, no. 1 (2003): 3-7.

16. Barbara Best-Nichols, “Community Use of Tax-Supported Academic Libraries in North Carolina: Is Unlimited Access a Right?” *North Carolina Libraries* 51 (Fall 1993): 120-125.

17. Nancy Courtney, "Authentication and Library Public Access Computers: A Call for Discussion," *College & Research Libraries News* 65, no. 5 (May 2004): 269-277.

18. Rita Barsun, "Library Web Pages and Policies Toward “Outsiders”: Is the Information There?" *Public Services Quarterly* 1, no. 4 (October 2003): 11-27.

19. *American Library Directory : a Classified List of Libraries in the United States and Canada, with Personnel and Statistical Data,* 62nd ed. (New York: Information Today, 2009)

20. http://statelibrary.ncdcr.gov/ld/aboutlibraries/NCLibraryDirectory2011.pdf.

21. Karen Schneider, “So They Won’t Hate the Wait: Time Control for Workstations,” *American Libraries*, 29 no. 11 (1998): 64.

22. Code of Ethics of the American Library Association.

23. Karen Schneider, “Privacy: The Next Challenge,” American Libraries, 30, no. 7 (1999): 98.