

# The Panoptic Librarian: The Role of Video Surveillance in the Modern Public Library

David P. Randall<sup>1</sup> & Bryce Clayton Newell<sup>1</sup>

<sup>1</sup> University of Washington

## Abstract

Libraries have long maintained strong protections for patron privacy and intellectual freedom. However, the increasing prevalence of sophisticated surveillance systems in public libraries potentially threatens these core library commitments. This paper presents the findings of a qualitative case study examining why four libraries in the US and the UK installed video surveillance and how they manage these systems to balance safety and privacy. We examine the experience of these libraries, including one that later reversed course and completely removed all of its previously installed systems. We find that the libraries who install surveillance initially do so as either a response to specific incidents of crime or as part of the design of new buildings. Libraries maintain varying policies about whether video footage is protected as part of patron records, about dealing with law enforcement requests for footage, and whether patrons ought to maintain any expectation of privacy while inside libraries.

**Keywords:** privacy, surveillance, library, ethics, policy

**Citation:** Randall, D. P., & Newell, B. C. (2014). The Panoptic Librarian: The Role of Video Surveillance in the Modern Public Library. In *iConference 2014 Proceedings* (p. 508–521). doi:10.9776/14132

**Copyright:** Copyright is held by the authors.

**Acknowledgements:** The authors wish to thank Karen Fisher for her role in encouraging and guiding the early stages of this research project, Adam D. Moore for his comments and suggestions on earlier drafts, the participants in the 2013 iConference Information Privacy Workshop (where a portion of this work was presented, as well as the anonymous iConference reviewers for their insightful comments on the initial submission.

**Contact:** dpr47@uw.edu, bcnewell@uw.edu

## 1 Introduction

Video surveillance is an ever-increasing issue in modern society. More and more security cameras and other surveillance technologies such as drones, biometric recording, facial recognition and even genetic profiling tools are becoming prevalent in our everyday lives. As a result there is a very real struggle emerging between maintaining personal privacy and ensuring a certain level of security, as well as upholding the law. Current large-scale security systems with networked video cameras, expansive control rooms, roaming security guards, and the incorporation of other cutting edge technologies, can be compared to the Panopticon designs of the English social theorist Jeremy Bentham (Mike, 1990; Norris, 2003). The possibility that the modern public library, the with profession's long held commitment to privacy and intellectual freedom, could be compared to Bentham's panoptic prison in which the few – as largely unobservable observers – watch the many in an act of power and domination, is striking. If video surveillance has the potential to change power relationships between the state and its citizens (Forcese & Freeman, 2011; Webster, 1998) and negatively affect civil liberties, its implementation and management in the public library setting should be studied rigorously. Surprisingly, there is scant literature addressing the subject, and research that does largely ignores the important civil liberties issues.

Bentham's panoptic vision involved a centralized ability of those in power to monitor large numbers of others, who had no ability to watch back – and often had no idea when they were actually being watched. It is designed, according to Bentham, so as to effect “a new mode of obtaining power of mind over mind, in a quantity hitherto without example.” (Lyon, 2006) The design became the basis of Michel Foucault's theory of Panopticism, which examines the way discipline, power and punishment work in modern society (Foucault, 1977). Foucault demonstrated that “there is a reciprocal relationship between power and space” (Koskela, 2000), and argued that a city can be seen as a “laboratory of power” (Foucault, 1977; Koskela,

2000). Many surveillance theorists have moved beyond a religious adherence to Foucault's panopticism, but his theories continue to underlie much surveillance discourse (Lyon, 1994) and many have found parallels between surveillance-filled cities and Foucault's ideas (Ainley, 1998; Cohen, 1985; Fyfe & Bannister, 1996; Hannah, 1997; Herbert, 1996; Koskela, 2000; Soja, 1996; Newell & Randall, 2013). Recent research also suggests that the implementation of video surveillance may lead to urban "purification" and discriminatory "social sorting" (Lomell, 2002; Stalder & Lyon, 2003). Other research has found that video surveillance itself is not effective at preventing crime, and that the function of video surveillance, and the rationale behind its further implementation, has shifted away from crime prevention (an oft cited rationale for its initial implementation) to matters of national security and community or workplace safety, a form of surveillance creep (B. C. Newell & Randall, 2013; Stalder & Lyon, 2003; Webster, 2009).

The Panopticon necessitated a rigid architectural design, so as to achieve the goal of watching without being seen to be watching. However, today this panoptic goal can be achieved in almost any building, thanks to the prevalence of surveillance technologies. It is therefore very easy to draw a contrast between Bentham's designs and many modern public institutions that have adopted video surveillance technologies, such as public libraries.

This paper presents the findings of a study that we hope can begin to fill this void. We present original research findings from a study of the surveillance practices of four large libraries, one in the United Kingdom and three in the United States, in an effort to determine what factors and considerations have driven these libraries to start utilizing surveillance technologies and what repercussions library administrations have felt as a result of the installation of those technologies. This paper builds on and extends our earlier research in this area (B. C. Newell & Randall, 2013).

## 2 Background and Prior Research

### 2.1 Video Surveillance in Public Libraries

The International Federation of Library Associations and Institutions statement on libraries and intellectual freedom reads:

"Library users should have the right to personal privacy and anonymity. Librarians and other library staff should not disclose the identity of users or the materials they use to a third party" (IFLA, 1999).

In the United States, the American Library Association (ALA) annually celebrates its "Choose Privacy Week", and the ALA's Office for Intellectual Freedom has been actively promoting the recognition of privacy in the public library setting for some time. The ALA's position in regard to video surveillance is particularly enlightening:

"...high-resolution surveillance equipment is capable of recording patron reading and viewing habits in ways that are as revealing as the written circulation records libraries routinely protect.... Since any such personal information is sensitive and has the potential to be used inappropriately in the wrong hands, gathering surveillance data has serious implications for library management" (American Library Association, 2006) (emphasis added).

One library security report asserts that states best practice for libraries should be to implement physical security measures and perform risk assessments before moving to the installation of video surveillance systems, however the report goes on to state "[video surveillance] systems are quickly becoming one of the most important and economical security and safety tools available to libraries" (McComb, 2004), but does not even mention privacy considerations. Reports also suggest that video surveillance should only be employed to "provide a safe and secure facility for library employees, library resources and equipment, and library patrons" (McComb, 2004).

In the United Kingdom, the Chartered Institute of Library and Information Professionals' (CILIP) guidelines on privacy astutely state that the use of video surveillance in libraries “raises the question of where the balance of security and privacy should lie” (CILIP, 2011). The guidelines also state a serious concern that cameras are used as an “easy solution” by library administrators who don't take privacy into consideration and recommend that before cameras are installed at any library location that it should be:

“clearly established that CCTV is a solution to the problem and that there are not other effective solutions with less impact on privacy” (CILIP, 2011).

In 2008 CILIP issued a survey of police, surveillance and libraries within the UK in response to claims of increasing police requests for information on library users. The survey found that 75% of libraries responding received a request for patron information from a UK police force or the Security Service (aka MI5). 66% of libraries reported having a formal policy to deal with these requests, with an additional 13% only having a policy that addressed the Data Protection Act (1998). Interestingly only 9% of respondents felt that they were the victims of police engaging in “fishing” activities – looking for patron records without reasonable suspicion – and one library reported having a member of the Metropolitan Police Service's Special Branch approaching staff members and asking for them to report patrons visiting extremist websites directly to him. (CILIP, 2008). Indeed, it is surprising that little empirical research has been conducted to understand the role of video surveillance in the public library setting (B. C. Newell & Randall, 2013).

## 2.2 Video Surveillance and Crime Reduction

Studies analyzing the impact of cameras on crime rates have typically involved systems installed in publicly accessible urban areas such as city streets or shopping centers. Research has been conducted in a variety of locations, including the United Kingdom (Gill & Spriggs, 2005; Welsh & Farrington, 2002, 2004a), United States (Cameron, Kolodinski, May, & Williams, 2008; King, Mulligan, & Raphael, 2008; La Vigne & Lowry, 2011; Schlosberg & Ozer, 2007), and Europe (Lomell, 2002; Sætnan, Lomell, & Wiecek, 2002). Despite that fact that crime prevention has typically been the preferred policy basis for governmental and private installation of cameras (Webster, 1998), these studies generally indicate that video cameras have little or no statistical effect on incidents of crime (Biale, 2008; Webster, 2009; Welsh & Farrington, 2004b). Webster argues that video surveillance systems do not prevent crime and that the evidence base does not support the continued expansion and use of video surveillance on the basis of crime prevention alone (Webster, 2009). Webster and others have also argued that the purposes and uses of video surveillance systems have been shifting over time, becoming a normal and widely accepted aspect of modern society, allowing unabated diffusion of video surveillance systems regardless of the evidence that their oft-promised crime prevention capabilities may be mythical in actual practice, and despite serious implications for the civil liberties of the local citizens (Webster, 2009). The theory of “surveillance creep” is premised on the idea that “the policy focus of video surveillance has shifted as the technology has diffused, from crime prevention, to community safety and now also to national security” (Lyon, 1994; Webster, 2009).

## 2.3 Privacy and the Legal Basis for Governmental Surveillance

A number of federal court decisions in the United States have reaffirmed the right of government to monitor publicly owned spaces, as long the surveillance does not capture areas where a reasonable expectation of privacy (measured both subjectively and objectively) exists (United States v. Jones, 2012; United States v. Knotts, 1983). In some cases, however, federal courts found that video surveillance violated Fourth Amendment guarantees against unreasonable searches in middle school and police station locker rooms (Bernhard v. City of Ontario, 2008; Brannum v. Overton County School Board, 2008), as well as a shared physical education teachers office adjacent to a school locker room (Doe v. Dearborn Public Schools, 2008), because the respective plaintiffs maintained reasonable expectations of privacy in those spaces. However, the stronger legal basis for governmental surveillance in the public areas of a library, compared to the

obviously more private nature of locker rooms and personal office space, is based on the premise that individuals do not maintain any objective expectation of privacy in their conduct in these public spaces, and that these surveillance systems represent a valid use of state power to protect public safety (Nieto, 1997). As a result, video surveillance in these areas is generally permissible (Carson, 2010; Nieto, 1997; Sher, 1996).

Despite the fairly clear legal basis for video surveillance in libraries in the United States, legal scholars have also noted the potential chilling effects that such systems may have on speech in public spaces (Nieto, 1997; Sher, 1996; Slobogin, 2002). Some commentators have argued that, because video surveillance raises the problem of the “unobservable observer”, where the watched do not – or cannot – know who is watching or for what purpose, national or local policy ought to require more overt surveillance practices, public disclosure, and independent oversight of control rooms (Goold, 2002).

The United Kingdom has a similar view of surveillance in public spaces as the United States. During a 2008 House of Lords debate Lord Bassam of Brighton - spokesman for the Home Office and Attorney General – made the following statement:

“There are no legal restrictions on photography in a public place and no presumption of privacy for individuals in a public place. There are no current plans to review this policy.” (*House of Lords Debate*, July 16 2008)

In the UK the use of data collected by any video surveillance system is covered entirely by a single piece of legislation, the Data Protection Act (1998). The Data Protection Act’s remit is to cover any data held on an identifiable living person; this includes video surveillance in public places. The law was passed to bring the UK in line with the European EU Data Protection Directive (1995), but, unlike the EU Directive, the law itself makes no explicit reference to privacy. Under the Data Protection Act anyone using a CCTV system for any purpose other than protection of a private residence must register with the UK Information Commissioner’s Office (ICO). The role of the ICO is to make sure that institutions and business comply with the Data Protection Act and to protect the rights that individuals have under the act (*CCTV Regulations*, ICO, 2008).

Interestingly, unlike US law, which requires a court order in order for law enforcement to gain access to personal information held by a public body such as a library, under Section 29 of the Data Protection Act UK law enforcement agencies, can gain access to this information freely, without the involvement of a judge (*Data Protection Act*, HMSO, 1998). Specifically Section 29 states that personal data held for the purposes of the “prevention or detection of crime” or the “apprehension or prosecution of offenders” is exempt from the protections of the act. However, this would simultaneously appear to contradict elements of the UK Human Rights Act (1998), which upholds a British Subject’s the right to privacy, even in public spaces (Gras, 2002).

Following on from this prior research we will investigate a number of libraries to discover their surveillance practices, policies and interactions with local law enforcement in relation to cameras in order to answer the following research questions:

**RQ 1:** What factors do libraries take into account when they design, implement, or change official policies related to on-site surveillance practices?

**RQ 2:** How do libraries balance the privacy of their patrons with the safety and security of their employees, patrons and facilities?

### 3 Methodology

#### 3.1 Locations

We investigated the surveillance activities of a number of libraries in the United States (n=3) and the United Kingdom (n=1). In the U.S., we selected three libraries from two different states. Two of these were smaller urban libraries in a state in the American Southwest and one was a large county-wide library system in the Pacific Northwest. Each of these three libraries was chosen because of their proximity to the researchers at the time of the research, their willingness to participate, and the fact that they currently (or had previously) used video surveillance as a part of their security strategy. We also limited our selection to libraries that were members of the Urban Libraries Council. In the U.K., on the other hand, we investigated the video surveillance practices at a large special collections library, which was chosen because of its unique history of utilizing surveillance technologies, which we thought would provide an interesting contrast to the experience of libraries in the U.S.

ID	Location	Branches	Collection Size / Circulation	Service Pop.
A	US - Southern	1	180,000 / 1.4M	116,000
B	US - Southern	3	240,000 / 1.4M	113,000
C	US - Pacific North West	46	4.1M / 22.4M	2,000,000
D	United Kingdom	2	150M / NA	63,000,000

Table 1: Research Locations - Size, Circulation and Service Population

#### 3.2 Procedure

At each of the four libraries, the researchers conducted semi-structured interviews with library administrators and analyzed documents and emails available publicly or by request under local freedom of information laws. We used these methods to gather as much detailed information as possible about each library system's video surveillance policies and the reasons behind the implementation and changes made to those policies in succeeding years. All participants were fully aware of the library policies concerning video surveillance and were actively involved in the decision making processes involved in their operation, installation, and, in one case, the ultimate removal of the cameras. Following each interview, we requested additional library documents and emails related to the surveillance cameras under local freedom of information laws. We analyzed these documents thematically, comparing the data with our interview transcripts in an effort to help ensure trustworthiness and validity, and to attempt to triangulate our findings and conclusions.

### 4 Findings

#### 4.1 United States

##### 4.1.1 Library A

Both of the smaller urban libraries from the American Southwest (libraries "A" and "B", respectively) had security cameras installed at the time this research was conducted. Library A has only installed and maintained one single camera, located in a stairwell. The camera was installed to alleviate safety concerns

of library administration because the stairwell was otherwise an unmonitored area away from public (and staff) view. However, the feed has never produced any needed security footage as little unwanted behavior has reportedly occurred on the upper landing of the stairwell (the area under surveillance). The feed from the camera is displayed at a reference desk, and is visible to staff and patrons – although the screen is small and the display was not functioning properly when the researchers were visiting the library. The camera itself was installed as part of the overall plan and construction of the building, and not in response to any specific incident.

Library A also shares its building with City Hall. Because of the dual purpose nature of the building space, the city utilizes its own security cameras in the building's atrium (which serves as the main entrance to both the library and City Hall); these cameras overlook the library's entrance and can view portions of the ground floor area of the library near the entrance. Despite never using its own solitary camera footage for security purposes, Library A did report several incidents involving footage from the atrium cameras. For instance, the library administrator stated that footage from the atrium cameras had been utilized by the library to investigate and identify an individual suspected in "a chronic theft problem" and due to allegations made by patrons against other patrons or library staff members. In these cases, law enforcement requested footage from City Hall directly, although the library was made aware of the investigations. On other occasions, the police had requested atrium footage from library staff, who directed them to City Hall. Because the library does not control the atrium cameras, it is likely that other requests for footage have been made directly to the city without the library's knowledge.

The library does not have an official written policy dealing with the installation or use of video cameras, but the administrator noted that the city's general push towards increasing levels of surveillance and automatic police access to many city camera feeds might cause the library to seriously discuss the implementation of a policy in the future. This potential need would be especially pronounced, according to the library administrator, because any future location would be away from "the umbrella of City Hall," and the ban on concealed weapons afforded by the library's current location in the shared building. The administrator stated, "I suspect [we are] going to move more toward surveillance than away from it, just simply because of the active shooter issues, as [this] is a concealed handgun state," and the library has been actively preparing for active shooter incidents. Additionally, the administrator noted that there was no explicit policy detailing who could request footage or whether footage was part of the patron record, adding that "we need one."

Although the stairwell camera was primarily installed to ensure safety in the stairwell, the administrator stated that, "we default to privacy" when considering the impact of library security policies and practices. However, when asked about the proper role of video surveillance in the public library setting, a library administrator stated, "I am at war with myself" due to the competing safety and privacy concerns. The library also does not have any signs posted to inform patrons or other visitors about the presence of the stairwell camera, and no signs exist in the atrium area controlled by the city government either. This decision was purposeful, as the library was concerned that behavioral signage (also including "no smoking" signs) would be "counter to... how we want our space to feel."

Library A has also never had any issues with public backlash against the existing cameras in either the atrium or the stairwell. The administrator noted that, "what I'm observing from our patrons is that they care less about their privacy than we do." Additionally, as the library has begun talking with patrons about the option to have borrowing histories and search patterns saved, patrons have largely preferred the convenience over any risks to their own privacy. As a result, the library is concerned about "responding to [its] customers appropriately" as it considers new electronic services – so-called library 2.0 services.

#### 4.1.2 Library B

Library B, the second library from the American Southwest, has a network of cameras in each of its branches which they have introduced over the last 4 years. The cameras cover the circulations desks, the entrance to

toilet areas, and the exterior of the buildings. The cameras were installed on an as-needed basis, beginning with the main branch and then spreading to the other two locations, primarily to protect staff and patron safety. The library does not have a written video surveillance policy. They view the cameras to be a tool for “safety and security” and cooperate fully with local law enforcement.

The library has had several instances where they have used the cameras to prosecute crimes or identify persons who have been involved in disturbances in the library. In each case they voluntarily released the needed footage to local law enforcement and did not require a court-order as they do not consider the camera footage to be a part of the patron record. However, the library will not release footage to members of the public without law enforcement involvement. In terms of the library relationship with local law enforcement, the administrator stated, “we love law enforcement; anytime they want to come in [to the library] is fine with me.”

The library administrator noted that the cameras didn’t seem to create many privacy issues for patrons, and that the cameras at the circulation desks were positioned “so that they don’t catch titles, you can see the activity happening at the desk ... but it’s not clear enough, or close enough to see what it is exactly they [patrons] are doing.” In a public library, stated the administrator, “you don’t have an expectation of privacy.” The administrator also stated that libraries implement security camera systems to ensure safety, and that, “you have to work in [a library] to understand the reality of what it is to work in the public library... I’m all for privacy, but safety trumps.” At the time of the interview, several criminal prosecutions that relied on library video footage were underway in local courts, and despite the lack of conclusive information about whether the presence of cameras has deterred crime, the administrator noted that, “we certainly catch the thieves.”

In addition to their active cameras, the library has also placed several dummy cameras in certain locations in direct response to theft or unwanted activity. As stated by the administrator, “occasionally we have people stealing the newspapers, and we have dummy cameras over the childrens’ [and] teens’ video and audio books because we had a rash of thefts.” The library makes use of signage to warn patrons they are being recorded, some of these are located next to the dummy cameras. Additionally, the library has installed mirrors in various places and provides access to live video feeds at the public services desks to allow library staff to monitor the library space for unwanted activity. Although these feeds are not actively monitored, and cannot be accessed by the general public, staff does have access on demand to view the feeds. In addition the feeds can be accessed by any employee on any library workstation using specially installed software which also allows several of the exterior cameras to be remotely controlled. Moving forward, the library administrator stated that “it would be in our best interests to have the entire library covered [with cameras]... for safety... and I think that it makes sense that we should have a security camera focused on the children’s areas specifically.

#### 4.1.3 Library C

Library C is a large library system that includes both urban and rural library locations in the Pacific Northwest. Prior to May of 2011, 10 of the library’s 46 branch locations had camera systems installed. In May of that year, the administration simultaneously removed all of the cameras under their control. The library system no longer manages or operates any video surveillance cameras at any of its locations. However, one location, which maintained a video security system prior to its annexation into the county-wide library system, continues to have cameras installed on the exterior of its building, although these cameras are now run by the city government directly. Additionally, in early 2012, another city government independently installed cameras at a building that the library shares with that municipality’s City Hall.

The cameras at all 10 branch locations were generally installed in response to repeated incidents of crime occurring in and around library buildings. Cameras were installed in the first branches in the late 1990s, as branch managers responded to specific incidents of criminal activity or safety concerns. For instance, cameras were “used in some of the libraries before [staff] left the building to see if there was

anybody around the building, so [a staff member] could get to their car.” When the cameras were present, the library maintained a policy that all law enforcement requests for footage must be accompanied by a court order or subpoena. In our interview, the administrator noted, “We did give the video if it were after hours and there was no one in the parking lot... But if there was somebody in the parking lot, they could be using our WiFi... then we would still require the subpoena.”

The library maintained this policy because their interpretation of the library records exemption to the state public records act held that video footage was part of the patron record – a position backed by a legal opinion from the library’s attorney. However, this policy became a point of contention with multiple law enforcement departments. As the administrator in charge of handling requests stated:

“What [the police departments] would do is they would, you know, basically try to get the front line people to turn it over to them by making them feel bad that they weren’t helping them... solve this crime and so they put a lot of pressure on them.... It really is bullying behavior.”

Ultimately, library legal counsel expressed some reservations about whether footage from the exterior cameras was actually exempt under the library records exemption to state public disclosure law, leading the administration to admit that it was not “totally comfortable that [their interpretation of the library records exemption] would be upheld in the courts.”

The administration’s concern about the library’s use of the camera systems was an on-going issue, but the impetus for the decision to remove cameras came in March of 2011 when a conflict arose with a local police department after the library demanded that police obtain a court order before the library would turn over camera footage of an assault in the library parking lot. This particular situation became further aggravated when police finally obtained a court order for the footage a week later and publicly stated that they had apprehended the suspect, a known transient, within 15 minutes of an officer viewing the footage. Shortly after the March 2011 incident, the administration set up a team to conduct a “critical review of security cameras to gauge the impact and effectiveness of the cameras and whether they are appropriate to our mission of protecting patron privacy and confidentiality.” The administration also discussed the issue with their legal counsel and its library managers and conducted research into the effectiveness of video surveillance as a crime prevention tool. The administration announced its decision in a memo to library staff, which read, in part:

“We cannot argue with the sentiment that cameras make some people feel safer.... However, the potential impact to our mission to provide equal and open access to the library with protection of privacy and advocacy of intellectual freedom are too great to continue to provide security cameras.”

The library quickly removed all cameras under its control at its ten branches. Two branches continue to have cameras, but these are not owned, operated, or maintained by the library and do not primarily focus on the libraries.

## 4.2 United Kingdom

### 4.2.1 Library D

Library D has one central location and an additional location used to house part of its collection, this second location has a small reading room with limited public access. The central library has an extensive network of cameras. The library was built with an analogue system in the late 90s and a constant program of upgrades and expansion has been taking place ever since. The cameras cover both internal and external locations within the library grounds and the entire system is controlled from a central control room, manned 24/7, where feeds are only accessible to members of the library’s security team. However, there is one exception, feeds are shown to the public at the entrance to the library and the entrance to the reading



rooms. The library was designed with cameras in mind, following a philosophy that “the cameras will solve all of your problems.”

The library views its use of the CCTV cameras in three main ways. Firstly the cameras are used to maintain the libraries external perimeters so that the security can monitor access to the library site, particularly at night, “It’s not an un-scalable perimeter, we haven’t got prison walls, but it just a demarcation, there is our fence and if you come across our fence then we’re going to ask you what you’re doing.” The exterior cameras are motion activated at night, to assist security in identifying sectors where an intruder may be trying to scale the fence. The second element to the CCTV cameras is to monitor the public areas of the library and observe what is happening in the library. Cameras are installed in all areas of the library with the exception of public restrooms. The highest quality cameras are within the reading rooms and are constantly monitored. Here they provide backup to the security guards when they go to an incident. “The aim being that if I’m questioning you about something there is a camera watching what’s going on so that we have got a record of who threw the first punch.” The third level is the CCTV use within the reading rooms inside the library. The library has a number of different types of reading rooms, from low security to high security, as well as a specific room for scientific journals. In the high security reading rooms the camera density is much higher and the recordings are kept for longer as the library is trying to hold a record of “what happened at each desk at a particular day”. The lower security reading rooms merely have area surveillance and the feeds aren’t as high quality. All feeds from all cameras are kept for a minimum of 31 days and a maximum of 1 year. Data is stored on site on secure servers, which only the security team have access to.

Overall the library has a very limited level of active surveillance. The number of cameras and patrons far outnumbers the ability of the one or two on duty security officers to monitor everything. As a result the library views the cameras as “largely a historical record that can be used after something has been detected.” The security team’s main role in active surveillance is therefore to monitor the reading rooms for patrons breaking the code of conduct, for example using a pen in the reading rooms, which is strictly forbidden, and also to monitor exterior areas for thieves. The level of surveillance at the library is, as established, very high, even if the level of active surveillance is somewhat limited. Patrons who enter a reading room sign up to accept the term and conditions of entering that room, part of which is to accept being filmed by the cameras. The library considers there to be no expectation or right of privacy in the reading rooms in order for them to protect the integrity of the collection. However the library operates a strict Code of Practice that limits who is able to view footage, and how that footage should be handled, violation of that policy is a dismissible offence. Outside of the reading rooms, surveillance is much more cursory, security is handled mostly by roving guards.

The library is fully compliant with the Data Protection Act and as a result requires no court order or warrant from Police or the Security Services when they request video surveillance footage. Police will fill out a form and sign for the footage under Section 29 of the act to gain access to any material they so wish. This Section 29 interaction is the library’s primary, and usually only, direct interaction with law enforcement, with the exception of when staff may be asked to provide written statements due an incident that occurred on the premises. Most incidents of crime that occur on the library grounds are related to theft (personal theft and bike theft) and dealt with by the library security staff themselves without police involvement. The library uses a system called Facewatch which allows the security staff to upload information about a crime directly to the police, including witness statements, photos, and CCTV footage, the system then generates a crime reference number for the individual, enabling them to claim on insurance, and in the case of the theft of a wallet it will cancel all the victims credit cards. Since the library was opened, minor theft has been its main security issue, along with several serious assaults outside of the library recorded on their cameras. Only one major incident related to the reading rooms and directly

involving the police has occurred. That incident involved a book dealer removing and stealing pages from rare books.

## 5 Discussion

ID	Camera Status	Installation Reason	Primary Purpose of Camera	Requires Warrant?
A	Single Camera	Safety Concern at Building Construction	Specific Safety Issue	Yes
B	Multiple Cameras	Reactionary to Specific Incidents	Crime Prevention	No
C	None - All Removed	Reactionary to Specific Incidents	Staff Safety and Crime Prevention	Yes
D	Multiple Cameras	Safety & Preservation Concern at Building Construction	Preservation of Collection	No

Table 2: Research Locations - Findings Summary

In this paper, we have been particularly focused on the role of video surveillance in a public library setting, and the findings of this study provide consistency with and, in a few places, stark contrast to, the expected increase in the adoption and implementation of modern surveillance technologies in our society. The libraries studied in this research implemented video surveillance systems primarily in response to either 1) staff safety concerns related to criminal activity occurring in or around library buildings or 2) general plans to construct new library buildings. In some cases, library staff ultimately utilized the cameras for various other purposes as well, including ensuring patron and employee safety and protecting library property. This finding is consistent with the idea of “surveillance creep”; that is, that the controllers of the surveillance systems begin to use the systems in ways not originally planned for or considered.

Our research shows a clear variety in the interpretation of how video footage is treated by different library systems. Libraries A and C both erred more on the side of privacy, although Library C was very explicit about this in regards to video footage, library A’s one camera setup restricted their need for an established policy, although they indicated that the installation of more cameras would force them to head in that direction. Conversely Libraries B and D had a different view, for Library B this was down to the choice of the library system itself, deciding to fully cooperate with law enforcement requests for footage - although purposefully designing their camera setup to not capture patron borrowing details where possible. In the case of Library D their policies are enshrined in law, nothing is privileged, their cameras are even capable of capturing handwritten notes made when reading a book. Furthermore the seeming contradiction between the Data Protection Act and Section 8 of the Human Rights Act in relation to privacy in public places is of some concern. The library essentially makes patrons give up their right to privacy in order to access a public institution, which by definition the public should have a right to freely use. It is in fact very troubling that UK law enforcement agencies have such ready access to patron information, not limited to CCTV footage but also to borrowing records, without there being any requirement for probable cause or judicial review.

## 6 Limitations and Direction for Future Research

The primary limitation of this study has been its scope, while we have a number of institutions within the U.S., we have only one within the U.K., and the U.K. library, as a special collections library, is not directly comparable with the more general purpose mission of the others. With the established differences in legislation and practices between the two countries, a more expansive study is required. This is also true of the number of libraries studied in the U.S., and in future research we hope to research libraries from more regions of the country. Additionally, our research is limited to information provided by library administrators and publicly accessible documents, and does not represent the views of library patrons, or even library staff members more generally.

In the future, we intend to pursue additional research into the effects of video surveillance on library access for poor and underserved populations that may be particularly impacted by library surveillance, and to conduct research with additional libraries that have implemented video surveillance systems. Expanding our current findings in these ways will enable us to make claims that are generalizable beyond the scope of this current study, gain a broader and more comprehensive understanding of the issues involved when libraries implement video surveillance, and further triangulate our data collection and analysis efforts. Because of differing theoretical definitions and practical approaches to the concept of privacy across national boundaries (Newell, 2011), we are also planning to extend our study to look at other countries in Europe and North America.

## 7 Conclusion

Library surveillance may take many forms, including traditional reading and borrowing histories, RFID tracking, e-book borrowing choices visible to outside vendors like Amazon and Barnes and Noble, electronic and web-based communication and interaction between patrons and library staff, Internet browsing histories, and video surveillance. The accumulation and aggregation of these forms of surveillance data can potentially pose a threat to the privacy of library patrons and staff in conflict with library commitments to privacy and intellectual freedom, especially if libraries do not establish policies to ensure prompt deletion or when local or national laws may not adequately protect all these forms of library records. The idea that “cameras will solve all your problems,” without more, is disingenuous, and without adequate protections for personal information privacy in public spaces (including privacy in information accessible through aggregation of data captured by a variety of surveillance mechanisms), library commitments to intellectual freedom and patron privacy are tested and stretched to their limits.

Surprisingly, libraries inconsistently adopted written or explicit verbal policies outlining the installation and use of video surveillance systems. The libraries in this study also differed in their conclusions about whether surveillance footage should be considered part of a patron record and protected from disclosure absent court order or some other judicially sanctioned process. The libraries also approached their working relationships with local law enforcement quite differently and, due perhaps partly to more restrictive policies for releasing footage to police, one library ultimately decided it was in its best interests to remove its entire video security system from 10 branches.

The adoption of surveillance technologies and the culture within the United States and the United Kingdom exhibit some similarities (e.g. little privacy protections for individuals in public spaces) as well as some historical and legal differences. In the United Kingdom, legislation requires very strict policies and protections for data on individuals, while at the same time allowing law enforcement to act to retrieve such data without probable cause. It's perhaps most revealing that the comprehensive law providing protection of personal data within the United Kingdom does not once use the word 'privacy' within its statutes. The continued and unclear application of Section 8 of the Human Rights Act (1998) in relation to personal data is also a contentious issue, especially in regards to its use in conjunction with the Data Protection Act.

It is clear that surveillance in public libraries is an expansive topic, of which this study only begins to scratch the surface. It is hoped that continued study and a greater expansion of this research will help to reveal the extent to which the privacy of library patrons in Europe and the United States is protected, and perhaps reveal potential holes that legal and policy reforms ought to address. In particular, lawmakers need to craft and adopt clear and precise legal provisions outlining the extent to which video surveillance footage is part of the patron record and ought to be protected from disclosure (to law enforcement or the general public). Additionally, libraries should be transparent about their surveillance activities by posting signs and alerting patrons to the presence of cameras, and should maintain written policies outlining the extent of video surveillance, policies related to the retention and destruction of recorded footage, the potential uses of video footage, and the processes and procedures required prior to disclosure to third parties, including law enforcement. Ideally, these policies would generally require judicial authorization (e.g. a warrant or court order) prior to allowing police access to footage that could potentially reveal a great deal about patron browsing and borrowing activities.

## 8 References

- Ainley, R. (1998). Watching the detectors: control and the Panopticon. In *New Frontiers of Space, Bodies and Gender*. (pp. 88–100). London: Routledge.
- American Library Association. (2006). Questions and Answers on Privacy and Confidentiality. Retrieved from <http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15347>.
- Bernhard v. City of Ontario. (2008).
- Biale, N. (2008). Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found. *American Civil Liberties Union*. Retrieved August 15, 2013, from <http://www.aclu.org/privacy/35775res20080625.html>
- Brannum v. Overton County School Board. (2008).
- Cameron, A., Kolodinski, E., May, H., & Williams, N. (2008). Measuring the effects of video surveillance on crime in Los Angeles. *California Research Bureau Report CRB-08-007*.
- Carson, B. M. (2010). The Legal Basis for Library Video Surveillance. *Against the Grain*, 22(5), 52–54.
- CCTV Regulations (2008). Information Commissioner's Office. Retrieved from [http://www.ico.gov.uk/for\\_organisations/data\\_protection/topic\\_guides/cctv.aspx](http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx)
- CCTV. (2008). CILIP Survey on Police, Surveillance and Libraries, June 2008, 1–7.
- CILIP. (2011). *User Privacy in libraries - guidelines for the reflective practitioner*. Retrieved from [http://www.cilip.org.uk/sites/default/files/documents/Privacy\\_June\\_AW.pdf](http://www.cilip.org.uk/sites/default/files/documents/Privacy_June_AW.pdf)
- Cohen, S. (1985). *Visions of Social Control: Crime, Punishment and Classification* (p. 336). Cambridge: Polity.
- Doe v. Dearborn Public Schools. (2008).
- Force, C., & Freeman, A. (2011). *The laws of government: the legal foundations of Canadian democracy*. Irwin Law.
- Foucault, M. (1977). Discipline and punish: The birth of the prison, trans. *Alan Sheridan (New York: Vintage, 1979)*, 227.
- Fyfe, N., & Bannister, J. (1996). City watching: closed circuit television surveillance in public spaces. *Area*, 28(1), 37–46.
- Gill, M., & Spriggs, A. (2005). *Assessing the Impact of CCTV*. Home Office Research Study 292. Home Office Research, Development and Statistics Directorate.
- Goold, B. (2002). Privacy rights and public spaces: CCTV and the problem of the “unobservable observer.” *Criminal Justice Ethics*, 21(1), 21–27.

- Gras, M. (2002). The legal regulation of CCTV in Europe. *Surveillance & Society*, 2(2/3), 216–229.
- Hannah, M. (1997). Imperfect panopticism: Envisioning the construction of normal lives. In *Space and social theory: Interpreting modernity and postmodernity* (pp. 344–59).
- Herbert, S. (1996). The geopolitics of the police: Foucault, disciplinary power and the tactics of the Los Angeles Police Department. *Political Geography*, 15(1), 47–59.
- HL Deb 16 July 2008, vol 703, col 1241. (n.d.).
- HMSO. Data Protection Act (1998). C.29. UK Parliament.
- IFLA. (1999). *Statement on Libraries and Intellectual Freedom*. Retrieved from <http://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom>
- King, J., Mulligan, D., & Raphael, S. (2008). CITRIS Report: An Evaluation of the Effectiveness of the City of San Francisco's Community Safety Cameras. In *Available at SSRN 2183381*.
- Koskela, H. (2000). "The gaze without eyes": video-surveillance and the changing nature of urban space. *Progress in Human Geography*, 24(2), 243–265. doi:10.1191/030913200668791096
- La Vigne, N., & Lowry, S. (2011). Evaluation of camera use to prevent crime in commuter parking facilities: a randomized controlled trial. *Technical Report of The Urban Institute Justice Policy Center*.
- Lomell, H. . (2002). Targeting the unwanted: Video surveillance and categorical exclusion in Oslo, Norway. *Surveillance & Society*, 2((2/3)), 347–361.
- Lyon, D. (1994). *The Electronic Eye: The Rise of the Surveillance Society*. U of Minnesota Press.
- Lyon, D. (2006). The search for surveillance theories. In *Theorizing Surveillance: The panopticon and beyond* (pp. 3–20).
- McComb, M. (2004). *Library Security*. San Francisco: RLS Inc.
- Mike, D. (1990). *City of quartz: excavating the future in Los Angeles* (pp. 223–236, 261–263). Verso.
- Newell, B.C. (2011). Rethinking Reasonable Expectations of Privacy in Online Social Networks. *Richmond Journal of Law and Technology*, 17(2).
- Newell, B. C., & Randall, D. P. (2013). Video Surveillance in Public Libraries: A Case of Unintended Consequences? In *System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences* (pp. 1932–1941). IEEE. doi:10.1109/HICSS.2013.595
- Nieto, M. (1997). *Public video surveillance: is it an effective crime prevention tool?* Sacramento, CA: California Research Bureau, California State Library.
- Norris, C. (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 249–281).
- Sætnan, A., Lomell, H., & Wiecek, C. (2002). Controlling CCTV in public spaces: Is privacy the (only) issue? Reflections on Norwegian and Danish observations. *Surveillance & Society*, 2(2/3), 397–415. Retrieved from <http://megafotos.ru/-NZbGlicmFyeS5xdWVlbnN1LmNhZN-ojs/index.php/surveillance-and-society/article/view/3385>
- Schlosberg, M., & Ozer, N. (2007). Under the Watchful Eye: The Proliferation of Video Surveillance Systems in California. *American Civil Liberties Union*.
- Sher, S. (1996). Continuous Video Surveillance and Its Legal Consequences. *University of California, Hastings College of the Law*.
- Slobogin, C. (2002). Public privacy: Camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, 72.
- Soja, E. (1996). *Thirdspace: Journeys to Los Angeles and other real-and-imagined places*. Oxford: Maxwell.

- Stalder, F., & Lyon, D. (2003). Electronic Identity Cards and Social Classification. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (pp. 77–93). London: Routledge.
- United States v. Jones 132 S. Ct. 945. (2012).
- United States v. Knotts 460 U.S. 276. (1983).
- Webster, C. (1998). Changing relationships between citizens and the state: the case of closed circuit television surveillance cameras. *Public Administration in an Information Age: A Handbook. Informatization Developments and the Public Sector Series*, (6), 79–96.
- Webster, C. (2009). CCTV policy in the UK: Reconsidering the evidence base. *Surveillance and Society*, 6(1), 10–22.
- Welsh, B., & Farrington, D. (2002). *Crime prevention effects of closed circuit television: a systematic review*. (Vol. 252). London: Home Office.
- Welsh, B., & Farrington, D. (2004a). Evidence-based crime prevention: The effectiveness of CCTV. *Crime Prevention & Community ...*. Retrieved from <http://www.palgrave-journals.com/cpcs/journal/v6/n2/abs/8140184a.html>
- Welsh, B., & Farrington, D. (2004b). Evidence-based crime prevention: The effectiveness of CCTV. *Crime Prevention & Community ...*, 6(2), 21–33.

## 9 Table of Tables

Table 1: Research Locations - Size, Circulation and Service Population.....	512
Table 2: Research Locations - Findings Summary .....	517