8-2013

Analysis of Ethical Management Policies for use of CCTV on College Campuses

Jeannine M. Jennette
St. John Fisher College

Analysis of Ethical Management Policies for use of CCTV on College Campuses

Abstract

This dissertation analyzed the policies of colleges in the Mid-Atlantic United States as they relate to the ethical use of surveillance cameras on college campuses. The quantitative study surveyed security professionals at these colleges to assess how each college developed, deployed, and integrated CCTV policies related to securing video data, safeguarding privacy, and prevention of the potential for the unethical use of surveillance cameras. This research used the Baldrige Criteria Scoring System to develop questions for the survey related to the Approach, Deployment, Learning, and Integration of each college's policies. The findings of this research will enable colleges to develop standardized best practices to use when developing ethical use of CCTV policies. The analysis of the survey responses determined that less than 50% of the colleges participating in the study actually had a written CCTV policy. Many of the policies that colleges did have, failed to include mandated training of personnel, or provisions ensuring that their policies remained up-to-date. The results indicated that all types of colleges, public and private, two-year and four-year, lacked consistent and comprehensive policies regulating the use of CCTV on their campuses.

Document Type

Dissertation

Degree Name

Doctor of Education (EdD)

Department

Executive Leadership

First Supervisor

Richard Maurer

Second Supervisor

Debra Thomas

Subject Categories

Education

Analysis of Ethical Management Policies for use of CCTV on College Campuses

By

Jeannine M. Jennette

Submitted in partial fulfillment

of the requirements for the degree

Ed.D. in Executive Leadership

Supervised by

Dr. Richard Maurer

Committee Member

Dr. Debra Thomas

Ralph C. Wilson, Jr. School of Education
St. John Fisher College

August 2013

Dedication

This dissertation is dedicated to my family, friends, colleagues, and Coach who have encouraged me and sacrificed so I could complete this journey.

To my Committee and Advisor: the advice and counsel provided by my Committee Chair, Dr. Richard Maurer, Committee Member Dr. Debra Thomas, and Advisor Dr. Ronald Valenti made this journey possible. Thank you for always being available with advice and support.

To my colleagues: this would not have been possible without your feedback, support, and understanding that allowed me to dedicate the time to complete my research.

To my sisters, brother, and extended family: your understanding of all the missed events, interest in my research, and broad shoulders to lean on, were instrumental in helping me reach my educational goals. Thank you for always being there for me.

To Coach: the best study buddy. Always under the desk at my feet making sure I finished my work, even though you would rather go for a walk.

To my daughter Chris and son Phil: your unwavering support, encouragement, and sacrifice these past two years gave me the strength to pursue my doctoral degree. We have been through a lot together and you have both become amazing adults. I love you both unconditionally.

Finally to my Father and late Mother: for instilling the importance of hard work and higher education. Dad, thanks for always showing such pride in me and for making me feel like I can do anything. I think Mom would have been proud too.

Biographical Sketch

Jeannine M. Jennette is currently the Executive Director of Public Safety at Columbia University in the City of New York. Ms. Jennette attended the State University of New York, Empire State and graduated with a Bachelor of Science degree in in 1998. She attended Marist College from 1998 to 2000 and graduated with a Master of Public Administration degree in 2001. She came to St. John Fisher College in the summer of 2011 and began doctoral studies in the Ed.D Program in Executive Leadership. Ms. Jennette pursued her research in the ethical use of CCTV cameras on college campuses under the direction of Dr. Richard Maurer and Dr. Debra Thomas and received the Ed.D. degree in 2013.

Abstract

This dissertation analyzed the policies of colleges in the Mid-Atlantic United States as they relate to the ethical use of surveillance cameras on college campuses. The quantitative study surveyed security professionals at these colleges to assess how each college developed, deployed, and integrated CCTV policies related to securing video data, safeguarding privacy, and prevention of the potential for the unethical use of surveillance cameras. This research used the Baldrige Criteria Scoring System to develop questions for the survey related to the Approach, Deployment, Learning, and Integration of each college's policies. The findings of this research will enable colleges to develop standardized best practices to use when developing ethical use of CCTV policies. The analysis of the survey responses determined that less than 50% of the colleges participating in the study actually had a written CCTV policy. Many of the policies that colleges did have, failed to include mandated training of personnel, or provisions ensuring that their policies remained up-to-date. The results indicated that all types of colleges, public and private, two-year and four-year, lacked consistent and comprehensive policies regulating the use of CCTV on their campuses.

Table of Contents

List of Tables

Chapter 1: Introduction

Introduction

In 2011, college campuses like many cities in the United States were the sites of protests related to the "Occupy Wall Street" movement (Wollen & Harris, 2011). Video footage of student protests at Harvard, Berkeley, and other campuses were shown nightly on the local news stations. This video immediately appeared around the world via social networking sites such as Facebook, Twitter, and YouTube. The United States constitution protects the rights of private citizens and the media to videotape and broadcast these events taking place in public locations. What about surveillance camera video recorded by colleges on their campuses, should this also be available for broadcast? Is it appropriate for colleges and universities to make video of incidents involving their student population, such as peaceful protests, available to the public, or should strong safeguards exist to protect the students' right to privacy on their college campuses?

Should video recorded by the colleges, primarily installed as a crime prevention measure, be used to identify students participating in lawful demonstrations, or other normal college functions? What if unethical operators of the university owned surveillance systems, released video to a social media site, such as YouTube, because the video was humorous, embarrassing, or controversial?

This research explored the ethical use of video surveillance technologies by colleges and universities in the United States. The researcher synthesized the relevant

literature and theoretical frameworks related to surveillance monitoring on college campuses and conducted an in-depth study of the ethical use of video surveillance.

Analyses were conducted on the existing literature published on the topic of Closed Circuit Television Cameras (CCTV) and video surveillance related to camera use by college campuses as a crime prevention method (Armitage, 2002; Clarke & Felson, 1993; Honess & Charman, 1992; Welsh & Farrington, 2002). Additionally, CCTV policies currently in use by colleges in the United States and United Kingdom were reviewed to assess the industry best practices related to surveillance cameras.

These analyses were used to design an Internet-based survey instrument designed to evaluate how colleges develop, deploy, and integrate CCTV policies on their campuses. The survey participants were Security and Public Safety professionals at colleges and universities located in the Mid-Atlantic region of the United States. Additionally all colleges were members of the International Association of College Law Enforcement Administrators (IACLEA). This research survey compared data on the actual policies and practices currently implemented by college and university on their campuses. Using this data, the security professionals may develop industry-wide best practice standards for the design of college CCTV surveillance policies.

Problem Statement

The problem that this research focused on is how colleges developed, deployed, evaluated, and integrated policies related to the ethical use of CCTV on their campuses. Each educational organization must develop their own policies for the ethical monitoring and use of CCTV technology and the data collected by these systems. The lack of industry-wide CCTV standards to guide colleges and universities in the ethical use of

video surveillance technology results in vastly differing policies and criteria for the security of the video data, and the prevention of potential unethical use of surveillance cameras. The hypothesis or starting point for this research was that a strong well-developed policy, based on a standardization of industry-wide best practices will prevent, detect, or deter the unethical use of video surveillance equipment and data in a university setting.

Theoretical Rationale

The study analyzed routine activities theory, rational choice theory, and social learning theory looking at the ethical arguments related to video surveillance, ethics, and privacy. First, the researcher examined the theoretical rationale for the use of video surveillance technologies as a crime prevention tool. Next, the researcher analyzed how the same criminological theories used to justify installation of CCTV systems to combat crime, rational choice, and routine activities theory, can be used to explain instances of unethical behavior committed by CCTV surveillance system operators.

Statement of Purpose

This study evaluated colleges' current practices and policies for the ethical use of video technology using an Internet based survey completed by experts in the college security field. The study analyzed the development, deployment, learning, and integration of actual policies used to guide the ethical use of CCTV on college campuses. These results of this study will allow practitioners in the field to assess or develop their own policies related to the ethical use of camera systems. This research has potential significance because prior research in this field was limited. This study identified potential gaps in current policies and recommended areas of improvement for use by

security professionals in the development of ethical use policies for college and university surveillance systems.

Research Questions

The five research questions this study answered are as follows:

1. How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campuses?

2. How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel?

3. How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff populations?

4. How do colleges ensure that their CCTV policies remain up to date as technology and university needs change?

5. How do colleges integrate their university's ethical use of CCTV policies with their university's other ethical policies, such as sexual harassment and discrimination?

Hypotheses. An analysis of the survey data was conducted using Chi-squared Test for Independence and logistical regression to test the following five null hypotheses:

Null Hypothesis 1 (*Ho1*): There is no significant difference between the type of school and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 2 (*Ho2*): There is no significant difference between campus location (metropolitan, urban, urban-adjacent, and rural) and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 3(*Ho3*): There is no significant difference between the type of security personnel (sworn, unsworn, mix of sworn and unsworn) and the frequency of negative response to having a CCTV policy.

Null Hypothesis 4 (*Ho4*): There is no significant difference between the number of students enrolled at a college and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 5 (*Ho5*): There is no significant difference between the number of cameras a college has installed on campus and the frequency of negative responses to having a written CCTV policy.

Significance of the Study

Colleges and universities are investing resources installing and monitoring CCTV camera systems on campuses. These schools must hire and train personnel to monitor these camera systems, used to protect their campuses, yet there are no industry-wide standards for the ethical use of these cameras. This study will enable creation of industry-wide best practices for the development, deployment, evaluation, and integration of policies related to the ethical use of CCTV on college campuses. Previously, each institution had to determine if a policy on the ethical use of cameras was necessary for their institution. Universities may now choose whether to develop and implement their own ethical use policies or use this studies findings to develop best practices. The design of these policies should; protect the data recorded from the cameras; restrict unethical or inappropriate use by their employees; and prevent exposure to civil liability incurred as the result of the unauthorized use or distribution of the data.

Ethical use of technology such as CCTV is an emerging problem. Like many new computer technologies, there is a lack of existing policies regulating how these new technologies should be used. Often, organizations attempt to use existing policies that inadequately address conduct related to new and rapidly growing technologies (Moor, 1985). "What is needed in such cases is an analysis that provides a coherent conceptual framework within which to formulate a policy for action" (Moor, 1985, p. 266).

Universities and colleges do not differ from private businesses or government agencies on the need to formulate strong ethical use policies for their CCTV systems. These policies should strictly regulate the conduct of those operating and monitoring these video surveillance systems and protect the recorded data. The potential impact, both positive and negative, of a university monitoring public spaces using CCTV, and a person's expectation or right to privacy while in these public spaces was appropriate and topical subject for this study.

Definitions of Terms

The terms related to the use of CCTV, cameras and surveillance technology are derived from the reported best practices of professionals in the field of college security.

Baldrige Criteria Scoring System. The scoring system is organized around four dimensions of Approach, Deployment, Learning, and Integration.

CCTV. Camera surveillance will be used as interchangeable with the notions of video surveillance and Closed Circuit Television (CCTV) (Dubbeld, 2003).

Control room. The facility used by the owner of surveillance technologies, college, police, or private business, to monitor the cameras and direct response to incidents observed on the CCTV screens.

Ethical behavior. "Ethical behavior is that which is morally accepted as 'good' and 'right' as opposed to 'bad' or 'wrong' in a particular setting" (Sims, 1992, p. 506). This would include the use of a video surveillance system, and the data the system records, only for its intended or lawful purpose. Ethical use of a surveillance system would prohibit any private use or illegal monitoring of persons or places.

Information gathering. A term used to encompass the wide variety of ways to find out what people are doing, thinking, or planning (Solove, 2011a).

Mid-Atlantic Region. A demographic area of the United States, as defined by the International Association of Campus Law Enforcement Administrators (IACLEA). The member States are New York, New Jersey, Delaware, Ohio, Pennsylvania, West Virginia, Maryland, Washington D.C., and Kentucky.

Policy. Provides guidelines, regulations, or the like, to achieve change (Fitzpatrick, Sanders, & Worthen, 2011).

Privacy. Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve (Westin, 1967). Respect for private life, family, property, and correspondence (Taylor, 2002).

Surveillance. Any focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction (Lyon, 2007).

Video surveillance. The continuous, systematic, and remote monitoring of people, and spaces, using video technology. Typically consists of a camera with a zoom lens; a recording device such as a digital video recorder (DVR); and a monitor that displays recorded images for real-time or subsequent viewing (Yesil, 2005).

Chapter Summary

Video surveillance technology is used by colleges, universities, public and private agencies throughout the United States. The surveillance system owners installed these systems with the intent of using the data recorded on these camera systems for the purposes of crime prevention and life safety (Armitage, 2002). Yet, there is little or no standardization of policies or regulations related to the installation or use of these systems.

College security professionals are responsible for the safety and security of the students, faculty, staff, and visitors who live on, and use the college campuses. Video surveillance has become a commonplace method of crime prevention on many college and university campuses, yet little regulation or oversight existed to prevent the misuse of recorded video data (Schlosberg & Ozer, 2007). Without strong policies, the potential for unethical use by control room operators and monitors will continue to exist (Cohen & Felson, 1979). This research focused on the development of industry-wide best practice recommendations enabling university, and college security professionals to assess the appropriateness of their current ethical use of CCTV technology policies and develop new policies were appropriate.

Chapter 2: Review of the Literature

Introduction and Purpose

A review of the literature revealed conflict between the crime prevention experts and privacy advocates. Hier and Greenberg (2009), and Hier, Walby, and Greenberg (2006) advocated the use of CCTV cameras to address various social problems such as crime, fraud, and terrorism. These researchers maintained that surveillance methods, including CCTV used by the government, should remain unregulated. They further endorsed a perception that any disagreement with public surveillance is dangerous to the safety of the United States, and therefore supportive of terrorists. This perception differed from the research of Schlosberg and Ozer (2007) that specifically addressed the threat posed by public video surveillance on an individual's right to privacy and an erosion of civil liberties, despite law enforcement's justification for these surveillance programs.

The literature identified potential conflicts and trends in both ideologies and research methods used by researchers to study the use of CCTV cameras and video surveillance. These research conflicts, analyzed through technological and philosophical lenses, were evaluated in this study to assess the value of video surveillance's use as a crime prevention/apprehension tool. Researchers contend that continued use of CCTV without ethical use policies, by government or private organizations, such as colleges and universities, would affect an individual's right to privacy (Dubbeld, 2003; Schlosberg & Ozer, 2007). Schlosberg and Ozer's (2007) study compared intended uses of CCTV as a

crime prevention method, to the potential loss of an individual's privacy through unethical use of CCTV surveillance technology. They contend that there is little correlation between installation of cameras and a decrease in crime.

A recent study of San Francisco's existing CCTV legislation conducted by King, Mulligan, and Raphael (2008) firmly supported implementation of reasonable oversight, as successfully balancing the needs of law enforcement, and the privacy rights of an individual. According to Goold (2006), the United States lags behind countries such as the United Kingdom in terms of the number of cameras placed in public spaces. If the current trend of rapid expansion of CCTV continues in the United States, it will only be a matter of time before we see cameras on virtually every street corner, in our parks, and throughout our public transportation system (Goold, 2006).

Although in the United States courts have not yet regulated CCTV or public surveillance under the First or Fourth Amendments, Goold (2006) supports local and state legislatures imposing their own restrictions on use of this technology. The indecisiveness of federal and state legislatures appeared to support the unregulated use of cameras by the police and other parties, therefore intimating support for further growth of public surveillance technology.

In 2006, New York City Police Commissioner Raymond Kelly began installing a surveillance network consisting of over 500 private and government owned cameras, license plate readers, and roadblocks in Lower Manhattan (Mullins, 2006). Mullins noted this "Ring of Steel," modeled after a similar strategy used for years in London, was created so every vehicle and person entering the area below 14th Street in Manhattan, is videotaped, and monitored by the New York City Police Department (NYPD). Operators

assigned to a video control center report suspicious vehicles or activities to NYPD personnel who respond, investigate, and apprehend the offenders. Additionally, cameras monitor and record the daily activities of private citizens as they drive, walk, or work in this area, and that data is stored for police department review in the event any incident occurs (Mullins, 2006). Successful use of CCTV, as a crime prevention method, relies on observations by a control room operator monitoring the cameras, properly identifying suspicious behavior, and their ability to direct responding officers to a location so those officers may apprehend the suspect (Hier et al., 2006).

Review of the Literature

Although blanketing every corner with CCTV as a method of public surveillance is widely used, privacy advocates criticize the excessive use of cameras, with little or no regulatory oversight, as intrusive on a citizen's rights to privacy (Hempel & Topfer, 2004). Moreover, some view the excessive deployment of this technology as an unproductive use of economic resources and vulnerable to abuse by the organizations monitoring the cameras (Hier & Greenberg, 2009).

Concerns over the potential for improper use of the video feeds from the cameras resulted in a few municipalities, such as the City of San Francisco, passing legislation regulating the use of security cameras (King et al., 2008). San Francisco's Community Safety Camera Ordinance of 2006 (CSC, 2006), limits government and private access to recorded data, restricts the length of time video data may be stored, requires community input on placement of any new cameras, and mandates annual reporting of crime statistics to justify the continued use of cameras at each location (King et al., 2008).

A review of the literature related to the effectiveness of cameras revealed that the usefulness of CCTV as a crime prevention tool is unsettled. Cameras are supported by some experts as a successful tool for crime prevention and invaluable for the apprehension of criminals (Horne, 1996). Others claim cameras are a waste of limited financial resources, have little documented success at combating crime, and affect the right to privacy of those under observation (Davies, 1996). Interestingly, the analysis revealed that individuals on both sides of the CCTV argument might suffer from technological determinism. Each side shares a belief that technology and not the actions of people, has an impact on crime, or affects an individual's right to privacy (Norris & Armstrong, 1999). The validity of technological determinism is not supported by research, which reports that the success of cameras in combatting crime is directly related to the active monitoring of these cameras by live camera operators not merely the installation of cameras (La Vigne, Lowry, Markman, & Dwyer, 2011).

The literature review revealed potential weaknesses in the methodologies of some of the research. These studies were conducted without using experimental control areas comparing the success of the camera installation on crime in one area, to a similar area without intervention (Taylor E., 2010). Other studies ignored interventions besides the cameras, such as increased street lighting, that were occurring in the area of observation during the studies (Welsh & Farrington, 2002). Additionally, some studies conducted for a relatively short period after the initial installation of cameras, did not collect data for a long enough time, to determine the full effect of the cameras on crime. Finally, these studies did not fully investigate whether the initial effect of the camera installation would dissipate over a period of time (Welsh & Farrington, 2002).

Since 2000, researchers have conducted few research studies evaluating the success of CCTV systems despite the increased installation of cameras in recent years. The one major study conducted by Gill and Spriggs (2005) reported that only one out of 14 CCTV systems had any significant impact on crime in the areas installed. Yet installation of large CCTV systems recording the daily routines of private persons in public places continues in cities throughout the world (Taylor E., 2010).

Privacy is an often-mentioned topic in the literature related to any discussion of CCTV monitoring (Goold, 2006; Lyon, 2002; Schlosberg & Ozer, 2007; Solove, 2011a). Solove (2011) writes that a common statement made when individuals accept without question, some government or private entity gathering personal information is, "I've got nothing to hide" (Solove, 2011a, p. 21). The assumption by many is that you do not have to worry if you have done nothing wrong (Solove, 2011). Privacy research conducted by Solove and supported by Goold (2006), argues that privacy should be protected at all costs because the failure to protect personal information can "inhibit such lawful activities as free speech, free association, and other first amendment rights" (Solove, 2011, p. 4).

The data collected by video surveillance cameras can be used in conjunction with other methods of identification such as access control cards and credit card purchases to track the activities of an individual (Senior et al., 2003). This may not worry individuals who have no fear of a loss of privacy, but Solove (2011) warns that the erosion of privacy is not one single act, but occurs over time, through small seemingly insignificant acts. He argues that these incremental losses of individual privacy, and the failure to protect what each individual may want to hide, will result eventually in loss of personal privacy. This

highlights a common concern that CCTV causes a loss of privacy and freedom (Jermyn, 2004, p. 76) and supports the recommendation that we should endeavor to create safeguards protecting an individual's right to privacy (Goold, 2006).

The researcher reviewed the literature related to the theories relevant to this research, i.e. rational choice theory, routine activities theory, and social learning theory, as they relate to the ethical use of video surveillance technology. These theories are applicable to CCTV owner and operator performance, the need for ethical guidelines addressing improper use of cameras, prevention of voyeurism, and subject targeting biases. This research reviewed the current literature on the issues related to the public and student's rights to privacy in public places.

Rational choice theory. Rational choice theory has its roots in economics and posits that criminals act to maximize the benefits of a crime committed and minimize the risk of apprehension. The offenders seek to positively benefit themselves and weigh the "choice-structuring properties" of alternatives such as not committing the criminal actions (Cornish & Clarke, 1987, p. 935). Rational individuals choose the alternative that is likely to give them the greatest satisfaction.

This theory assumes that criminals are making rational choices when deciding to commit crimes. This theory, also known as environmental criminology, emphasizes that the behavior of criminals is place-based, and any change in environment has a direct impact on whether a crime occurs (Brantingham & Brantingham, 2003). According to the theory, these decisions are rational because criminals weigh the cost and benefits of committing a crime versus the potential for apprehension.

Researchers report that the mere presence of video surveillance reduces crime in the area of surveillance because criminals fear the increased risk of arrest (Welsh & Farrington, 2002). This theory tends to support the decisions of many cities to install cameras as a measure to deter crime (Armitage, Smyth, & Pease, 1999). Surette (2005) supports the rational choice theory, reporting that the camera's effect on crime depends on the potential increase in risk criminals associate with apprehension. If the criminal decides that the risk of apprehension outweighs the benefit of the crime he intended to commit, the criminal will not commit the crime, or they will commit the criminal act elsewhere.

Practitioners often use rational choice theory as an explanation to justify the installation of cameras as a crime prevention tool (Armitage et al., 1999). As a focus of this study, the researcher will use this theory to explain the choice made by surveillance system monitors to use these systems in either an ethical or, an unethical manner. If the camera system operator perceives the outcome, reward, or pleasure derived from the unethical use of the camera system, exceeds the risk of discipline or detection, rational choice theorizes the operator may choose to act in an unethical manner (Cornish & Clarke, 1987).

Opponents of the rational choice theory, as it related to CCTV, report that interviews of armed robbers in prison revealed, that the presence of CCTV technology near the crime scene, was of little or no consideration on a criminal's choice of intended target (Erickson & Stenseth, 1996). Lupia, McCubbins, and Popkin (2000) suggest that researchers considering the use of rational choice theory need to look at the actions of people through a lens that considers an individual's ability to make rational choices.

These researchers further contend that not every person is capable of making an informed choice. Some individuals suffer from diminished cognitive ability, and their capacity for rational decision-making is impaired. If a criminal's judgment is impaired, or affected by their lack of cognitive ability or substance abuse, their ability to make a rational choice is doubtful.

Routine activities theory. The second theoretical examination of the unethical behavior of CCTV system operators is through the lens of routine activities theory. This theory proposed by Cohen and Felson (1979) explains the three elements are necessary for the criminal event to occur. The elements of the triangle are; a motivated offender, the criminal; a suitable target, the victim; and the absence of a suitable guardian, no police presence (Clarke & Felson, 1993). If any one of these elements is not present, a crime does not occur.

The installation of cameras as a crime prevention tool may affect a change in the daily routine of the victim, offender, or location. This varying of routine changes the dynamics of the crime triangle (La Vigne, Lowry, Markman, & Dwyer, 2011). The cameras act as "controllers" effecting the completion of the crime (Clarke & Felson, 1993). The crime may occur but in another place, or to a different victim, causing a displacement of crime, not actually a decrease in crime.

Recently research has begun to apply routine activities theory to cybercrimes as the anonymity to and availability of victims gives motivation to the offender (Choi, 2008). The literature reveals a few recent studies using routine activities theory to study computer-based crimes (Marcum, 2008; Mensch, 2009). The suitability of using a CCTV system to commit an unethical or illegal act without the victim's knowledge, or suitable

guardian to prevent the act supports the applicability of routine activities theory as a theoretical framework (Cohen & Felson, 1979).

Surette (2005) states that boredom of CCTV operators, and the inability of most surveillance systems to prevent unethical use by these operators, has led to voyeuristic use of the cameras. Camera operators may use moveable cameras to view the inside of private homes, women's breasts, or other inappropriate behavior. In other instances, camera operators may unlawfully target people for surveillance based solely on race or other demographic factors (Norris & Armstrong, 1998). Without a reliable guardian to monitor the behavior of CCTV operators, instances of unethical behavior related to bias and voyeuristic behavior are possible.

The research on ethical use of cameras also investigated the role of strong ethical use policies acting as a guardian over the behavior of video system operators. Will a strong policy (guardian) remove one leg of the crime triangle and therefore prevent the unethical use of video surveillance systems or the recorded data (Cohen & Felson, 1979)?

The criticism of routine activities theory primarily stems from those researchers who endorse the social learning theory of crime as the more accurate explanation of the occurrence of crime. Researchers in studies related to CCTV and operator performance (Rye & Meaney, 2007) have used social learning theory as their theoretical framework. Social learning theory of crime, based on a behavioral science theory developed by Ronald Akers (Akers & Jensen, 2009) maintains that criminals learn to commit crime by associating with other criminals. The theory stresses the important role that a criminal's peer group plays in determining if an individual engages in criminal activity.

Social learning theory. Akers' social learning theory states that the three primary mechanisms that teach people to engage in crime are reinforcement, values and attitudes, and imitation (Akers & Jensen, 2009). This model, proposed by Akers, asserts that social structure, peers, family, and environment, that the person is exposed to, have a direct effect on their values and attitude. An individual exposed to a peer group exhibiting criminal behavior, will begin to emulate that peer group, and model their behavior. These behaviors are reinforced or rejected, based on the punishment or reward the learned behavior receives.

Prior research related to both voyeurism (Rye & Meaney, 2007; Surette, 2005) and operator bias (McCahill, 2002; Norris & Armstrong, 1999) supports the relationship of social learning theory, as applicable to evaluating CCTV operator performance. The literature describes voyeurism as "the act of becoming sexually aroused by watching some form of activity of unsuspecting, unconsenting individuals" (Adams, 2000, p. 216). Norris and Armstrong (1999) explain operator room bias as surveillance targeting individual(s) for no particular reason other than that individual belonging to a particular demographic group.

Operators of CCTV may target groups for surveillance as a method of social control. Prior studies of control room behavior (McCahill, 2002; Norris & Armstrong, 1999; Saetnan, Lomell, & Wiecek, 2004) showed that individuals and groups were routinely targeted based on appearance. These individuals were targeted "for no obvious reason" rather than overt criminal behavior (Norris & Armstrong, 1999, p. 200). Their research concluded that in many instances, the use of CCTV surveillance was a method

of remotely following targeted individuals or groups, based on a category of appearance, rather than any actual criminal or disorderly behavior.

Often noted in the research, are reported abuses of CCTV surveillance equipment by control room operators based solely on appearance (Electronic Privacy Information Center, 2008; McCahill, 2002; Norris & Armstrong, 1999; Schlosberg & Ozer, 2007). In areas where security or police were deployed by the control room operators, McCahill reports that there was a greater "chance that teenagers would be ejected" solely based on operators targeting profile rather than behavior (2002, p. 202). The social learning theory suggests that the basis for these behaviors, are the modeling of peer behavior. If the organization, such as the university, does not have strong policies regulating this behavior, the values and attitudes of the operator may, only be based on what they learned from their peer, or social group (Akers & Jensen, 2009; Rye & Meaney, 2007).

Social learning theory is also the basis for studies on voyeurism (Akers & Jensen, 2009; Draeger, 2011). Research reveals that an operator of a CCTV system is five times as likely to use cameras for voyeuristic purposes, as opposed to protectionist motives, like crime prevention, for which it was intended (Norris & Armstrong, 1999). The operator of a camera system may choose to use the system to view and record inside a home or even watch a sexual act occurring on a rooftop, using infrared cameras (Electronic Privacy Information Center, 2008). Both of these reported acts of voyeurism, committed by cameras system controllers, were without the knowledge or consent of the victims.

The increased instances of social and news media using recorded surveillance video footage escalates the potential reward for operators to view, record, and distribute

unauthorized video data (Jermyn, 2004; Norris & Armstrong, 1999). This seeming reward for voyeuristic use of the cameras only encourages continued unethical use by CCTV operators (Rye & Meaney, 2007). Operators may feel the reward of approval from their peers, or the excitement of breaking rules justifies the use of cameras for this purpose (Rye & Meaney, 2007). Conversely, if the rules and penalties, related to the ethical use of cameras, were strong and enforced, the negative reinforcement of the penalty, would help to curb this unethical use (Caron, 1998).

Voyeurism is an important reason for colleges to consider strong use policies for their CCTV operators. The release of the video data recorded of students, without their permission, for other than authorized use, may violate FERPA regulations (Department of Education, 2008). Discussions on the loss of privacy and freedom, due to installation of CCTV in public places, are a prevalent and common theme in the literature (Dubbeld, 2003; Electronic Privacy Information Center, 2008; Gallagher, 2004; Lyon, 2007).

Issues of privacy. An alternate way for the researcher to view this research, on the ethical use of CCTV, was through an ethical lens. The researcher considered the issues related to the ethical use of the surveillance systems, security of the recorded data, and a person's right to privacy. The research on privacy was limited as it applied to surveillance technology and cameras. Many research articles discuss the impact of CCTV, as it relates to a loss of privacy and infringement on individual rights, yet there is no clear definition of the ethical use of surveillance technology (Dubbeld, 2003; Gallagher, 2004; Hempel & Topfer, 2004).

This researcher has instead chosen to give an overview of the theoretical framework of privacy, as it relates to CCTV and video surveillance, through a literature

review on the privacy issues. Lyon (2002) warns of the possibility of the control room operators and security professionals using the cameras as a method for sorting out unwanted persons using social stereotypes based, not on behavior, but on preconceived social biases. This makes the area less inviting or open to those not fitting the social norm of the area under surveillance (Lyon, 2002).

Norris and Armstrong (1999), warn that without ethical surveillance monitoring policies, those having surveillance control over a place will unduly target the young, and ethnic minorities, for enforcement. Some camera systems and their assigned operators have little or no formal regulations when it comes to CCTV monitoring. Schlosberg and Ozer (2007) reviewed ethical use policies in California and found while many municipalities did not have any policies, many of the policies that were in existence, were weak and unenforceable. One policy in Fresno, California has a section that prohibits racial profiling yet, in another section of the same regulation, supports race as a criterion for targeted surveillance (Schlosberg & Ozer, 2007).

Currently, in the United States there are few existing regulations on the growth of CCTV systems, either on campuses or in public (Schlosberg & Ozer, 2007). The lack of strong regulations may permit a "*Functional Creep*" of technology which Winner (1977) describes as a circumstance when technologies installed or designed for specific purposes, such as crime prevention, are used for other, unintended purposes. An example would be traffic cameras recording video of a plane crashing in the Hudson River or recording a robbery on a street corner. This dramatic video was not the intended purpose for installation of the cameras and seemingly, no harm occurred by these unintentional recordings but potential for harm is possible in other cases (Gallagher, 2004).

Privacy advocates argue that this functional creep has a potential in other less benign circumstances to infringe on a citizen's right to privacy. For example, a demonstration on the street recorded by cameras where the protester's image later appears on television or an attempted suicide where the victim's identity is revealed to the public and the video of this disturbed person's private act later is released for the public to view (Gallagher, 2004; Taylor N. , 2002). This is an unintended consequence and yet once these videos become public, for example on the news, YouTube, or Facebook, the victims right to privacy cannot be restored (Gallagher, 2004). Privacy regulations and the ethical use and safeguarding of video data would help prevent these types of future occurrences.

Universities and other non-governmental owners of CCTV cameras and surveillance systems monitor and record video images of public areas and use this data for criminal and internal investigations. This research will analyze the methods used by universities to ensure that the significant cost of installing, maintaining, and monitoring a large CCTV system on a college campus includes policies implemented to ensure the ethical use of these systems.

University administrators and public safety departments should be cognizant of the Family Educational Rights and Privacy Act (FERPA), legislation enacted to protect the privacy of student information (Department of Education, 2008). When universities use CCTV to record student protests, on or off campus, the recording of these lawful protests may be in violation of the student's right to free speech, assembly, and association. FERPA is a federal statute that generally bars colleges from giving law enforcement agencies any student records, without written consent of the student, unless

presented with a court order or subpoena. The video recordings of student activities on campus pose unique legal and ethical issues. Careful consideration should be given by any university administration before release of this video data or any data regulated by FERPA (Department of Education, 2008).

The researcher reviewed the literature on the best practices on the ethical use of CCTV systems. The studies recommended various methods for safeguarding video surveillance data and controlling the rapid deployment of CCTV technology. The American Civil Liberties Union (ACLU) recommended that installation of all CCTV cameras cease immediately (Schlosberg & Ozer, 2007). To solidify this point, the Electronic Privacy Information Center (2008) filed briefs with the Department of Homeland Security requesting the use of video surveillance only be permitted in instances when no other, less invasive, technology is appropriate.

The ACLU argues that research studies have shown that cameras are ineffective and are a threat to civil liberties (Baile, 2008; Schlosberg & Ozer, 2007). These studies recommend no active monitoring of cameras in an effort to prevent discriminatory targeting or voyeuristic monitoring of the public. This recommendation is supported by research on cameras systems in San Francisco (King et al., 2008). While the recommendations contained in those studies were the most drastic, as they relate to surveillance cameras, others have recommendations that are more realistic (Elizabeth II, 1998; Information and Privacy Commissioner of Ontario, 2007; Community Safety Camera Ordinance, 2006; U.S. Department of Homeland Security, 2007).

The Data Protection Act of 1998 (Elizabeth II, 1998) was one of the first laws enacted in the United Kingdom attempting to regulate and protect the exchange,

safekeeping, and privacy of personal data. This act requires the registration of all public CCTV systems. The registration of CCTV systems is mandatory in the United Kingdom to ensure that all systems operate in accordance with the data protection principles (Elizabeth II, 1998). Goold (2006) and King et al. (2008) also supported the registration of systems and oversight by a regulatory agency for implementation in the United States.

Goold's (2006) recommendations although similar, do not include a specific regulatory body that should oversee the registration of video systems, but a similar version of the recommendation is in place in San Francisco (Community Safety Camera Ordinance, 2006). The Community Camera Safety Ordinance enacted in 2006 mandates even government agencies must apply for permission from the Police Commission prior to installation of public cameras (Community Safety Camera Ordinance, 2006). The proposal for camera installation requires the Police Commission, to publish a report justifying the installation of a camera, and hold a public hearing for neighborhood comment on the installation. If the Police Commission approves the camera installation, then public notice is required by both mailing those residing in the area of installation, and the placement of signage announcing the pending installation of surveillance cameras.

The Community Safety Camera Ordinance mandates that video recording be restricted to areas readily visible from the streets, and sidewalks, by the human eye (Community Safety Camera Ordinance, 2006). This is similar to the recommendations made to safeguard privacy by other studies and municipalities (Information and Privacy Commissioner of Ontario, 2007; Hempel & Topfer, 2004; Electronic Privacy Information Center, 2008; U.S. Department of Homeland Security, 2007). The installation of cameras

may impact the privacy and civil liberties of individuals and Goold (2006) along with other experts (La Vigne et al., 2011; U.S. Department of Homeland Security, 2007) recommend that cameras are placed so even individually controlled cameras, cannot be aimed into private residences or other areas, that have a reasonable expectation of privacy. This will avoid the voyeuristic gaze of an unethical camera operator.

Best practice recommendations also endorse controls on the release of data without written request and limit review of recorded data only for investigation of specific past crimes (Cavoukian, 2001; Goold, 2006; Hempel & Topfer, 2004). The use of signage, warning an individual they are entering area of surveillance, is mandated in some municipalities and countries (Cavoukian, 2001; Community Safety Camera Ordinance, 2006; Data Protection Act 1998, 2000), and recommended by other studies (Hempel & Topfer, 2004). The Department of Homeland Security recommends not only notification to the public but suggests in their literature that, "public agencies installing CCTV camera systems permit public inspection of these systems to build community trust" (U.S. Department of Homeland Security, 2007, p. 31).

The final recommendations were consistent through many of the reports, regulations, and studies. The requirement for policies guiding the use of CCTV surveillance technology was recommended or mandated by La Vigne et al. (2011) and others (Information and Privacy Commissioner of Ontario, 2007; Community Safety Camera Ordinance, 2006; Goold, 2006; Hempel & Topfer, 2004; Electronic Privacy Information Center, 2008) to assure transparency and oversight of the surveillance systems. These policies should include how each institution deals with privacy breaches and data security (Information and Privacy Commissioner of Ontario, 2007).

Additionally recommended best practices included regular auditing of camera use and mandatory training of personnel on camera use policies.

CCTV policies currently in use by colleges and universities were reviewed and compared to the recommended best-practices guidelines of International Association of Law Enforcement Administrators (IACLEA) (2007) and Department of Homeland Security (U.S. Department of Homeland Security, 2007). A sample of publicly available CCTV policies, from colleges in the United States and United Kingdom, were obtained from the Internet. In the United Kingdom college and university CCTV policies, consistently referred to complying with the Data Protection Act 1998 (DPA) (Elizabeth II, 1998) as the requirement of the law (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010).

London South Bank University's policy is well developed and comprehensive. They assign responsibility for the system to the head of security and direct that the CCTV system be registered on the "Data Protection register which is held by the Information Commissioner" (London South Bank University, 2010, p. 1). This college additionally mentions retention of data for approximately 28 days, and limits access to video data to those authorized to view the cameras. Canterbury Christ Church University (2006) and Callington Community College (2011) both have similar standards as London South Bank University requiring data held only as long as necessary, restricting recording of private residences, and requiring registration with the Information Commissioner.

The consistency of the three policies of the schools in the UK reflected the standards of the DPA (Elizabeth II, 1998). There are provisions in the policies reviewed allowing persons who believe they were recorded to request copies of the video from the

colleges (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010). The colleges must record these requests and comply within a reasonable time but no longer than 40 days (London South Bank University, 2010).

Additionally these previously mentioned policies require all authorized personnel to handle CCTV data confidentially, and access to view the video is limited to authorized personnel. Finally, the DPA (1998) requires the prominent display of signage in areas where video surveillance is conducted. This signage must contain the name of the person in control of the recorded data, the purpose of the recording, and the telephone number of the contact person. The policies of the colleges in the UK reviewed for the study all met or exceeded these guidelines related to proper signage (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010). The mandatory requirements of the DPA (1998) are obvious when reviewing plans of the colleges under the laws jurisdiction.

There is consistency throughout the policies published by colleges in the United Kingdom. They are all very similar in message and format, quite dissimilar to the CCTV policies of the colleges reviewed in the United States. In the US, there is no single legal statute or standard policy guiding the use of CCTV on college campuses. A review of policies publicly available on the Internet reveals policies that vary in scope and oversight among the institutions.

The University of Nevada, Reno (UNR) (2006) has a comprehensive policy that is regulated by Nevada law (Nevada Revised Statutes, 1993) and the Nevada Board of Regents (2010). The UNR policy restricts the use of covert camera installation to mirror

the Nevada regulations, and only allows covert installations in criminal investigations with prior permission of the UNR President. Additionally, a Committee on Video Surveillance (CVS) must approve all camera installations. This group consists of representatives of various departments and groups including Facilities and Residential Life; faculty and union staff; graduate and undergraduate students; and Public Safety. The policy requires posted signage announcing the presence of cameras on campus, regular review of requests for new cameras and the removal of existing cameras, and regulates that video data are stored no longer than 30 days. Finally, the UNR policy only allows viewing of video by authorized personnel and the university president must approve the release of recorded video to any outside entity.

Syracuse University (2012) and Washington University in St. Louis (2011) have similar policies to UNR (2006) requiring a committee to oversee camera installations. Both schools place restrictions on installation of covert cameras, and allow for procedures to appeal installation of new or removal of existing cameras. Syracuse University's Physical Safety and Security Systems Committee (PSSSC) and University of Washington's CCTV Committee both ensure that the security and Public Safety Departments at their respective universities my review recorded video in case of criminal investigations and ensure that all personnel are required to undergo training regulating the use of this video. This training includes nondiscrimination policy and the professional and ethical use of the cameras (Syracuse University, 2012) and restricts using cameras to follow people unnecessarily. Both schools specifically restrict the use of cameras in residential or private spaces where there are reasonable expectations of privacy (Syracuse University, 2012; Washington University in St. Louis, 2011).

Similar to the previously cited policies, the policies of Johns Hopkins University (2005) and University of Minnesota (2005) both restrict monitoring based on characteristics prohibited in the non-discrimination policies and restrict use to legitimate security functions. Differing then the policies of the other US schools reviewed (Syracuse University, 2012; University of Nevada, 2006) both Johns Hopkins and University of Minnesota assign full oversight of the CCTV systems, training, and policies to their security departments. Neither of the above-mentioned schools has a CCTV committee or needs approval before installing or releasing data. Training in the proper use of the systems is required for all camera operators. Villanova University (2010) has a similar policy but does not require oversight of any committee or person unless they are requesting covert camera installation and specifically mentions release of images to local law enforcement in accordance with FERPA (Department of Education, 2008).

Finally, Franklin & Marshall College (2008) and Bates College (2008) have policies that vary from the prior colleges policies reviewed. While Bates College, and Franklin & Marshall restrict viewing to only authorized personnel, they both have shorter retention time for recorded data, 14 days for the former, and 15-20 days for the later. Additionally, neither college's policy requires training of personnel on the ethical use of CCTV. Their policies only reference other college policies that should not be violated, such as sexual harassment or discrimination policies.

Chapter Summary

At first, the use of CCTV seems a reasonable and prudent use of resources to ensure the safety of a changing world, a more objective look may reveal this method of Orwellian supervision as ineffective, and an erosion of the citizen's right to privacy

(Schlosberg & Ozer, 2007). Surveillance cameras have proven effective in identifying offenders after a criminal act is committed, yet research has shown CCTV as a crime prevention tool has had limited documented success (King et al., 2008). The threat of future terrorist incidents after September 11, 2001 and an effort to combat the fear of crime in our neighborhoods, empowered many cities, private businesses, and colleges to utilize video surveillance as an acceptable means of crime prevention (Hier et al., 2006).

Theories of criminal and social behavior as well as issues of privacy as they relate to control room operators and privacy rights were examined for this research. The researcher examined rational choice and routine activities theories as they relate to the installation of CCTV for the purpose of crime deterrence. Social learning theory was discussed as it relates peer and social pressures on control room operators' professional and ethical use of CCTV technology. Finally, the research on issues related to privacy examined the potential infringement on individual rights, of students and other persons when using CCTV and surveillance technologies on a college campus in an unethical manner.

The review of multiple college CCTV policies publicly available on the Internet revealed differing levels of oversight at each college depending on the country the college is located, either the UK or US, and the individual college's regulations. In the United Kingdom, the Data Protection Act of 1998 regulates use of CCTV (1998) so consequently college policies published in the UK followed the law and were found to be similar in content (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010).

Some of the more comprehensive policies in the US required strict oversight of all aspects of the CCTV policy and did not allow security personnel to make decisions on camera placement or use (Syracuse University, 2012; University of Nevada, 2006; Washington University in St. Louis, 2011). Other colleges require less oversight and allow campus security or public safety personnel to make decisions related to CCTV (Johns Hopkins University, 2005; Franklin and Marshall College, 2008; University of Minnesota, 2005). The effectiveness of cameras as a crime prevention tool for industries, such as universities versus the potential for liability through unethical use, is reason to implement strong ethical use policies.

Chapter 3: Research Design Methodology

Introduction

The review of the literature related to the ethical use of CCTV on college campuses revealed that there are a myriad of CCTV policies currently in use. Yet, no uniform standard for CCTV policy exists that all colleges are required to follow. In order to obtain data on policies currently used in colleges and universities in the Mid-Atlantic United States, an Internet-based survey was developed related to the ethical use of CCTV on college campuses. This survey will gather data from a sample population of college and university Directors of Public Safety and Security in the Mid-Atlantic United States.

The problem that this research focused on is the lack of standardized CCTV policies related to the ethical use of surveillance camera technology, guiding colleges and universities. Each educational organization must develop their own policies for the ethical monitoring and use of CCTV technology and the data collected by these systems. The starting point for this research looked to show that a strong well-developed policy, based on a standardization of industry-wide best practices will prevent, detect, or deter the unethical use of video surveillance equipment and data in a university setting.

The research used a quantitative survey-based research methodology. The researcher developed and distributed an Internet-based survey instrument that requested security professionals to evaluate their college or university's policies related to the ethical use of video surveillance. The literature review for this research identified policies currently in use by colleges and universities. These policies, retrieved from open

sources on the Internet via college web pages or publications were coded using Hyper RESEARCH qualitative analysis software to create a codebook of themes, as recommended by Creswell (2007). These themes then served as the basis for development of the survey questions used in this study.

The survey, developed using the coding analysis data, asked the members of the research population a series of questions assessing their CCTV policies, related to the ethical use of video surveillance on their college campuses. The research participants consisted of 265 college security directors and public safety administrators belong to the International Association of College Law Enforcement Administrators (IACLEA) Mid-Atlantic region of the United States.

Using the IACLEA (2012) database of colleges and universities as the source of the population, surveys were emailed via SurveyMonkey to the entire 265 members listed as working at IACLA member schools in Mid-Atlantic region of the United States. Use of a quantitative research survey was appropriate for this research, as the goal is to obtain self-reported information from a sample population of all accredited colleges in the Mid-Atlantic United States, and extrapolate this information to design industry best practices for the entire population of US colleges (Rea & Parker, 2005).

An analysis of the survey response data was conducted using SPSS, statistical analysis software. This data, compared to the recommended practices for the installation and use of CCTV issued by the security industry (IACLEA , 2007; U.S. Department of Homeland Security, 2007), can be used by professionals to develop best practice recommendations for use by college security professionals to formulate more

comprehensive, and consistent, ethical use of CCTV policies for US colleges and universities.

The research questions that this study attempted to answer are as follows:

1. How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campuses?

2. How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel?

3. How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff populations?

4. How do colleges ensure that their CCTV policies remain up to date as technology and university needs change?

5. How do colleges integrate their university's ethical use of CCTV policies with their university's other ethical policies such as sexual harassment and discrimination.

Research Context

The research study endeavored to reach the entire population of 265 Public Safety and Security professionals at colleges and universities in the Mid-Atlantic United States. All participants' colleges were members of International Association of Campus Law Enforcement Administrators (IACLEA) and their database of colleges and universities served to identify and contact the research study population (International Association of Campus Law Enforcement Administrators, 2012). The research population, described as the entire group of persons or institutions that the researcher wants the study to generalize (Vogt & Johnson, 2011), was comprised of colleges and universities located in the Mid-Atlantic United States.

The research format consisted of a quantitative survey administered to Security and Public Safety professionals working at colleges and universities. The survey, designed using Likert-type response choices, consisted of fixed-response multiple-choice questions with the option to select an open-ended response choice with space to comment if the none of the fixed answers were applicable to their school's policy.

Additionally, the survey participants were requested to provide demographic data on their schools, including location, security department size, and if the security department was sworn or unsworn. Finally, there was an open-ended comment box at the end of the survey for participants to add any additional information on their use of CCTV or the development of their college's CCTV policy they felt appropriate.

The study participants received an Internet-based survey sent to their email address via SurveyMonkey. The questions were relevant to the development, deployment, and integration of the ethical use of CCTV policies on college campuses. The researcher ensured that identifying information on the survey, including the identities of the research participants and their affiliated institutions, remained confidential.

Research Participants

Participants for this research study consisted of public safety and security professionals from institutions of higher education in the United States. The researcher will sample the entire population from the Mid-Atlantic region of colleges, as identified by IACLEA (2012), to facilitate the generalizability of the research findings.

IACLEA is an organization of over 1200 colleges and universities around the world. The purpose of IACLEA is to provide educational resources and professional development for member schools. IACLEA also serves as an accrediting agency so

colleges can strive to maintain the highest professional standards in the industry. IACLEA is recognized in the college security and public industry as a source of guidance and information on best practices in the profession. It is appropriate to use the members of this organization as the research participants as they represent a cross section of the industry.

The entire database of colleges and universities, obtained from IACLEA (2012) was used to obtain a sample from the Mid-Atlantic region of colleges belonging to IACLEA. The resulting total population consisted of 265 colleges and universities in the Mid-Atlantic region. The name of participants and their affiliated schools will remain anonymous in this study.

Instruments Used in Data Collection

This study used a quantitative Internet-based survey, administered to security professionals at colleges and universities in the Mid-Atlantic region of the United States. The survey used the Baldrige Criteria for Professional Excellence model (National Institute of Standards and Technology, 2011-2012) as a method to assess college's policies.

The Baldrige Criteria assists organizations in identifying areas that need improvement. Additionally, the Baldrige Criteria was developed to help organizations improve their processes, by pinpointing their strengths and weaknesses. These criteria enable organizations to develop an overall performance map and identify areas that need improvement. For the purposes of this study and the design of the research survey, the scoring dimensions for the process area of the Baldrige Criteria were used. The survey consisted of specifically developed questions related to a college's CCTV policy and how

that policy met the Baldrige Criteria related to, *Approach*, *Deployment*, *Learning*, and *Integration* of the policy (2011-2012).

Questions based on the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) category of Approach, were related to the effectiveness of the methods used to accomplish a process. In this research study, Approach refers to how a school actually developed and implemented their CCTV ethical use policy. Deployment questions on the survey assessed the schools distribution, consistent application, and actual use of the policy. Questions related to the Learning criterion considered if the colleges and universities re-evaluated their policies on a regular basis, and refined their policies, as technology or their school's needs changed. Finally, the survey inquired whether the Integration of each school's policy was designed to support their organizational goals. Used in the design of this study's survey, these criteria will serve as a tool to assess and evaluate the design, operations, and processes used by colleges and universities to create their CCTV ethical use policies.

The literature review for this research identified policies currently in use by colleges and universities. College CCTV policies from schools located both the United States (Bates College, 2008; Franklin and Marshall College, 2008; Johns Hopkins University, 2005; Syracuse University, 2012; University of Nevada, 2006) and United Kingdom (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010) were examined and served as the framework for questions used on the survey. The recommended CCTV guidelines issued by the Department of Homeland Security (U.S. Department of Homeland Security, 2007) and International Association of Campus Law Enforcement Administrators (IACLEA , 2007)

for the installation and use of CCTV technologies were also reviewed to ensure that any industry-wide best practices recommendations were incorporated into the development of the survey. The survey contained a series of questions for the chief security officials, at colleges and universities, directly related to assessing their current policies and the need for further policies related to the ethical use of video surveillance.

This study for education purposes used human research participants so was subject to additional ethical and legal guidelines. The structure and content for this research study, and the survey instrument were submitted to the Institutional Review Board (IRB) of St. John Fisher College for research approval. The St. John Fisher College IRB approval document is shown in Appendix D.

An Internet-based survey (see Appendix B), emailed to the research participants, consisted of three sections. The first section consisted of informed consent form explaining the intent of the study, the method of protecting each participant's anonymity, and the participant's rights regarding the research study (Appendix A). Study participants were asked to read and electronically acknowledge consent to participate in the study.

The second section of the survey, contained closed-ended, fixed-response multiple choice questions with the option to select *Other(please specify)* if the none of the fixed answers were applicable to their schools policy. Following the responses choice, *Other (please specify,)* there were spaces for open-ended comments. Rea and Parker (2005) recommend closed-ended fixed answer questions as they fix the number of alternative responses to questions. This allows ease of data transfer and more uniform answers. Open-end follow-up questions are appropriate if the researcher seeks

information not readily discernible solely from fixed answer questions. (Rea & Parker, 2005).

The survey requested participants to answer each question in the second section by electronically marking a box, placed under each question, which most correctly aligned with their college or university CCTV policy. One of the participant's multiple choice response options was to answer the open-ended question selection of *Other (please specify)* if appropriate, and expand on their answers in the open-ended follow-up space if more clarity of response is necessary.

The third section of the survey, inquired about the participating schools' demographic information. The school demographic information requested included, size of the student population, size of the security department, if the department is sworn or unsworn department, type of school location: (a) metropolitan/inner city or large city, (b) urban or located in a smaller city, (c) urban-adjacent, defined as near a city, (d) and rural not in close proximity to a city. Additionally, this section contained an open-ended comment box at the end of the survey for all participants to write any additional information on their use of CCTV or the development of their college's CCTV policy they felt appropriate.

As this was a new survey instrument, reliability and validity had to be established prior to use on the research participants. Validity requires that the questions measure what they are purported to measure and that the participants interpret the questions as the researcher intended (Czaja & Blair, 2005). To aid in establishing validity and reliability of the survey instrument, an expert panel of nine college security professionals were

selected to evaluate the survey. The panel consisted of a convenience sample of security professionals from colleges belonging to IACLEA.

The panelists pre-tested the Internet-based survey to ensure that the questions were appropriate and assessed the time necessary for the research participants to complete the survey. A pre-test is a small-scale distribution of the survey to a convenience group, in this case a group of college security professionals (Rea & Parker, 2005). The panelists were asked to suggest alternative verbiage if necessary and ensure the content of the questions were clear. These nine panelists then returned the survey with their written comments.

After review of the panel's comments and responses, survey questions were reworded for clarity, and mechanical flaws in the electronic version of the survey corrected. The panelists correctly recommended the elimination of two questions on the pre-test from the final version of the research survey. The first was redundant and unnecessary and the second deemed not directly related to the purpose of this study. The corrected survey was prepared for a test distribution to the expert panel.

The nine members of the expert panel were sent an email via Survey Monkey containing an Internet link to the survey. The test surveys were distributed to the panelists in the same manner as the actual research participants to most simulate the actual research conditions. The panelists were requested to complete the survey and return it electronically via SurveyMonkey. They were also encouraged to include any comments or suggestions for additional changes to the survey.

The nine panelists completed the entire Internet-based survey and returned their surveys electronically. The data from this test survey were analyzed and this revealed the

survey was mechanically sound. A review of the data on SurveyMonkey showed all data recorded correctly. Three recommended changes were to correct typographical errors on the survey. Those corrections were incorporated into the final version of the survey (Appendix B), and redistributed to the same expert panel for re-test and finalization of the survey (Kelley, 1999). The panel of expert members was ineligible to participate in the research study.

Procedures for Data Collection and Analysis

The fixed answer survey results collected via SurveyMonkey from the research participants were downloaded into Statistical Package for the Social Sciences (SPSS) data analysis software. The survey responses were analyzed using inferential statistics to tabulate the scores collected and summarize the values. Demographic statistics provided the count and percentile statistics. Descriptive statistics and analysis of quantitative data were used to assess the research questions.

The process to answer research question one (RQ1), "*How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campuses*" included analyzing the frequency and percentile for each response to the survey questions related to policy development, and the Baldrige Criteria of Approach (National Institute of Standards and Technology, 2011-2012). Survey questions SQ4 and SQ6 obtained information on whether participants had CCTV policies, and if so who on their campus is responsible for that policy's development. Information of the content of the colleges CCTV policies were obtained from the participants through answered submitted for SQ10-12 and SQ18-23.

Research question two (RQ2), "*How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel*" and research question three (RQ3) "*How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff population?*" were answered through analysis using frequency and count of the responses to multiple choice questions SQ13-SQ16. Research questions two and three were aligned with the Baldrige Criteria of Deployment (National Institute of Standards and Technology, 2011-2012).

The Baldrige Criteria of Learning (National Institute of Standards and Technology, 2011-2012) was associated with research question four (RQ4) "*How do colleges ensure that their CCTV policies remain up to date as technology and university needs change.*" In addition to assessing the development of CCTV policies at colleges, the survey endeavored to assess if colleges reviewed and maintained their existing CCTV policies, keeping them up-to-date. The survey questions related to research question 4 (RQ4) were SQ7and SQ8. These questioned were analyzed for frequency and count.

Research question five (RQ5) "*How do colleges integrate their university's ethical use of CCTV policies with their university's other ethical policies, such as sexual harassment and discrimination*" assesses the schools' integration of other ethical policies at their college, including policies related to sexual harassment and discrimination. Integration is included in the assessment of organizations processes in the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012). Integration of the CCTV policy ensures that the policy and procedures in the colleges are working together to meet clear organizational goals. Analysis of the integration of policy was explored using frequency and count of participant responses to SQ17 and SQ19.

Three exploratory analyses were conducted using chi-squared tests for independence to determine if significant associations existed in school type, location, and type of security personnel. Chi-squared tests for independence are used when the relationship between two categorical variables are explored. The test compares the observed frequencies or proportions of cases that occur in each of the categories with the values expected if there were no association between the variables (Vogt & Johnson, 2011).

The first use of the chi-squared test for independence was for null hypothesis 1 (*Ho1),* "*There is no significant difference between the type of school and the frequency of negative responses to having a written CCTV policy."* Exploratory Analyses 1-3 used *Cramer's V* to determine the effect size. *Cramer's V* is used for cross tabulations larger than 2x2 whereas the most commonly reported effect size for 2x2 cross tabulations is the *phi coefficient* (Huck, 2012). Criteria for determining the size of the effect are .01 ≤ small < .30, .30 ≤ medium < .50, and large ≥ .50.

The second exploratory analysis was conducted on null hypothesis 2 (*Ho2*), "*There is no significant difference between campus location (metropolitan, urban, urban-adjacent, and rural) and the frequency of negative responses to having a written CCTV policy*." This analysis used the chi-squared test for independence to determine if a significant association existed between the location of a campus (metropolitan/inner city, urban, urban-adjacent, and rural) and CCTV written policy.

The third, exploratory analysis, testing null hypothesis 3(*Ho3*) "*There is no significant difference between the type of security personnel (sworn, unsworn, mix of sworn and unsworn) and the frequency of negative response to having a CCTV policy*"

was also conducted using the chi-squared test for independence. This third test was conducted to determine if schools with a written camera policy had similar occurrences of sworn, unsworn or, combination of sworn and unsworn security personnel as schools without a written camera policy.

Two final exploratory analyses of the survey data results were performed using logistic regression to determine if the number of students enrolled (school size), or number of cameras installed on campus predicted whether the school has a written camera policy. Results of the fourth analysis tested null hypothesis (*Ho4*) "*There is no significant difference between the number of students enrolled at a college and the frequency of negative responses to having a written CCTV policy.*" Huck (2012), reports that logistic regression does not calculate the regular r-square statistic that other forms of regression use so it was necessary to use Cox & Snell R square and Nagelkerke R square to account for the *r*-square. Cox & Snell R square and Nagelkerke R square are commonly reported "pseudo-measurability" r-squared statistics that provide an indication of the amount of variation observed in the dependent variable (Huck, 2012, p. 399).

The final exploratory analysis was conducted using logistic regression. The analysis tested null hypothesis 5 (*Ho5*),"*There is no significant difference between the number of cameras a college has installed on campus and the frequency of negative responses to having a written CCTV policy*." This analysis was to indicate if the number of cameras predicted if a college would have a CCTV written policy.

Chapter 4: Results

Research Questions

The Internet-based research survey was designed to collect data pertinent to answer the five research questions. The survey (Appendix B) consisted of specifically developed questions related to college's CCTV policies and how those policies met the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) related to, *Approach*, *Deployment*, *Learning*, and *Integration*.

The results of the survey are presented the following order. Demographics of the survey population first, followed by each survey question as it related to the specific research questions. This method of presentation and organization is recommended for clarity of information (Glatthorn & Joyner, 2005). Finally, a presentation of the analysis of the survey data to determine if differences exist in the demographic data of, schools that report having a written CCTV policy and those that do not. The five research questions were:

Research Question 1 (RQ1): How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campuses?

Research Question 2 (RQ2): How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel?

Research Question 3 (RQ3): How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff populations?

Research Question 4 (RQ4): How do colleges ensure that their CCTV policies remain up to date as technology and university needs change?

Research Question 5 (RQ5): How do colleges integrate their university's ethical use of CCTV policies with their university's other ethical policies, such as sexual harassment and discrimination?

Hypotheses. An exploratory analysis of the survey data was conducted using Chi-squared Test for Independence and logistical regression to test the following five null hypotheses:

Null Hypothesis 1 (*Ho1*): There is no significant difference between the type of school and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 2 (*Ho2*): There is no significant difference between campus location (metropolitan, urban, urban-adjacent, and rural) and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 3(*Ho3*): There is no significant difference between the type of security personnel (sworn, unsworn, mix of sworn and unsworn) and the frequency of negative response to having a CCTV policy.

Null Hypothesis 4 (*Ho4*): There is no significant difference between the number of students enrolled at a college and the frequency of negative responses to having a written CCTV policy.

Null Hypothesis 5 (*Ho5*): There is no significant difference between the number of cameras a college has installed on campus and the frequency of negative responses to having a written CCTV policy.

Data Analysis and Findings

The study assessed the test-retest reliability of the survey instrument using Microsoft Excel to test the correlational coefficients, standard deviation, and means of the test-retest survey responses. The data analyzed was obtained from the survey question responses for both the test and retest completed by the expert panel. Survey questions that contained strictly demographic data (SQ24-SQ32) were not included in this analysis.

The reported survey results for the first test (Test 1) completed by the nine members of the panel of experts, was compared to the responses from the survey retest (Test 2) that the panel members completed 10 days later. Both surveys were substantially the same only small typographical errors, not effecting the meaning of the questions were changed between the issuance of the two surveys. The issuance of the same survey instrument to the same population was performed to establish test-retest reliability of the survey instrument (Pettee, Ham, Macera, & Ainsworth, 2009).

The strength of agreement for the correlation coefficients used in this study were recommended by Landis and Koch (1977) and supported by Pettee (2009). The ranges are interpreted as follows: "<0.00, poor: 0-00-0.20, slight; 0.21-040; fair; 0.41-0.60, moderate; 0.61-0.80, substantial; and 0.81-1.0, almost perfect" (Pettee et al., 2009, p. 490). The range of correlation for the responses to the test-retest test of the survey instruments were the upper limit, r =1.00, almost perfect, on SQ1, SQ3-SQ6, SQ9, SQ13, SQ14, and SQ1-SQ19 to r=0.71 and r =0.66 substantial on SQ15-SQ16 (Appendix C).

The ranges of all the responses to the survey questions supported the reliability of the survey instrument. Survey question (SQ16) had a lower correlation but the standard deviation is low (*SD*=.38) indicating the response is similar on both tests. One question

that had an abnormally high standard deviation SQ15 (*SD*=2.56, *r* =71) and further investigation was conducted to establish the possible cause of the high deviation. One panelist had changed their answer from reporting that they never conducted training on their CCTV policy on Test 1 to reporting that their college trained only when new personnel were hired or promoted. The panelist reported that after taking the first survey their college changed their CCTV policy to include training provisions. The correlation remained in the range of *substantial* ranking *(r* =.71) but the small sample size (*n*=9) and one substantial change in the question response. The analysis supported the reliability of the survey instrument.

Inferential statistics were used to draw conclusions from the sample tested. The Statistical Package for the Social Sciences (SPSS) was used to code and tabulate scores collected from the survey and provide summarized values where applicable including the mean, central tendency, variance, and standard deviation. Demographic statistics were provided including count and percent statistics. Descriptive statistics and analysis of quantitative data were used to assess the research question.

Demographics. The population consisted of 265 of public safety and security professionals from institutions of higher education in the Mid-Atlantic United States. The Internet-based survey was administered to the entire population and that resulted in a voluntary return rate of n=96. That is, 96 Mid-Atlantic colleges, as identified by IACLEA (2012), responded to the research questions. Specifically, 50 (52.1%) colleges were four-year private colleges, 16 were four-year public colleges, 16 were two-year colleges, and three schools identified themselves as having graduate programs. Eleven

schools did not complete this portion of the demographic survey questions. The types of schools participating in the study are depicted in Table 4.1.

Table 4.1

Frequency Statistics for College Type

College Type	*n*	%
Four-year Private College	50	52.1
Four-year Public College	16	16.7
Two-year Public or Private college	16	16.7
Other	3	3.1
Missing	11	11.5

Note. $n = 96$

The Mid-Atlantic Region as defined by the International Association of Campus Law Enforcement Administrators (IACLEA, 2012) includes the member States of New York, New Jersey, Delaware, Ohio, Pennsylvania, West Virginia, Maryland, Washington D.C., and Kentucky.

The sample population from these States includes colleges that self-identified as located various types of neighborhoods. This includes: (a) metropolitan/inner city or large city, (b) urban or located in a smaller city, (c) urban-adjacent, defined as near a city, (d) and rural not in close proximity to a city. Two schools self-identified their institution as located in a Suburban area, which was not a listed choice. The locations of the schools participating in the study are depicted in Table 4.2.

Table 4.2

Frequency Statistics for Campus Location

Campus Location	*n*	%
Metropolitan/Inner-City	22	22.9
Urban	25	26.0
Urban-Adjacent	16	16.7
Rural	20	20.8
Other (specify)	2	2.1
Missing	11	11.5

Note. $n = 96$

The sample population included schools of various sizes of student populations and security departments. Most schools reported student populations of 7500 or less n=53 (55.2%), and security departments of 50 or less employees n=73 (64.6%). The sample size of, student populations and, security departments are presented in Table 4.3.

Security departments in colleges and universities vary in whether the security personnel are sworn, having expanded powers of arrest, or unsworn, having the same power of arrest as a civilian, or a mix of sworn and unsworn. This includes colleges that employ their own sworn and armed police departments and those colleges that employ only unsworn and unarmed guards.

Table 4.3

Frequency Statistics for Number of Students and Security Personnel

Number of Students	*n*	%	Number of Security Personnel	*n*	%
Under 1500	7	7.3	25 or less	43	44.8
1501 – 2500	20	20.8	26 – 50	19	19.8
2501 – 5000	14	14.6	51 – 100	11	11.5
5001 – 7500	12	12.5	101 – 150	9	9.4
7501 - 10,000	3	3.1	151 – 200	1	1.0
10,001 - 15,000	10	10.4	201 – 250	1	1.0
15,001 - 20,000	3	3.1	251 – 300	0	0.0
20,001 - 25,000	7	7.3	301 – 400	0	0.0
25,001 - 30,000	2	2.1	401 or more	1	1.0
30,001 - 35,000	1	1.0	Missing	11	11.5
35,000 or more	6	6.3			
Missing	11	11.5			

Note. $n = 96$

The sample population contained sworn, unsworn, and mixes of both. Departments that have armed and sworn personnel, have additional legal licensing, certification, and reporting requirements to maintain that status. These requirements vary depending on the State the college is located. This demographic data is included in the survey to analyze if those enhanced requirements had an effect of the percentage having policies for the use of CCTV on their campus. Table 4.4 provides the description of the types of security personnel at the participating schools.

Table 4.4

Frequency Statistics for Types of Security Personnel

Sworn/Unsworn Security	*n*	%	Armed/Unarmed Security	*n*	%
Sworn	15	15.6	Armed	17	17.7
Unsworn	33	34.4	Unarmed	48	50.0
Both sworn and unsworn	36	37.5	Both armed and unarmed officers	20	20.8
Missing	12	12.5	Missing	11	11.5

Note. $n = 96$

Of the 96 participating colleges, 93 (96.9%) reported that they used CCTV, or another method of video surveillance, on and/or off campus. Two colleges reported that they do not use any type of video surveillance and one college stated that they do not have any CCTV cameras on their campus. Three colleges that do not use video surveillance cameras were removed from further analyses. Thus, 93 colleges were evaluated in Research Questions 1-5 ($n = 93$).

The 93 participating schools that responded that they did have CCTV cameras on the campuses were asked if they had a written policy guiding the use of their CCTV cameras. Many of the colleges n=44 (47.3%), reported that they did have written policies related to the use of CCTV. The same number of colleges n=44 (47.3) reported that they either had no policy at all or were in the process of developing a policy. The results are reported in Table 4.5.

Table 4.5

Frequency Statistics for CCTV Written Policy

CCTV Written Policy	*n*	%
Yes	44	47.3
No, but we are currently developing a CCTV Policy	23	24.7
No, we have CCTV but no written policy	21	22.6
Other	3	3.2
Missing	2	2.2

Note. $n = 93$

The number of CCTV cameras each college or university owned varied from 100 or less cameras on campus n=40 (43%) to over 2000 n=2 (1.1%). As described in table 4.6, the majority of schools n=62(66.7%) have 200 or less cameras.

Table 4.6

Frequency Statistics for Number of Cameras

Number of Cameras	*n*	%
100 or less	40	43
101-200	22	23.7
201-500	18	19.4
501-1000	10	10.8
1001-2000	1	1.1
2001 or more	2	2.2

Note. $n = 93$

Research question 1. The following data analysis is related to Research Question 1 (RQ1): How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campuses? Each school that reported they have CCTV cameras on their campus was asked who was the responsible person(s) for developing and/or maintaining their current CCTV policy. This research question (RQ1) is related to the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) of Approach. Approach refers to the effectiveness of the methods used to accomplish a process.

The large majority of schools n=74 (79.6%) reported that it is the responsibility of their security, public safety, or police department to develop and/or maintaining their current CCTV policy. This mirrors the research which revealed that law enforcement, or security personnel usually staff CCTV control rooms as part of a successful crime prevention program (Hier et al., 2006).

As shown in Table 4.7 only three colleges reported using a committee to develop their colleges CCTV policy. This is differs from a state such as Nevada that legally mandates colleges having CCTV committees participate in the development and maintenance of their CCTV policies (Nevada Board of Regents, 2010).

Table 4.7

Frequency Statistics for Survey Question 4

Who in your college is responsible for developing and/or maintaining your CCTV policy?		
Response Option	*n*	%
Security/Public Safety or Police Department	74	79.6
College CCTV or Camera Committee	3	3.2
General Counsel or Legal Department	1	1.1
Other (Specify)	7	7.5
Unknown	5	5.4
Missing	3	3.2

Note. $n = 93$

Colleges that reported they did not have written policies were asked how they regulate camera use on their campus. The survey question permitted respondents to choose multiple answers to best convey their methods of communicating their unwritten policy. In survey question SQ3, which asked if colleges had a written CCTV policy on campus, 44 of 93 participants responded that they had a written policy, as previously noted in Table 4.5. Yet in SQ6, which asked participants if they had CCTV cameras on campus but did not have a written policy, how they regulated the use of their CCTV cameras, 60 participants answered the question. That would add up to 104 responses, which exceeds the total number of survey participants n=93. It is probable that schools with written policies also answered this survey question. The responses to SQ6 are listed in Table 4.8.

Twelve schools answered *Other* and then specified varied policies. Two schools answered that only the Director of Security/Chief have access to the cameras therefore they stated formal policies are not necessary. An additional two schools wrote that their cameras were in public places so they did not have to have policies related to the ethical use of cameras, even stating there was no legal issue of privacy.

Table 4.8

Frequency Statistics for Survey Question 6

If you have CCTV cameras on your campus but do not have any written policies, how do you regulate the use of your CCTV cameras?		
Response Option	*n*	%
Verbal training of employees	36	38.7
Written memos	25	26.9
Address each incident or question regarding CCTV as it occurs	31	33.3
Other	12	12.9

Note. $n = 93$

To analyze the types of information included in policies a survey question was included asking who investigates violations of the college's policies. Similar to questions related to developing policies related to CCTV, the majority $n=70$ (75.3%) of participating colleges responded that the person in charge of their public safety, security, or police department investigated and violations.

The data reveals that in many cases the same person or group is responsible for developing, writing, utilizing, and policing the CCTV policy the individual colleges. The

participant responses related to the responsible investigator are described in Table 4.9. The responses from participants who chose *Other college or outside agency, n*=8 (8.6%) ranged from colleges that used a Physical Safety and Security Steering Committee to investigate violations of CCTV policy to Risk Management in conjunction with Public Safety. Three of the schools wrote that the responsible investigating department depended on the type of violation or allegation requiring investigation.

Table 4.9

Frequency Statistics for Survey Question 22

Who on your campus is responsible for investigating violations of your college's CCTV policy?		
Response Option	*N*	%
Person in charge of college Public Safety/Security/Police	70	75.3
Equal Opportunity Office EEO/OEEO or equivalent on your camp	3	3.2
Other college or outside agency	8	8.6
Missing	12	12.9

Note. $n = 93$

The ethical use of CCTV requires that the viewing of CCTV data is restricted to authorized personnel. A comprehensive policy will include regulations related to the viewing, recording, and dissemination of data (Schlosberg & Ozer, 2007).

The participants were asked if their college's policy placed any restrictions on who may record, or view live video. Most participants *n*=49 (52.7%) answered that their school's policy restricted live and recorded video viewing to authorized personnel use. An additional 16.1% (*n*=15) colleges further restricted review of recorded video to

emergencies only. The responses of the participant schools in Table 4.10, describes the differing guidelines related to the authorized use of live and recorded video data.

Table 4.10

Frequency Statistics for Survey Question 12

Does your CCTV policy, written or unwritten, restrict who may view live or recorded surveillance video?		
Response Option	*n*	%
Yes, restrict viewing of live and recorded video to Security or other authorized personnel	49	52.7
Yes, require permission to view recorded video unless emergency, live viewing restricted to security or other authorized personnel	15	16.1
Yes, video is not actively monitored. Recorded video review only after incident or authorized request	10	10.8
Yes, other restrictions	3	3.2
No	7	7.5
Missing	9	9.7

Note. $n = 93$

Schlosberg and Ozer (2007) contend that organizations that record video data have an obligation to safeguard this data from unauthorized or illegal use. The survey data revealed that most colleges did include the protection of data in their policy, 8.6% (*n*=8) of colleges did not have a policy restricting copying or disseminating CCTV video data.

As outlined in Table 4.11 the person responsible for granting permission is usually the person in charge of public safety, security, or campus police *n*=60 (64.5%). Other responsible persons include the college General Council or legal department. Three schools initially were counted in the *Yes, other (specify)* group were recoded and added to the *Yes only upon receipt of subpoena* group. Their opened ended comments answers substantially stated that their college required a subpoena for review of video data.

Table 4.11

Frequency Statistics for Survey Question 11

Does your CCTV policy, written or unwritten restrict copying and disseminating video data?		
Response Option	*n*	%
Yes, only with permission of person in charge of Security/Public Safety or campus police	60	64.5
Yes, only with permission of General Counsel or college legal department	4	4.3
Yes, only upon receipt of subpoena	6	6.5
Yes, other (specify)	6	6.5
No	8	8.6
Missing	9	9.7

Note. $n = 93$

For the survey question, "Does your written or unwritten CCTV policy include guidelines on how long video data is stored?" Of the 93 participating colleges 49

answered that they did have guidelines regulating how long data was stored, 33 reported they did not, and 11 did not respond to the question. Three participants commented that the length of time their college stored video data was determined solely by the capacity of their recording devices. There were no policy restrictions, determining the length of time video could be stored.

The participants were asked what the average time their college stored CCTV video data not required for an investigation. The difference in the times colleges store data (Table 4.12) is consistent with the research of publically available college CCTV policies noted previously in Chapter 2. Bates College (2008) restricted viewing to 14 days, Franklin and Marshall (2008), 15-20 days, and University of Nevada (2006) 30 days while other colleges listed no restrictions on length of time video may be retained (Villanova University, 2010).

Table 4.12

Frequency Statistics for Survey Question 10

What is the average number of days your college stores CCTV video data, not required for a specific incident or investigation?		
Response Option	*N*	%
Less than 7 days	1	1.1
7 days but less than 14 days	10	10.8
14 days but less than 30 days	32	34.4
30 days but less than 120 days	36	38.7
Over 120 days (specify)	5	5.4
Missing	9	9.7

Note. $n = 93$

Participants were asked two questions related to the recording of non-criminal activities on the campuses. The first question (SQ8) asked if their college's CCTV policy included guidelines related to the monitoring of non-criminal activities on campus. Of the 80 participants that answered this question, 56.25% (n=45) said they had guidelines or policies regulating the monitoring of non-criminal activities (Table 4.13).

Table 4.13

Frequency Statistics for Survey Question 18

Does your CCTV policy include guidelines regulating the monitoring of non-criminal activities on campus?		
Response Option	*n*	%
Yes	45	48.4
No	35	37.6
Missing	13	14.0

Note. $n = 93$

The second question (SQ20), related to monitoring of on-campus activities was similar yet in this instance an example to non-criminal behavior was presented as part of the question. The non-criminal activity was described in the second question (SQ20) as a protest or student event. The 77 participants that answered the second question now responded that 59.7% (n=46) percent to the colleges did not have guideline regulating the recording of non-criminal student events or protest on campus. Table 4.14 describes the results of the second question related to non-criminal activities.

Table 4.14

Frequency Statistics for Survey Question 20

Does your CCTV policy include guidelines regulating the monitoring of non-criminal activities on campus (i.e. protests, student events)?		
Response Option	*n*	%
Yes	31	33.3
No	46	49.5
Missing	16	17.2

Note. $n = 93$

A person has an expectation of privacy in certain areas (Solove, 2011a). These areas normally include bathrooms, locker rooms, and personal offices. The survey participants were asked if their college CCTV policy includes guidelines restricting the use of cameras where a person would have an expectation of privacy. The participants reported that 71% (Table 4.15) had guidelines related to private's spaces.

Additionally participants were question if they had experienced any misuse of CCTV or recorded video data that required investigation or resulted in discipline. Only 4.3% (n=4) reported any misuse of CCTV cameras or recorded video.

Table 4.15

Frequency Statistics for Survey Questions 21 and 23

Does your CCTV policy include restrictions on installing cameras where a person may have an expectation of privacy (i.e. locker rooms, bathrooms, or private offices)?			Has your college experienced any misuse of CCTV cameras or recorded CCTV data that required an investigation or resulted in disciplinary action?		
Response Option	*n*	%	Response Option	*N*	%
Yes	66	71.0	Yes	4	4.3
No	13	14.0	No	79	84.9
Missing	14	15.1	Missing	10	10.8

Note. $n = 93$

Research question 2 – 3. Research Question 2 (RQ2): How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel? Research Question 3 (RQ3): How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff populations? Research questions 2 and 3 relate to the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) of Deployment. Participants were asked two questions related to how they communicate their CCTV policy. The first question (SQ13) asks how they conveyed their policy to students, faculty, and staff (Table 4.16). Only 15.1 % of the schools made their CCTV policy publically available to students, faculty, or staff. The remainder of the colleges considered their policy restricted, or only available via subpoena.

Table 4.16

Frequency Statistics for Survey Question 13

How is your CCTV policy communicated to students, faculty, and staff?		
Response Option	*n*	%
Policy is publicly available on the Internet or in written documents	10	10.8
Policy is available on college website but access restricted to students, faculty, and staff	4	4.3
Policy is on college website but restricted to authorized personnel	1	1.1
Policy is not publicly available; restricted to security personnel only	39	41.9
Not applicable. Do not have a policy	27	29.0
Other (specify)	3	3.2
Missing	9	9.7

Note. $n = 93$

The second question (SQ14) asked if students, faculty, or staff have any input into the development or implementation of the college's CCTV policy. Students were only included in CCTV policy decisions in 5.4% (n=5) of participating schools. Table 4.17 shows that the majority of the colleges n=56 (60.2%) do not permit students, faculty, or staff from contributing input into the development or implementation of their colleges CCTV policy.

Although the majority of the colleges reported they do not involve students, faculty, and staff, the participants that answered *Other* n=10 (10.8%) reported that

individuals at the college in departments other than Security/Public Safety did have input. The responses included the General Counsel, Human Resources, senior level members of the university and the President. One school reported that they work directly with the groups involved in the area a camera installation is proposed. They meet to resolve any privacy concerns including, patient care environments, and windows in student residences.

Table 4.17

Frequency Statistics for Survey Question 14

Do students, faculty, and staff (non-security personnel) have any input into the development, or implementation of the college's CCTV policy?		
Response Option	*n*	%
Yes; Students, Faculty and Staff	5	5.4
Yes; Faculty and Staff only	11	11.8
Yes; Faculty only	1	1.1
No	56	60.2
Other	10	10.8
Missing	10	10.8

Note. $n = 93$

The deployment of a policy is important, as is the training of personnel. The survey asked participants if their college conducts formal training of security personnel, and if so, how often they conduct re-training (SQ15). Table 4.18 displays the results including the results of the open-ended questions. Four of the five comments reported

that their college only retrained when new personnel were hired or the policy was changed. The fifth said they only train as needed.

Learning one of the four Baldrige Criteria (National Institute of Standards and Technology, 2011-2012), recommends regularly scheduled training and review of an organizations policies to keep up-to-date. The majority of the colleges surveyed did not regularly, once a year or more, train their security personnel on their CCTV policy.

Table 4.18

Frequency Statistics for Survey Question 15

Do you conduct formal training of security personnel on your CCTV policy? If yes how often are they trained/retrained?		
Response Option	*n*	%
Once a month	2	2.2
2-3 times a year	4	4.3
Once a year	14	15.1
Only when newly hired or promoted	29	31.2
Only if policy changes	14	15.1
Other (Specify)	8	8.6
Never	9	9.7

Note. $n = 93$

Participants were then asked if their college CCTV policy required Security personnel to sign any document that they are aware of the college's CCTV policy, and will comply with all policies related to CCTV cameras on campus (SQ16). The majority

of the colleges 54.8% (*n*=54) do not require security personnel to sign and acknowledge that they must comply with the college's CCTV policy (Table 4.19).

Table 4.19

Frequency Statistics for Survey Question 16

Does your college require that security and/or public safety personnel, sign a document acknowledging that they understand your college's CCTV policy, and will comply with all policies related to the ethical use of CCTV cameras on campus?

Response Option	*n*	%	Other (Specify)	*N*
Yes	26	28.0	No Policy	1
No	51	54.8	Do not have a policy to distribute.	1
Other (Specify)	4	4.3	Will be part of the policy when it's developed.	1
Missing	12	12.9	Not specific to CCTV. They sign an acknowledgement to comply with all Campus Safety Policies and college rules and regulations.	1

Note. $n = 93$

Research question 4. Research Question 4 (RQ4): How do colleges ensure that their CCTV policies remain up-to-date as technology and university needs change? Training and review of policies and updating of procedures is a part of the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) of Learning. Survey participants were asked how often in the past five years they had reviewed and/or

updated their CCTV policy. Of the 93 participants, 64 skipped this question (SQ7). Participants who previously stated their college had a written CCTV policy (SQ3) was n=44. The 29 participants who did answer (SQ7) n=10 had never updated or reviewed their CCTV policy in the last five years and n=16 had updated 1-2 time over that period (Table 4.20).

Table 4.20

Frequency Statistics for Survey Questions 7

In the last 5 years how often, have you reviewed and/or updated your written CCTV policy?		
Response Option	*n*	%
0 times	10	10.8
1-2 times	16	17.2
3-4 times	2	2.2
5 or more times	1	1.1
Missing	64	68.8

Note. $n = 93$

The same 29 participants then responded to a question regarding how long ago their CCTV policy was last updated (Table 4.21). Seven participant colleges had never updated their policy and six colleges had not updated their policy in over two years.

Table 4.21

Frequency Statistics for Survey Question 8

When was your written CCTV policy last updated?		
Response Option	*N*	%
Less than 6 months	3	3.2
More than 6 months - 1 year	9	9.7
More than 1 - 2 years	4	4.3
More than 2 - 3 years	4	4.3
3 years or more	2	2.2
Never updated policy	7	7.5
Missing	64	68.8

Note. $n = 93$

Research question 5. How do colleges integrate their university's ethical use of CCTV policies with their university's other ethical policies, such as sexual harassment and discrimination? Survey questions 17 and 19 (SQ17 & SQ19) relate to the integration of colleges CCTV policy into their university's policies on sexual harassment and discrimination. The Baldrige Criteria of Integration (National Institute of Standards and Technology, 2011-2012) evaluates how well each school integrates their CCTV policy with the colleges other policies such as sexual harassment and discrimination. The responses listed in Table 4.22 showed, that the majority of the colleges 64.5% (n=60) (SQ17) did not integrate the university's sexual harassment policy or discrimination policy 49.5% (n=46) into their CCTV policy.

Table 4.22

Frequency Statistics for Survey Questions 17 and 19

Does your CCTV policy integrate your university's policy on Sexual Harassment?			Does your CCTV policy include guidelines on monitoring persons based solely on race, ethnic origin, or sexual preference?		
Response Option	*n*	%	Response Option	*n*	%
Yes	19	20.4	Yes	32	34.4
No	60	64.5	No	46	49.5
Missing	14	15.1	Missing	15	16.1

Note. $n = 93$

Exploratory analyses. Five exploratory analyses were conducted using chi-squared tests for independence and logistic regression analyses to determine if significant associations existed in school type, location, type of security personnel, size, and the number of CCTV cameras between schools with a written camera policy and schools without a written policy. Chi-squared tests for independence and logistic regression are non-parametric inferential tests that do not make assumptions concerning the distributions of scores except for random sampling and independent observations; the aforementioned assumptions were not violated. The dependent variable for the five exploratory analyses was whether the schools had a written policy (CCTV written policy). Written policy was measured by Question 3 on the survey instrument and had four possible responses including: Yes; No, but we are currently developing a CCTV policy; No, we have CCTV but no written policy; and Other (specify). For the

exploratory analyses, both responses indicating No were combined and since there were, only three cases that responded with Other were removed. Thus, there were 44 Yes (n = 44) responses and 44 No (n = 44) responses that were used in the exploratory analyses.

The independent/predictor variables used in the exploratory analyses were school type, location, type of security personnel, size, and the number of CCTV cameras at each school. Specifically, Exploratory Analyses 1- 3 used chi-squared tests for independence and Exploratory Analyses 4 and 5 used logistic regression.

The independent variable for Exploratory Analysis 1 was the type of school (four-year private college, four-year public college, and two-year public/private college); the independent variable for Exploratory Analysis 2 was campus location (metropolitan/inner city, urban, urban-adjacent, and rural). The independent variable for Exploratory Analysis 3 was the type of security personnel at each campus (sworn officers, unsworn officers, and a combination of sworn and unsworn officers). The predictor variable for Exploratory Analysis 4 was school size and was measured by the number of enrolled students and the predictor variable for Exploratory Analysis 5 was the number of CCTV. Displayed in Table 4.23 is a summary of the variables and statistical tests used to evaluate the four exploratory analyses.

Table 4.23

Summary of Variables and Statistical Tests used to Evaluate Exploratory Analyses 1-5

Exploratory Analysis	Dependent/Criterion Variable	Independent/Predictor Variable	Statistical Test
1	CCTV Written Policy	School Type	Chi-squared Test for Independence
2	CCTV Written Policy	Campus Location	Chi-squared Test for Independence
3	CCTV Written Policy	Type of Security	Chi-squared Test for Independence
4	CCTV Written Policy	School Size	Logistic Regression
5	CCTV Written Policy	Number of Cameras	Logistic Regression

Exploratory analysis 1. Using SPSS, Exploratory Analysis 1 used chi-squared test for independence to determine if significant associations existed between school type and whether schools had a written camera policy. Results indicated that a significant association did not exist between school type (four-year private colleges, four-year public colleges, and two-year public/private colleges) and CCTV written policy (yes and no), $\chi 2(2) = 5.497$, $p = .064$, Cramer's V = 0.265. Cramer's V is the effect size for cross tabulations larger than 2x2 whereas the most commonly reported effect size for 2x2 cross tabulations is the phi coefficient (Huck, 2012). These results suggest that the type of school did not determine whether the school had a written camera policy. A cross tabulation of school type and CCTV written policy is displayed in Table 4.24.

Table 4.24

Cross Tabulation of School Type and CCTV Written Camera Policy

	CCTV Written Policy		
School Type	Yes	No	Total
4-year Private College	24	23	47
4-year Public College	5	10	15
2-year Public/Private College	12	4	16
Total	41	37	78

Note. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.12.

Exploratory analysis 2. Exploratory Analysis 2 used chi-squared test for independence to determine if significant associations existed between schools with written camera policies and schools without written camera policies and the location of their campus. Results indicated that a significant association did not exist between the location of a campus (metropolitan/inner city, urban, urban-adjacent, and rural) and CCTV written policy, $\chi 2(3) = 2.041$, $p = .564$, Cramer's $V = 0.162$. These results suggest that the schools' location did not determine whether the schools had a written camera policy. A cross tabulation of campus location and CCTV written policy is displayed in Table 4.25.

Table 4.25

Cross Tabulation of Campus Location and CCTV Written Camera Policy

	CCTV Written Policy		
School Type	Yes	No	Total
Metropolitan	10	12	22
Urban	14	9	23
Urban-adjacent	6	9	15
Rural	10	8	18
Total	40	38	78

Note. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.31.

Exploratory analysis 3. Exploratory Analysis 3 used a chi-squared test for independence to determine if significant associations existed between the type of security personnel and whether schools had a written camera policy. Results indicated that a significant association did not exist between different types of security personnel (sworn officers, unsworn officers, and a combination of sworn and unsworn officers) and CCTV written policy (yes and no), $\chi 2(2) = 0.177$, $p = .915$, Cramer's $V = 0.047$. These results suggest that schools with a written camera policy had similar occurrences of sworn, unsworn and combination of security personnel as schools without a written camera policy. Displayed in Table 4.26 is a cross tabulation of type of security personnel and CCTV written policy.

Table 4.26

Cross Tabulation of Type of Security Personnel and CCTV Written Camera Policy

	CCTV Written Policy		
Type of Security Personnel	Yes	No	Total
Sworn Officers	7	7	14
Unsworn Officers	17	14	31
Combination of Sworn and Unsworn Officers	17	17	34
Total	41	38	79

Note. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.73.

Exploratory analysis 4. Using SPSS, Exploratory Analysis 4 was evaluated using logistic regression to determine if the number of students enrolled, (school size) predicts whether the school has a written camera policy. The null hypothesis tested in Exploratory Analysis 4 was that there is no significant difference between the number of students enrolled in a college and the frequency of negative responses to having a written CCTV policy. Table 4.27 shows the observed results of the survey versus the expected results.

Results indicated that school size did not predict CCTV written policy, $\chi^2(1, n = 80) = 1.997$, $p = .158$. School size explained between 2.5% (Cox and Snell R square = .025) and 3.3% (Nagelkerke R square = .033) of the variance observed in CCTV written policy. Cox &Snell R square and Nagelkerke R square are commonly reported "pseudo-measurability" r-squared statistics that provide an indication of the amount of variation observed in the dependent variable (Huck, 2012, p. 399). Huck (2012), reports that

logistic regression does not calculate the regular r-square statistic that other forms of regression use. At this time, the research was unable to reject the null hypothesis.

Table 4.27

Comparison of Observed Versus Expected Results for School Size

Number of Students	CCTV Written Policy Yes		CCTV Written Policy No		Total
	Observed	Expected	Observed	Expected	
Under 1500	5	4.746	2	2.254	7
1501-2500	6	4.317	1	2.683	7
2501-5000	5	7.359	8	5.641	13
5001-7500	2	1.590	1	1.410	3
7501-10000	4	6.005	8	5.995	12
10001-20000	7	6.121	6	6.879	13
20001-35000	10	8.387	9	10.613	19
35001 or more	2	2.475	4	3.525	6

Exploratory analysis 5. Exploratory analysis 5 was evaluated using logistic regression to determine if the number of cameras on college campuses predicts whether the school has a written camera policy. The null hypothesis tested in Exploratory Analysis 5 was that there is no significant difference between the number of cameras a college has installed on campus and the frequency of negative responses to having a written CCTV policy.

Results indicated that the number of cameras did not predict CCTV written policy, $\chi^2(1, n = 88) = 2.515, p = .113$. The number of cameras explained between 2.8% (Cox and Snell R square = .028) and 3.8% (Nagelkerke R square = .038) of the variance observed in CCTV written policy. At this time, the research was unable to reject the null hypothesis.

Table 4.28

Comparison of Observed Versus Expected Results for Number of Cameras

Number of Cameras	CCTV Written Policy Yes		CCTV Written Policy No		
	Observed	Expected	Observed	Expected	Total
501or more	7	7.258	4	3.742	11
201-500	11	10.280	7	7.720	18
101-200	10	10.426	11	10.574	21
100 or less	16	16.036	22	21.964	38

The results of the five Exploratory Analyses and the corresponding statistical significance are listed on Table 4.29. It is noted that no analysis reached a set level of significant of $p < .05$ to reject the null hypothesis. All five analyses revealed no significant relationship between the independent and dependent variables. The null hypothesis was not rejected in any of the five analyses.

Table 4.29

Summary of Results for Exploratory Analyses 1-5

Exploratory Analysis	Dependent/Criterion Variable	Independent/Predictor Variable	Statistical Test	Sig.
1	CCTV Written Policy	School Type	Chi-squared test for Independence	.064
2	CCTV Written Policy	Campus Location	Chi-squared Test for Independence	.564
3	CCTV Written Policy	Type of Security	Chi-squared test for Independence	.915
4	CCTV Written Policy	School Size	Logistic Regression	.158
5	CCTV Written Policy	Number of Cameras	Logistic Regression	.113

Summary of Results

This research study was designed to analyze the CCTV policies of colleges and universities. Specifically the study looked at how college's policies met the Baldrige Criteria related to *Approach, Deployment, Learning*, and *Integration* (National Institute of Standards and Technology, 2011-2012).

The study results were obtained from an Internet-based survey of security and public safety professionals at institutions of higher education in the Mid-Atlantic United

States. The population of 265 colleges and universities resulted in a voluntary return rate of 96 participants.

The demographic information on each participating college was self-identified by their security professional. The colleges consisted of a mix of public, private, two-year, and four-year institutions. Colleges were located in metropolitan, urban, and rural areas. The sizes of the student populations at the participating colleges varied from, under 1500 to over 35,000 students.

The types of security departments varied between participating schools. The schools employed either armed, unarmed, or a mix or armed and unarmed security personnel.

The 96 colleges participating in the survey reported that 96.9 % used CCTV cameras on campus, yet only 47.3% had written policies regulation the use of the cameras. An additional 24.7% reported they were in the process of developing a policy regulating CCTV use on campus.

The survey then questioned the participants on the content and administration of their colleges CCTV policies. The Baldrige Criteria of *Approach* (National Institute of Standards and Technology, 2011-2012) is related to the methods an organization uses to accomplish a desired outcome, and the effectiveness of that outcome. The investigation of Research Question 1 required the survey questions to examine the approach colleges used to develop policies that regulate the ethical use of CCTV cameras on their campuses.

Consistently, the development, maintenance, and enforcement of the policy were the responsibility of the college's security or public safety department. The colleges'

security departments would determine where to put in cameras, how long to keep recorded video, and who had the right to view live and recorded video data.

The colleges surveyed varied in the length of time recorded CCTV data is stored. Participants reported recording times of less than seven days for some colleges, to over 120 days for other CCTV systems. Multiple colleges reported that recording times even varied among cameras located on their individual campuses.

Most colleges had policies in place either verbally or in written form, restricting viewing of live and recorded video. The majority restricted live viewing to security or law enforcement personnel. Viewing of previously recorded video was restricted on most campuses to emergencies or after a reported incident. These practices or policies also restricted the copying and dissemination of video. Participants consistently reported in the survey that colleges required the permission of the person in charge of security, or a subpoena, prior to releasing recorded video.

The issues of privacy were addressed in the survey as it related to cameras in public spaces. The survey questioned if colleges had guidelines regulating the monitoring of non-criminal activities on campus. While 48.4 % stated they had policies restricting non-criminal viewing, when the term non-criminal was described, in detail, as non-violent protests and/or student events that number dropped to 33.3%.

Research Questions 2 and 3, addressed the Baldrige Criteria of Deployment (National Institute of Standards and Technology, 2011-2012). Deployment pertains to the consistent application of the college's policies throughout the organization.

The survey results showed that most colleges did not openly communicate their CCTV policies either publicly or throughout their organization. Nor did they involve the

college community in developing their CCTV policy. Only 10.8% of the CCTV policies were availably publicly and 41.9 % were restricted to viewing by security personnel only. The policy development at 60.2% of the colleges surveyed was the sole responsibility of the security personnel. Only 11.8 % of the colleges allowed input from their faculty and staff and only 5.4% from their student population.

The amount of required training for college personnel on the ethical use of CCTV cameras and the safeguarding of CCTV data varied among colleges. Participants varied in their responses, from reporting that their colleges trained security personnel on CCTV once a month to other colleges stating they have never trained their personnel. Some colleges had a program to train all new personnel on the policies related to CCTV and only re-trained if their policy changed. Other colleges trained on a consistent basis and CCTV training was part of their scheduled training regime. Yet, the majority of colleges did not have any policy requiring security personnel to sign a document stating that they understand, and have received, the college's CCTV policy.

The survey addressed Research Question 4 by questioning participants on how often their college updated or reviewed their current CCTV policy. This research question is related to the Baldrige Criteria of Learning (National Institute of Standards and Technology, 2011-2012). Learning relates to how often your organization evaluates policies and procedures to keep it relevant.

Interestingly, 68.8% of the survey participants did not answer the two questions related to how old their CCTV policy is and how often the policy is updated. Of the remaining 29 participants who did answer, 10 schools have never reviewed or updated their policy in the last five years and 16 had reviewed or updated it 1-2 times. Two

colleges had reviewed or updated it 3-4 times, and only one had reviewed or updated their CCTV policy at least five times in the past five years.

The final portion of the survey addressed Research Question 5. How do colleges integrate their ethical use of CCTV policy with other ethical university policies, such as sexual harassment or discrimination? The question relates to the Baldrige Criteria of Integration (National Institute of Standards and Technology, 2011-2012). Integration is how your policy or process integrates with the organizations other policies and procedures.

The analysis of the survey results showed that a majority of colleges do not include or integrate their college's existing policies related to ethics, discrimination, and harassment in their ethical use of CCTV policy. Only 20.4 % of the colleges include integration of sexual harassment guidelines in their CCTV policy and 34.4 % include discrimination language.

Exploratory analyses were conducted of the research data related to the research hypotheses *Ho1-Ho5*. The five analyses were conducted using SPSS data analysis software. The first three tests, Exploratory Analysis 1-3, were conducted using Chi-squared tests for independence, and the last two tests, Exploratory Analysis 4 and 5, using logistic regression. The dependent/predictor variable for all five tests was if the schools had a written CCTV policy. The independent variables in the exploratory analysis were school type, location, type of security personnel, school size, and the number of CCTV cameras at each school.

None of the five analyses could disprove the null hypotheses. The results showed that neither school type, size, location, number of cameras, nor type of security personnel

determined if schools had an ethical use of CCTV policy. There was no significant association between the demographic information on the school and the existence of a policy. The research could not show any determining factors as to why a school had or did not have a written policy regulating the ethical use of CCTV on their campus.

Chapter 5: Discussion

Introduction

Colleges are using CCTV cameras routinely on their campuses for crime prevention and monitoring purposes. While almost 98% of the colleges surveyed in this study had surveillance camera systems installed on their campuses, less than 48% have any written policy regulating the placement or use of these cameras.

The objective of this study and the development of the research questions were designed to assess if a well-developed CCTV policy will prevent or deter the unethical use of video surveillance equipment and the video data recorded on this equipment in a university setting. There is no current standard to guide the industry or structured model policy for all colleges to follow. This supports the need for development of a single standard and model template of regulating CCTV policy requirements on college campuses.

This research investigated how colleges develop, deploy, evaluate, and integrate policies related to the ethical use of CCTV on campuses. Current college policies and security industry best practices recommendations related to CCTV were evaluated to develop an Internet-based survey instrument. The survey, administered to college security and public safety directors in the Mid-Atlantic United States was designed to assess if colleges had CCTV policies and if so, how they developed and administered those policies. The recommendations of this study are developed from the literary research and an analysis of the survey responses.

The recommendations resulting from this study include suggested mandated sections for inclusion in all colleges CCTV policies. These include recommendations for colleges to align their future policies with the Baldrige Criteria of Approach, Deployment, Learning, and Integration (National Institute of Standards and Technology, 2011-2012). This alignment ensures that future college policies are well thought out and effective.

After their CCTV policy is developed, schools must ensure that they communicate their policy to all pertinent parties and that training is conducted on an ongoing basis. All policies need constant review, and updating when appropriate, to ensure that they remain fresh and relevant as technologies and legal standards change.

Finally, colleges must ensure that all ethical policies at the university are integrated. This includes provisions in this research's proposed standards for CCTV policy that integrates the specific guidelines of individual colleges as it relates to their Sexual Harassment, Discrimination and other ethical policies.

Implications of Findings

The implications of the findings are discussed as they relate to the five research questions. Included in this discussion is the relationship to the three crime theories; rational choice, routine activities, and social learning theories, to the results of the research.

Research question 1. How do colleges and universities develop policies regulating the ethical use of CCTV technology on their campus? The colleges that did have written CCTV policies report that they primarily developed the policies with little input from anyone outside of their public safety or security department. Only 3% of the

schools have camera or CCTV committees who are responsible for policies related to surveillance cameras. A few schools include either the legal entity from the college or the human resources department in CCTV policy decisions but the security department is primarily responsible for CCTV policy development.

Most college's security departments that reported having a CCTV policy are subject to little oversight from outside their department, in the development or maintenance of that policy. Two colleges report that they do not have a written CCTV policy because only the Director of Security has access to the cameras. In that situation, the research supports that outside oversight by another department is justified to prevent any appearance or actual impropriety in use of the CCTV system. This justification is further supported by the responses summited by 75.3% of the participants stating that their security department is also solely responsible for investigating any allegations of misuse of the college CCTV system or the recorded video data on the system.

The Baldrige Criteria of Approach (National Institute of Standards and Technology, 2011-2012) assessed the appropriateness of this method of policy development as lacking in thoroughness and transparency. An effective policy includes the entire organization in the evaluation process with all departments having an opportunity for input. By limiting the input on CCTV policy to one department, even though the system potentially effects the entire organization, fails to consider ideas and evaluations of outside entities.

The findings of the study reveal that less than half of the colleges participating in the survey actually have written CCTV policies. One of the respondents even commented on the survey that their CCTV cameras were in all public places so they did

not need a policy, as there was no legal expectation of privacy. Solove (2011) and Goold (2006) would argue that even though there may not be a legal expectation of privacy the institution should take every measure to protect the individuals whose images were captured on their CCTV systems. This study supports the implication that having a strong policy does not infringe on the college's right to videotape but it does protect an individual from having their image unnecessarily released to the public without cause.

The colleges that did not have formal written policies regulated the use of their CCTV systems through various less formal guidelines. Many colleges state that they verbally train employees on camera use and others used written memos. Of concern to this research was that 33.3% of the respondents report that they address each incident as it happens, forgoing any formal policy. Crime theories support that having a strong policy provides a deterrent to poor behavior. The lack of any policy leaves open opportunities for those operators of CCTV cameras who may be inclined to act in an unethical manner.

Rational choice theory supports the use of a strong written policy as a deterrent to criminal or unethical behavior. The effect of a strong CCTV policy outlining the penalties for violating the standards may serve as a deterrent to unethical operators of the systems, if the risk outweighs the rewards (Cornish & Clarke, 1987). The lack of a strong policy eliminates this penalty as a deterrent.

The majority of colleges that have written CCTV policies include guidelines on viewing live and recorded video. Most security departments restrict viewing to authorized personnel only and limit the viewing of recorded video to emergencies. This serves to protect the data and prevents viewing of recorded data for voyeuristic purposes.

Also equally important, is the restriction included in most college policies regulating the copying or distribution of video data without permission. This restriction places strong deterrents on copying of video data for personal reasons. It also protects the privacy of individuals by preventing the unauthorized release of video data to social media or the press.

The need for a strong policy is further supported by routine activities theory. Camera operators, not bound by a written policy acting as a guardian over the operator's behavior, may use the cameras in an unethical manner. A strong policy may prevent the voyeuristic behavior of a bored operator or the targeting of a person based solely on race or sex if guidelines for use of the cameras include prohibition on targeting non-criminal behavior (Norris & Armstrong, 1998).

The survey participants were asked two questions related to monitoring of non-criminal activities. The first asked if their college's policy included guidelines for monitoring of non-criminal activities on campus. This distinction is important, as students on campus should feel free to participate in college activities without fear of being targeted for surveillance. While 56% of the schools state their policy restricts monitoring of non-criminal activity, that number dropped to 40% when non-criminal activity was described as student protests and student events. Additionally, three participants skipped the more descriptive question.

Colleges that do not restrict the monitoring of non-criminal, peaceful student events are not recognizing the students' rights to peacefully assemble. If students feel, their activities are recorded and subject to unrestricted review, they may not feel comfortable engaging in many student activities. The American Civil Liberties Union

(King et al., 2008) recommends that cameras not be actively monitored. While that may be an excessive guideline in all circumstances, it does prevent unwarranted targeting of innocent behavior.

While public spaces do not permit a person to have any expectation of privacy, as they are already in the public eye, a person would not expect to be subject to surveillance in private areas. Solove (2011a) asserts that a person has an expectation of privacy in certain areas. These private areas may include private offices, dorm rooms, bathrooms, and locker rooms. Most colleges that do have policies include a section restricting installation in places were persons have a reasonable expectation of privacy. Unfortunately, there are still schools that do not include any limitations on where cameras are installed. It is important that safeguards are in place to protect an individual's privacy and prevent release of potentially compromising video.

Research question 2. How do colleges communicate their ethical use of CCTV policies to their security or public safety personnel? The questions on the survey aligned to research question two and research question three are related to the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) of Deployment. The Baldrige Criteria (2011-2012) of Deployment is best described as the colleges' ability to employ the policy consistently throughout the organization. This would include training of personal on the content of the policy and ensuring that all departments follow the policy.

The survey questions asked if security personnel receive formal training on their college's CCTV policy. The participants from those schools that do conduct training were asked how often they train or retrain their security personnel on their CCTV policy.

Only 21.6% of the responses state their college trains on their policy at least once per year. Over 31% of the colleges only train personnel when they are hired or promoted and have no provisions for ongoing training. Nearly 10% of the colleges state they never train personnel on their CCTV policy.

Reinforcement of existing policies through ongoing training is important. Akers' social learning theory (Akers & Jensen, 2009) supports the effect of a person's peer group, social structure, and environment on their values. If the college is not influencing the camera operator's behavior through constant training and reinforcement of the correct and ethical use of cameras, less ethical social pressures may reinforce the operator's behavior. Colleges must train their personnel to understand the responsibilities of using a CCTV system, and the consequences of any misuse. If proper training is not conducted, these procedures may be unclear to the camera operator, or discounted as unimportant. If the operators' believe the reward or peer recognition for voyeuristic or unethical behavior outweighs the punishment, inappropriate behavior may occur. Strong rules and penalties that are consistently enforced will help to curb any unethical behavior (Caron, 1998).

Colleges need to reinforce the importance of their CCTV policies through training. Additionally, everyone that receives CCTV training should sign a document acknowledging they are aware of, and agree to follow the policy. Over 50% of the participating schools surveyed do not require any documentation attesting to the receipt of required training. Requiring a camera operator to sign a document that they understand the guidelines for using the surveillance system serves to reinforce the importance placed by the organization of that policy.

Research question 3. How do colleges communicate their ethical use of CCTV policies to their student, faculty, and staff populations? Related to the Baldrige Criteria of Deployment (National Institute of Standards and Technology, 2011-2012) as stated above, the survey questions developed to answer research question 3, determine how colleges communicate their CCTV policy to the members of the college or university community, who were not members of their security or public safety departments. According to the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) successful deployment of a policy should include the entire organization. The survey results show that the majority of colleges that do have policies do not make the policy available to anyone outside of their security department. Only 10% of the colleges have open policies that were publicly available to anyone on the Internet.

Participants were asked if anyone in departments, other than security or public safety at their college, had input into the development or implementation of their CCTV policy. The majority of the schools do not involve any other departments in developing their CCTV policy and only 5% of the schools report permitting student involvement in the process.

These results are is in direct conflict with the recommendations of the U.S. Department of Homeland Security (2007) who recommends that operators of CCTV systems welcome public inspection to build trust and the City of San Francisco (Community Safety Camera Ordinance, 2006) which mandates public input prior to camera installation.

The state of Nevada regulates the requirements for camera use on Nevada college campuses (Nevada Revised Statutes, 1993). Nevada statute mandates colleges have a

Committee on Video Surveillance. This video committee is responsible for developing, implementing, and regulating camera policy on campus. The committee must include representatives from multiple departments, union members, and students. This is an excellent example of an inclusive policy that is transparent at every level of the organization.

Research question 4. How do colleges ensure that their CCTV policies remain up-to-date as technology and university needs change? Learning, as it applies to the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012), refers to colleges' evaluation and training processes promoting improvement and innovation in their organization. Inconsistences in the requirement for training, and timeliness of the training related to the use of CCTV of security personnel, were discussed previously. Lack of standardized and mandated training and retraining of personnel on the CCTV policies prevents reinforcement of the rules and procedures. Equally important is keeping policies updated as the needs of the college and technology evolves.

An effective CCTV policy should be reviewed and updated regularly to remain current. The technologies related to CCTV systems are evolving quickly. Policies developed only 10 years ago may include instructions for the reuse of VCR tapes. This is an outdated technology. Recording surveillance video on a VCR has been replaced by high definition digital systems that stream over wireless networks and may be viewed on a Security Director's smart phone. If the college has not reviewed or updated their CCTV policy in years, they are vulnerable to misuse.

Participants were asked how often in the last five years they had updated or reviewed their college's CCTV policy. Slightly over 10% responded that they have

reviewed it at least three times in the previous five years. Over 34 % report they have never reviewed their policy in the past five years. The lack of review and failure to maintain an updated policy is difficult to understand.

Digital technologies require rules and procedures that that are fresh and innovative. Security departments must address the introduction of Facebook, Twitter, and other social media technologies and their impact on safeguarding CCTV systems. The amount of video data that can be copied in seconds onto a small thumb drive makes security of data essential. Colleges guided by CCTV policies older than, or unchanged in over five years old may not have imagined the widespread changes in technology when developing these policies. Yet 24% of the participants report that their college has never updated their CCTV policy. As technology changes so must the policies regulating these technologies.

Research question 5. How do colleges integrate their university's ethical use of CCTV policies with their university's' other ethical policies, such as sexual harassment and discrimination? CCTV technology as discussed previously is vulnerable to misuse by unethical or untrained camera system operators. Lyon (2002) advises that unethical use of cameras could result in social sorting of unwanted persons in the surveillance area. Whether that sorting is based merely on age, sex, race, or other bias, it is improper to target non-criminal behavior. The development of research question 5 was designed to analyze how colleges integrated their policies developed to prevent discrimination and sexual harassment on their campus, into their CCTV policy.

Integration is described in the Baldrige Criteria (National Institute of Standards and Technology, 2011-2012) as the alignment of all policies, plans, and goals of an

organization. The expectation is that all policies in a college support the mission and values of the college, and demand compliance with all ethical standards of conduct.

The inclusion in a CCTV policy, guiding the behavior of a camera operator, of a prohibition on sexual harassment or racial discrimination seems appropriate. While every college had a policy for both sexual harassment and racial discrimination only 34.4 % of participants report their CCTV policy includes guidelines for monitoring a person solely on race, ethnic origin, or sexual preference. Even fewer colleges, 20.4% integrate the schools policy on sexual harassment in their CCTV policy. Integration of all ethical behavior policies into their college's CCTV policy is important to set a standard of use for the camera operators.

Exploratory analyses. After analyzing, the survey responses using inferential statistics the researcher was able to tabulate the scores collected and summarize the values. Demographic statistics provided the count and percentile statistics. Because of these analyses, it was apparent that many schools did not have written policies. The original expectation of this study intended to assess if colleges had CCTV policies and if so, how they develop and administer these policies. What was unexpected was the number of schools that had active CCTV systems on their campuses, yet no formal policy. Further exploratory analyses were conducted to determine if significant associations exists in schools with written CCTV policies compared to schools without written CCTV policies.

Five exploratory analyses were conducted on the survey response data. Three analyses use a chi-squared test for independence and two use logistic regression. The independent variables for these three tests, using the chi-squared test for independence,

are the type of school (four-year public, four-year private, and two-year public/private); campus location (metropolitan/inner city, urban, urban adjacent, and rural); and the type of security personnel on campus (sworn, unsworn, and a combination of sworn and unsworn officer). The dependent variable for all three tests is whether the schools have a written CCTV policy.

The result of the analyses reveals that no significant association exists between school type, location, or type of security department and whether they have a written CCTV policy. Four-year universities in major cities with sworn, armed police officers had the same percentage of CCTV policies as small, unsworn, two-year rural community colleges.

The final two analyses conducted use logistical regression to determine if the school size or the total number of cameras on campus could predict whether a college has a CCTV policy. These two predictors are chosen to see if the size of the student population or the size of the camera surveillance system predicts if a school has developed a CCTV policy. There are no significant differences between student population or the size of a colleges CCTV system, and the presence of a written CCTV policy.

The outcome of all the exploratory analyses is that there are no observed factors that attribute to the presence of a written camera policy. Four of the schools that do not have a policy, have over 500 cameras installed on their campus. Regulating a camera system that large without policies and procedures seems a daunting task. There was no explanation discovered by this research why more than 50% of the colleges who use

camera surveillance on their campus do not have a policy regulating the use of CCTV technology.

Limitations

Although efforts were made to minimize the gaps and limitations in this study, they did exist. The survey population is limited to a sample group of a specific organization. Only colleges that are members of IACLEA and located in the Mid-Atlantic region of the United States were asked to take part in this study. Although not uncommon for Internet-based surveys to have response rates of less than 20%, an increase on this study's return rate of 38% would provide a more representative sample (Witmer, Colman, & Katzman, 1999). Additionally, only Directors and Chiefs of the respective Security and Public Safety Departments participated in the survey. College administrators, students, and personnel in non-security related departments are not included in this study.

This research obtained responses by surveying the entire population of IACLEA member colleges in the Mid-Atlantic region. Therefore, the results of this study may be representative of all colleges inside of this region, but the results cannot be generalized on a larger scale without expanding the survey population outside of one area of the United States.

The distribution of the survey was conducted by sending an email to the listed email addresses of the Director or Chief of each college in the Mid-Atlantic region. Some participants may have feared releasing information electronically if the researcher could trace the origin of each survey response. Although anonymity was guaranteed to participants in the survey's consent agreement, security professionals are trained to

protect confidential information. This may partially explain why on two sensitive questions related to inclusion of Sexual Harassment and Discrimination policies in the CCTV policy, a higher than average number of participants skipped those two questions. If a college fails to include one or two of those important policies in their ethical use of CCTV policy, publicizing that oversight may not be in the schools best interest.

Recommendations

The research in this study reveals that nearly every college surveyed (97.89%) use CCTV or another method of video surveillance on their campus. The original purposes of this study was determine if colleges have CCTV policies regulating the use of cameras on campus and evaluate how they develop and administer those policies. Security professionals may use the study results to develop a set of standard guidelines, and recommendations, that colleges could use to develop ethical use of CCTV camera policies in the future. What was an unexpected result of this study was the number of colleges that do not have formal written CCTV policies. Less than 48% of the colleges surveyed have any written policy regulating the use of the cameras.

The large number of schools reporting the lack of a formal policy regulating the ethical use of their camera system supports the need for mandating a written comprehensive CCTV policy. Privacy issues outlined in the literature related to use of cameras such as, unauthorized release of video to the press or putting video on social media make this an important requirement. FERPA (Department of Education, 2008) regulates the privacy of student information yet recorded images of student activities occurring in the public view of surveillance cameras are unregulated. Students, faculty, and staff at all colleges deserve every protection possible from the unauthorized release

of CCTV video without their permission. Once video is released publicly that wrongly violates a person's right to privacy, that privacy can never be restored (Gallagher, 2004).

While the majority of colleges report they do not have written CCTV policies, 25% of the participants report they are currently developing a policy. Further qualitative research should investigate why there is a lack of quality and consistency in developing CCTV policies at these colleges. Law enforcement as a field is highly regulated by law. The research participants representing the law enforcement arm of their colleges acknowledged the need for policy but do not seem able to complete the task. Research should investigate if the academic environment and/or oversight prevent agreement on development and distribution of regulatory policies. Higher education by nature is more collaborative and collegial then law enforcement, which has a paramilitary structure. Does a need for collaborative agreement on policy prevent approval of a final product? What other factors are effecting the creation and implementation of CCTV policies that the survey participants acknowledged, was necessary.

Replication of this survey with a larger sample population including all regions of the United States and colleges that are not members of IACLEA would provide a larger sample. While many colleges are members of IACLEA, it is not all-inclusive and to sample every college the population would need to expand outside this organization.

Addition of a survey question asking if the Commission on Accreditation for Law Enforcement Agencies (CALEA) or similar accrediting agency accredits the college security department is recommended. CALEA requires a law enforcement or campus security department "to develop a comprehensive, well thought out, uniform set of written directives" (CALEA® | The Commission on Accreditation for Law Enforcement

Agencies, Inc., 2013, para. 7). This requirement for accredited college public safety departments to document all policies may show this as a predictor if a college would have a written CCTV policy.

The prior research on this topic and the results of the study reveal a gap in the industry. College security departments have no single resource to obtain a comprehensive template for developing their CCTV policy. Using the survey responses and available best practices, college security professionals should develop and publish a formal set of guidelines for CCTV policy implementation. It is recommended these guidelines include instructions on how colleges should: (a) develop a CCTV plan to fit a college's specific needs; (b) integrate all the ethic policies such as discrimination and sexual harassment in the plan; (c) implement staff training requirements that requires regular refresher training on the ethical use of CCTV; and (d) ensure timely review of the CCTV policy to ensure that it remains up-to-date as technology and legal statutes change. Making these guidelines available to security professionals inside and outside of higher education will add consistency to CCTV policy planning.

Conclusion

This study focused on the policies colleges use to regulate the ethical use of Closed Circuit Television (CCTV) cameras on their campuses. The methods the colleges use to develop, deploy, evaluate, and integrate these policies was of particular interest. The research uses the Baldrige Criteria of process scoring evaluation dimensions, Approach, Deployment, Learning, and Integration (National Institute of Standards and Technology, 2011-2012) as the basis for assessing the quality of existing college CCTV policies.

The availability of prior literature and research related specifically to industry-wide standards for CCTV policies at colleges were limited. Many colleges have developed their CCTV policy yet not integrated other college ethical policies regulating discrimination and sexual harassment. Other college's policies do not address issues related to unauthorized copying and distribution of recorded video data. This research supports the need for an industry-wide model for CCTV policy development.

The study uses a quantitative Internet-based survey issued to college and university security professionals in the Mid-Atlantic region of the United States. All colleges in the survey population are members of the International Association of Campus Law Enforcement Administrators (IACLEA). The survey requests participants respond to questions related to the development of their college's CCTV policy and demographic data.

The survey instrument was developed using the research on the literature including policies currently in use by colleges in the United States (Bates College, 2008; Franklin and Marshall College, 2008; Johns Hopkins University, 2005; Syracuse University, 2012; University of Nevada, 2006) and United Kingdom (Callington Community College, 2011; Canterbury Christ Church University, 2006; London South Bank University, 2010). Additionally, current CCTV industry best-practice recommendations from the United States Department of Homeland Security (2007), ACLU (King et al., 2008), the City of San Francisco (Community Safety Camera Ordinance, 2006) and the Data Protection Act of 1998 (Elizabeth II, 1998) are used for content development. These sources of literature were coded for common themes and from these themes, the initial questions were developed.

As this is a new survey instrument, reliability and validity had to be established prior to use. The survey consists of fixed answer multiple-choice questions with both open and closed-end response choices. The survey design uses Likert-type response choices. The questions consist of fixed response multiple-choice questions with an option to add additional open-ended information in a comment box

To establish validity and reliability a panel of nine experts in the college security field was used. The panel members were given the initial survey as a pre-test and requested to read the questions for validity and construct. A pre-test is a smaller scale distribution of the survey to a convenience group, in this case the panel of experts (Rea & Parker, 2005). Validity requires that the questions measured what they are purported to measure and that the participants interpret the questions as the researcher intended (Czaja & Blair, 2005). The panelists then returned the survey with written comments.

After review of the panel's responses questions were reworded for clarity and mechanical flaws in the electronic survey were corrected. Two questions from the original survey were eliminated from the final research version of the survey instrument. The first was redundant and unnecessary and the second was not directly related to the subject of the study. A corrected version of the survey was finalized and prepared for test distribution to the panelists.

The test survey was distributed to the nine panelists via an Internet link to replicate the manner the survey will be delivered to the research participants. The nine test survey responses were returned electronically.

The members of the expert panel returned the survey via SurveyMonkey an on-line survey tool. The data from this test of the survey instrument revealed the survey

mechanically sound and all responses recorded accurately. The only three comments from the panelists were related to typographical errors on the survey. These errors were corrected on the next version of the survey.

Ten days later the panel was then distributed the same test, with minor corrections (Kelley, 1999). Similar to the previous test the re-test was sent via the Internet using SurveyMonkey. The members of the expert panel had not been informed previously that a second re-test would be sent. The original link to the survey instrument was no longer valid so the panelists could not compare, or copy, their previous survey responses.

The re-test resulted in the return of all nine surveys. The analysis of the responses to the re-test revealed the survey results were statistically similar. The only difference from the test to the re-test was the lack of open-ended comments. The second test did not include comments containing additional information about the individual college's CCTV policies. Upon questioning of the panelists, they stated they had provided that information of the previous version of the survey. All fixed answer questions revealed test-retest reliability (Patten, 2009). Members of the expert panel were not eligible to participate in the research survey.

After establishing reliability and validity, the Internet-based survey was issued to the research participants, 265 Security Directors at colleges and universities in the Mid-Atlantic region of the United States. All participating colleges are members of IACLEA, an organization for college law enforcement professionals. The survey responses were returned electronically at a rate of 38%.

The survey results were analyzed using Statistical Package for the Social Sciences (SPSS) statistical analysis software. Inferential statistics were used to draw conclusions

from the samples tested. The statistical analysis on the demographic data included percentage and frequency of responses. Descriptive statistics and analysis of the quantitative data were used to assess the research questions.

The analysis of the survey responses determined that less than 50% of the colleges participating in the study actually have a written CCTV policy. The purpose of this study is to determine how colleges develop, deploy, evaluate, and integrate policies regulating the use of CCTV on their campuses. The unexpected result is identifying how many colleges have not yet developed a CCTV policy for their school.

Further exploratory analyses were conducted using chi-squared test of independence and logistic regression analyses. These chi-squared tests for independence are used to determine if any significant associations exist in the school type, location, or type of security department between schools with written CCTV policies and schools without a written CCTV policy. Additionally, logistic regression analyses are used to determine if school size or the number of cameras a school has installed on campus are predictors that can be used to determine if a college has a written CCTV policy.

The results of chi-squared tests for independence is that there is no significant association between any of the independent variables; school type, location, or type of security and the dependent variable, and whether a school has a written CCTV plan. The result of the logistic regression test is that neither school size nor number of cameras installed on the college's campus can predict whether a school has a written CCTV policy. Therefore, after analysis of the research data the study is unable to reject the five null hypotheses.

The small sample size and participants drawn only from a single organization's geographical region limited this study. Further research on a larger scale will increase the generalizability of these results. I recommend that further studies research the possible reasons security departments in higher education institutions do not have written policies regulating the use of surveillance cameras on their campuses. Lack of policies regulating the monitoring of cameras, and restricting the unauthorized release of recorded video, has potential implications on the privacy of their students, faculty, and staff.

Development of a single resource where colleges may obtain information and templates to help them develop, deploy, evaluate, and integrate a policy regulating the ethical use of CCTV technology on their campus is necessary. Consistency in the guidelines colleges are using to safeguard the privacy of their students and staff, as it relates to CCTV, will enable colleges to ensure that cameras are maintained as a crime prevention tool and not an ethical liability.

References

Adams, H. E. (2000). Voyeurism. In *Encyclopedia of Psychology* (Vol. 8, pp. 216-218). New York, NY: Oxford University Press. doi:10.1037/10523-084

Akers, R. L., & Jensen, G. F. (2009). *Social learning theory and the explaination of crime.* New Brunswick: Transaction Publishers.

Armitage, R. (2002). *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime.* NACRO. Community Safety Practice Briefing.

Armitage, R., Smyth, G., & Pease, K. (1999). Burnley CCTV evaluation. *Surveillance of Public Space, CCTV, Street Lighting and Crime Prevention*. (K. Painter, & N. Tilley, Eds.) Monsey, New York: Criminal Justice Press.

Baile, N. (2008). *Expert findings on surveillance cameras: What criminologist and others studying cameras have found.* The ACLU Technology and Liberty Program. Retrieved January 6, 2012, from http://www.aclu.org/files/images/asset_upload_file708_35775.pdf

Bates College. (2008, May 27). *CCTV Monitoring Policy*. Retrieved October 14, 2012, from Security & Campus Safety: http://www.bates.edu/security/policies/cctv-monitoring-policy/

Brantingham, P., & Brantingham, P. (2003). Anticipating the displacement of crime using the principles of environmental criminology. In D. C. M. Smith (Ed.), *Theory for Practice in Situational Crime Prevention. Crime Prevention Studies* (Vol. 16). Monsey, NY: Criminal Justice Press.

CALEA® | The Commission on Accreditation for Law Enforcement Agencies, Inc. (2013, July 12). *The Commission*. Retrieved from CALEA: The gold standard in public safety: http://www.calea.org/content/commission

Callington Community College. (2011, June). *CCTV policy and procedures*. Retrieved from College Policies: http://www.callington.cc/templates/add-files/uploadedfiles/CCTV.pdf

Canterbury Christ Church University. (2006). *Policy on the use of closed circuit television systems*. Retrieved October 11, 2012, from http://www.canterbury.ac.uk/data-protection/CCTV%20Policy.pdf

Caron, S. L. (1998). *Cross-cultural perspectives on human sexuality.* Toronto, ON: Allyn & Bacon.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Clarke, R. V., & Felson, M. (1993). Routine activity and rational choice. In R. Clarke, & M. Felson (Eds.), *Advances in Criminolgical Theory* (Vol. 5). New Brunswick, NJ: Transaction Books.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608. doi:10.2307/2094589

Community Safety Camera Ordinance. (2006). *S. F., Cal., Admin Code § 19.* Retrieved from http://www.amlegal.com/nxt/gateway.dll?f=templates&fn=default.htm&vid=amlegal:sanfrancisco_ca

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-947.

Creswell, J. W. (2007). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Czaja, R., & Blair, J. (2005). *Designing surveys: A guide to decisions and procedures* (2nd ed.). Thousand Oaks, CA: Pine Forge Press.

Davies, S. (1996). The case against: CCTV should not be introduced. *International Journal of Risk, Security and Crime Prevention, 4*(2), 149-167.

Department of Education. (2008, December 9). *Family Educational Rights and Privacy Act 1974.* Federal Register. 73 (2008): 74806 -74855. Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Draeger, J. (2011). What Peeping Tom did wrong. *Ethical Theory and Moral Practice, 14*(1), 41-49. doi:10.1007/s10677-010-9225-z

Dubbeld, L. (2003). Observing bodies. camera surveillance and the significance of the body. *Ethics and Information Technology, 5*(3), 151-162. Retrieved from http://ezproxy.cul.columbia.edu/login?url=http://search.proquest.com/docview/222250195?accountid=10226

Electronic Privacy Information Center. (2008). *Comments of the electronic privacy information center to the Department of Homeland Security of docket no.DHS-2007-0076.* Washington, DC: NGO. Retrieved March 1, 2012, from http://epic.org/privacy/surveillance/epic_cctv_030112.pdf

Elizabeth II. (1998). Data Protection Act 1998, Chapter 29. London: UK Parliament. Retrieved from http://www.legislation.gov.uk/ukpga/1998/29/section/29

Erickson, R. J., & Stenseth, A. (1996). Crimes of convienence. *Security Management, 40*(10), 60. Retrieved from http://proquest.com/docview/231175527?accountid=10226

Fitzpatrick, J. L., Sanders, J. R., & Worthen, B. R. (2011). *Program evaluation: Alternative approaches and practical guidelines.* Upper Saddle River, NJ: Pearson Education.

Franklin and Marshall College. (2008, June 14). *CCTV Policy*. Retrieved October 14, 2012, from Franklin and Marshall College: http://www.fandm.edu/publicsafety/cctv-policy

Gallagher, C. (2004). CCTV and human rights: The fish and the bicycle? An examination of Peck v. United Kingdom. *Surveillance and Society, 2*, 2-3.

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV.* Home Office Research Study 292. London: Home Office.

Glatthorn, A. A., & Joyner, R. L. (2005). *Writing the winning thesis or dissertation: A step-bystep guide.* Thousand Oaks, California: Corwin Press.

Goold, B. J. (2006). Open to all? Regulating open street CCTV and the case for "symmetrical surveillance". *Criminal Justice Ethics, 25*(1), 3-17.

Hempel, L., & Topfer, E. (2004). *CCTV in Europe: Final report.* Urban Eye. Working Paper No. 15. Retrieved from http://www.urbaneye.net/results/ue_wp15.pdf

Hier, S., & Greenberg, J. (2009). The politics of surveillance: Power, paradigms and the field of visibility. In S. Heir, & J. Greenberg, *Surveillance: Power probelms, and politics* (pp. 15-29). Vancouver, BC: UBC Press.

Hier, S., Walby, K., & Greenberg, J. (2006). Supplementing the panoptic paradigm: Surveillance, moral governance and cctv. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and Beyond.* (pp. 230-237). Portland, OR: Willan Publishing.

Honess, T., & Charman, E. (1992). Closed circuit television in public spaces. *Crime Prevention Unit Series Paper 35*. London: Home Office.

Horne, C. (1996). The case for: CCTV should be introduced. *International Journal of Risk, Security and Crime Prevention, 1*(4), 317--326.

Huck, S. W. (2012). *Reading statistics and research* (6th ed.). Boston, MA: Pearson Education.

IACLEA . (2007, September/October). CCTV Systems. *Campus Law Enforcement Journal, 39*(5), pp. 17-28. Retrieved May 15, 2012, from http://www.iaclea.org/members/clej/pdf/September_October_2007.pdf

Information and Privacy Commissioner of Ontario. (2007). *Guidelines for the use of video surveillance cameras in public places.* Toronto. Retrieved from http://www.ipc.on.ca/images/Resources/video-e.pdf

International Association of Campus Law Enforcement Administrators. (2012, November 18). *Organizational Directory*. Retrieved from IACLEA: http://www.iaclea.org/visitors/membership/category.cfm

Jermyn, D. (2004). This is about real people! Video technologies, actuality and affect in the television crime appeal. In S. Holmes, & D. Jermyn (Eds.), *Understanding Reality Television* (pp. 71-90). New York: Routledge.

Johns Hopkins University. (2005, April 18). *Closed circuit television (CCTV) monitoring and recording:Standard operating procedures.* Retrieved July 15, 2012, from Johns Hopkins University: http://webapps.jhu.edu/jhuniverse/administration/minutes_policies_reports/policies/monitor/

Kelley, L. D. (1999). *Measurement made accessible:A research approach using qualitative, quantitative, and quality improvement methods.* Thousand Oaks, CA: Sage Publications, Inc.

King, J., Mulligan, D., & Raphael, S. (2008). *Citris report: The San Francisco community safety camera program. An evaluation of the effectiveness of San Francisco's community safety cameras.* Center for Information Technology in the Interest of Society. University of California Berkeley. Retrieved from http://www.muniwireless.com/reports/sf-video-study-2008.pdf

La Vigne, N. G., Lowry, S. S., Markman, J. A., & Dwyer, A. M. (2011). *Evaluating the use of public surveillance cameras for crime control and prevention.* Community Oriented Policing Services, U.S. Department of Justice. Washington, D.C.: The Urban Institute. Retrieved from http://www.urban.org/url.cfm?ID=412402

Landis, J. R., & Koch, G. G. (1977, March). The measurement of observer agreement for catagorical data. *Biometrics, 33*(1), 159-174.

London South Bank University. (2010, August). *Policy & standards for CCTV operation at London South Bank University*. Retrieved October 11, 2012, from http://www.lsbu.ac.uk/foi/documents/cctvpolicy.pdf

Lupia, A., McCubbins, M. D., & Popkin, S. I. (2000). Elements of reason: Cognition, choice, and the bounds of rationality. In A. Lupia, M. D. McCubbins, & S. I. Popkin (Eds.), *Elements of reason: Cognition, shoice, and the bounds of rationality.* New York, NY: Cambridge University Press.

Lyon, D. (2002). *Surveillance and social sorting: Privacy, risk, and digital discrimination.* London, UK: Routledge.

Lyon, D. (2007). *Surveillance studies; An overview.* Cambridge, UK: Polity Press.

Marcum, C. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology, 2*, 346-367.

McCahill, M. (2002). *The surveillance web: The rise of visual surveillance in an English city.* Portland, OR: Willan.

Mensch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychology and Behavior, 12*(4), 387-393. doi:10.1089/cpb.2009.0068

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266-275. doi:10.1111/j.1467-9973.1985.tb00173.x

Mullins, J. (2006). Ring of steel II. *IEEE Spectrum, 43*(7), 12-13. doi:10.1109/MSPEC.2006.1652996.

National Institute of Standards and Technology. (2011-2012, 6 30). *2011-2012 Education Criteria.* Retrieved from Baldrige Performance Excellence Program: http://www.nist.gov/baldrige/publications/upload/2011_2012_Education_Criteria.pdf

Nevada Board of Regents. (2010). *Title 4 - Codification of Board Policy Statements.* Chapter 1, Section 21.

Nevada Revised Statutes. (1993). NRS 396.970. Retrieved from http://www.leg.state.nv.us/NRS/NRS-396.html#NRS396Sec970

Norris, C., & Armstrong, G. (1998). Introduction: Power and vision. In C. Norris, J. Moran, & G. Armstrong (Eds.), *Surveillance, Closed Circuit Television and Social Control* (pp. 3-18). Ashgate, England: Aldershot.

Norris, C., & Armstrong, G. (1999). *Maximum surveillance society: The rise of CCTV*. Oxford: Berg.

Patten, M. L. (2009). *Understanding research methods: An overview of the essentials* (7th ed.). Glendale, CA: Pyrczak .

Pettee, K. K., Ham, S. A., Macera, C. A., & Ainsworth, B. E. (2009, March). The reliability of a survey question on television viewing and associations with health risk factors in US adults. *Obesity, 17*(3), 487-493.

Rea, L. M., & Parker, R. A. (2005). *Designing and conducting survey research: A comprehensive guide* (3rd ed.). San Francisco, CA: Jossey-Bass.

Rye, B. J., & Meaney, G. J. (2007). Voyeurism: It is good as long as we do not get caught. *International Journal of Sexual Health, 19*(1), 47-56. Retrieved from http://dx/doi.org/10.1300/J514v19n01_06

Saetnan, A. R., Lomell, H. M., & Wiecek, C. (2004). Controlling CCTV in public spaces: Is privacy the (only) issue? Relections on Norwegian and Danish observations. *Surveillance & Society, 2*(2/3), 396-414. Retrieved from http://www.surveillance-and-society.org/cctv.htm

Schlosberg, M., & Ozer, N. (2007). *Under the watchful eye: Proliferation of video surveillance systems in California.* San Francisco, CA: American Civil Liberties Union. Retrieved July 11, 2011, from https://www.aclunc.org/docs/criminal_justice/police_practices/under_the_watchful_eye_the_proliferation_of_video_surveillance_systems_in_california.pdf

Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y., & Ekin, A. (2003). Blinkering surveillance: enabling video privacy through computer vision. *IEEE Security & Privacy, 3*(3), 50-57.

Sims, R. R. (1992, July). The challenge of ethical behavior in organizations. *Journal of Business Ethics, 11*(7), 505-513. Retrieved from http://ezproxy.cul.columbia.edu/login?url=http://search.proquest.com/docview/198178754?accountid=10226

Solove, D. J. (2011, May 15). *Why privacy matters even if you have 'nothing to hide'.* Retrieved March 12, 2012, from The Chronicle of Higher Education: http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

Solove, D. J. (2011a). *Nothing to hide: The false trade off between privacy and security.* New Haven, CT: Yale University Press.

Surette, R. (2005). The thinking eye: Pros and cons of second generation CCTV surveillance systems. *Policing, 28*(1), 152-173.

Syracuse University. (2012, June 12). *Closed-circuit television (CCTV) monitoring and recording policy.* Retrieved July 12, 2012, from Syracuse University: http://publicsafety.syr.edu/PublicSafety/ckfinder/userfiles/files/CCTV%20Policy.pdf

Taylor, E. (2010). Evaluating CCTV: Why the findings are inconsistant, inconclusive and ultimately irrelevant. *Crime Prevention and Community Safety, 12*(4), 209-232. Retrieved from www.palgrave-journals.com/cpsc/

Taylor, N. (2002). State surveillance and the right to privacy. *Surveillance & Society, 1*(1), 66-85.

U.S. Department of Homeland Security. (2007). *CCTV: Developing privacy best practices. Report on the DHS privacy office public workshop.* Washington, DC: U.S. Department of Homeland Security. (December 17, 2007). Retrieved from www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf

University of Minnesota. (2005). *Video surveillance (CCTV) and card access (CA) monitoring, recording, and data retrieval policy.* Retrieved June 30, 2012, from University of Minnesota: http://www1.umn.edu/dcs/assets/pdf/CCTV-CA_Policy%5B1%5D.pdf

University of Nevada. (2006, January). *7004: Policy on video and audio equipment usage.* Retrieved July 2, 2012, from University of Nevada, Reno: http://www.unr.edu/administrative-manual/7000-7999-miscellaneous/7004-policy-on-video-and-audio-equipment-usage

Villanova University. (2010). *Villanova University CCTV policy.* Retrieved May 2, 2012, from Department of Public Safety: http://www1.villanova.edu/content/villanova/publicsafety/policies/_jcr_content/pagecontent/download_0/file.res/CCTV%20University%20Policy.pdf

Vogt, W. P., & Johnson, R. B. (2011). *Dictionary of statistics & methodology: A nontechnical guide for th social sciences* (4th ed.). Thousand Oaks, CA: Sage.

Washington University in St. Louis. (2011, February). *Policy on closed circuit television (CCTV)*. Retrieved from Washington University in St. Louis: http://facilities.wustl.edu/PDF%20Documents/cctvpol.pdf

Welsh, B. C., & Farrington, D. P. (2002). Crime prevention effects of closed circuit television: A systematic review. *Home Office Research Study 252*. London, UK: Home Office Research, Development and Statistics Directorate.

Westin, A. (1967). *Privacy and freedom.* New York, NY: The New Press.

Winner, L. (1977). *Autonomous technology: Technic-out-of-control as a political thought.* Cambridge, MA: MIT Press.

Witmer, D. F., Colman, R. W., & Katzman, S. L. (1999). From paper-and-pencil to screen-and-keyboard. In S. Jones (Ed.), *Doing Internet research: Critical issues and methods for examining the net* (pp. 145-162). Thousand Oaks, CA: Sage.

Wollen, M., & Harris, E. A. (2011, November 13). *Occupy wall street protests shifting to college campuses.* Retrieved from New York Times Online: http://www.nytimes.com/2011/11/14/us/occupy-wall-street-protests-shifting-to-college-campuses.html?_r=1&pagewanted=print

Yesil, B. (2005). *Blind spots: The social and cultural dimensions of video surveillance.* (Ph.D., New York University). ProQuest Dissertations and Theses. Retrieved from ProQuest Dissertations & Theses (PQDT): http://search.proquest.com/docview/305467732?accountid=10226. (MSTAR_305467732)

Appendix A

Informed Consent to Participate in Research

Title of study: Analysis of Ethical Management Policies for the use of CCTV on College Campuses
Researcher: Jeannine M. Jennette
Dissertation Chair: Dr. Richard Maurer

Introduction:
You are requested to consider participating in a research study being conducted by Jeannine Jennette for a dissertation under the supervisor of Dr. Richard Maurer of the Department of Education at St. John Fisher College. You are asked to participate because you are a security professional at a college or university in the Mid-Atlantic United States. In this study, security professionals receive an Internet-based survey designed to obtain information on their schools policies related to the ethical use of Closed Circuit Television Camera (CCTV) technology on their campus. Participants will also to be asked to voluntarily participate in a follow-up telephone interview to expand on their survey answers. Participants may agree to only participate in the survey anonymously and not participate in a follow-up interview. It is hoped that security professionals will be willing to share their views relating to the survey and interview questions.

Please read the form carefully and ask any questions you may have before deciding whether to participate in the study.

Purpose of study:

This study will evaluate colleges' current practices for the ethical use of video technology, and develop through survey and interviews with experts in the field, recommended best practice guidelines for the ethical use of CCTV on college campuses. These guidelines will be available to practitioners in the field to assess or develop their own policies related to the ethical use of camera systems.

Study Procedures:

If you agree to participate in the study, you will be asked to complete an online survey that will take approximately 10-15 minutes to complete. This survey is designed to gather information on your college's policies related to the ethical use of CCTV on your campus. Upon completion of the survey, you will be asked if you are willing to participate in a brief 10-minute recorded telephone interview to expand on the answers you provided on the survey. This interview will be used to clarify and most accurately

reflect your college's current policies. The identifying data from these surveys, as well as follow-up interviews, will be destroyed once the data is transcribed and coded

Approval of study: This study has been reviewed and approved by the St. John Fisher College Institutional Review Board (IRB).

Risks and benefits: The researcher will protect confidentiality and anonymity of all research
data. There are no risks involved in participating in this research.

Confidentiality/privacy: All information gathered in this study will remain confidential. No data will be released identifying participants or their schools. All research will be conducted with the highest ethical standards for confidentiality. The names of the participants will be coded when the surveys are returned. The survey results and the interviews will be coded and the master coding list associating participants names with survey and interview results will be destroyed once the interviews are complete. Only the researcher and her dissertation chair will have access to the master coding list and interview data. Audio recordings of the follow-up interviews will be destroyed immediately after the data is coded. The researcher will retain the coded interview materials in a locked cabinet for a period of four years following the completion of the research and then it will be destroyed by shredding these records.

Your rights:

As a research participant, you have the right to:

1. Have the purpose of the study, and the expected risks and benefits fully explained to you before you choose to participate.
2. Withdraw from participation at any time without penalty.
3. Refuse to answer a particular question without penalty.
4. Be informed of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to you.
5. Be informed of the results of the study.

I have read the above, and by electronically participating in this survey, I agree and consent to participate in the above-named study.

If you have any further questions regarding this study, please contact the researcher, Jeannine Jennette at 212-305-1292 or jmj03926@sjfc.edu.

Appendix B

Survey Questions

1. Does your college use CCTV or other method of video surveillance on or off campus?

Yes
No

2. How many CCTV cameras on your campus does your college monitor and/or record?

100 or less
101-200
201-500
501-1000
1001-2000
2001 or more

3. Does your college have a written policy related to the use of CCTV cameras on campus?

Yes
No, but we are currently developing one
No, we do not have any CCTV cameras on campus
No, we have CCTV but no written policy
Other (please specify)

4. Who at your college is responsible for developing and/or maintaining your CCTV policy?

Security/Public Safety or Police Department
College CCTV or Camera Committee
General Counsel or Legal Department
Unknown
Other (please specify)

5. What year was your camera CCTV policy originally written?
Year

6. If you have CCTV cameras on your campus but do not have any written policies, how do you regulate the use of your CCTV cameras? Select all that apply.

Verbal training of employees
Written memos
Address each incident or question regarding CCTV as it occurs
Other (please specify)

7. In the last 5 years how often have you reviewed and/or updated your written CCTV policy?

O times
1-2 times
3-4 times
5 or more times

8. When was your written CCTV policy last updated?

Less than six (6) months ago
Between six (6) months and one (1) year ago.
More than one (1) year but less then two (2) years ago.
Two years but less than three (3) years ago
Three (3) years or more
Never updated policy

9. Does your written or unwritten CCTV policy include guidelines on how long video data is stored?

Yes
No

10. What is the average number of days your college stores CCTV video data, not required for a specific incident or investigation?

Less than 7 days
7 days but less than 14 days
14 days but less than 30 days
30 days but less than 120 days
Over 120 days (specify)

11. Does your CCTV policy, written or unwritten, restrict copying and disseminating video data?

No
Yes, only with permission person in charge of security/public safety or campus police
Yes, only with permission of General Counsel or college legal department

Yes, only upon receipt of subpoena
Yes, other (specify)

12. Does your CCTV policy, written or unwritten, restrict who may view live or recorded surveillance video?

No
Yes, restrict viewing of live and recorded video to Security or other authorized personnel only.
Yes, require permission to view recorded video unless emergency, live viewing restricted to security or other authorized personnel.
Yes, video is not actively monitored. Recorded video reviewed only after incident or request from authorized person.
Yes, other restrictions.

13. How is your CCTV policy communicated to students, faculty, and staff?

Policy is publicly available on the Internet or in written documents.
Policy is available on college website but access restricted to students, faculty, and staff.
Policy is on college website but restricted to authorized personnel
Policy is not publicly available restricted to security personnel only.
Not applicable. Do not have a policy.
Other please specify.

14. Do students, faculty, and staff (non-security personnel) have any input into the development, or implementation of the college's CCTV policy?

No.
Yes, Students, Faculty, and Staff
Yes, Faculty and Staff only
Yes, Faculty only
Other (please specify)

15. Do you conduct formal training of security personnel on your CCTV policy? If yes how often are they trained/retrained?

Never.
Once a month.
2-3 times a year.
Once a year.
Once a week.

Only when newly hired or promoted.
Only if policy changes.
Other (please specify)

16. Does your college require that security and/or public safety personnel, sign a document acknowledging that they understand your college's CCTV policy, and will comply with all policies related to the ethical use of CCTV cameras on campus?

Yes.
No.
Other (please specify)

17. Does your CCTV policy integrate your university's policy on Sexual Harassment?

Yes.
No.

18. Does your CCTV policy include guidelines regulating the monitoring of non-criminal activities on campus?

Yes.
No.

19. Does your CCTV policy include guidelines on monitoring persons based solely on race, ethnic origin, or sexual preference?

Yes.
No.

20. Does your CCTV policy include guidelines regulating the monitoring of non-criminal activities on campus (i.e. protests, student events)?

Yes.
No.

21. Does your CCTV policy include restrictions on installing cameras where a person

may have an expectation of privacy (i.e. locker rooms, bathrooms, or private offices)?

Yes.
No.

22. Who is responsible for investigating violations of your colleges CCTV policy?

Person in charge of college Public Safety/Security/Police Department
General Counsel or college Legal Department

Equal Opportunity Office EEO/OEEO or equivalent on your campus
Other college or outside agency (please specify)

23. Has your college experienced any misuse of CCTV cameras or recorded CCTV data that required an investigation or resulted in disciplinary action?

Yes.
No

24. Your college is best described as:

Four-Year Private College
Four-Year Public College
Two-Year Public or Private College
Other (please specify)

25. Where is your college located?

Metropolitan Inner-City campus
Urban campus- inside a smaller city
Urban-Adjacent –Easy access to a city
Rural Setting Campus – more distant from a city
Other (please specify)

26. What is the student population of your college or university?

Under 1500 students
1501-2500 students
2501-5000 students
5001-7500 students
7501-10,000 students
10,001-15000 students
15,001-20,000 students
20,001-30,000 students
25,001-30,000 students
30,001-35,000 students
35,000 students or over

27. What is the size of your security, public safety, or campus police department?

Under 25 employees
26-50 employees
51-100 employees
101-150 employees
151-200 employees
201-250 employees
251-300 employees
301-400 employees
401 employees or more

28. Is your department sworn or unsworn, or a mix of sworn and unsworn officers?

Sworn
Unsworn
Both Sworn and unsworn

29. Are the members of your public safety/security department armed, unarmed, or a mix of armed and unarmed officers?

Armed
Unarmed
Armed and Unarmed officers

30. Please add any comments regarding your college's CCTV policy or CCTV practices that were no covered in this survey that you feel are beneficial to this study?

31. Are you willing to participate in a brief telephone interview with this researcher to further clarify any responses given in this survey? All information will be kept strictly confidential.

31. Please enter your contact information Below. Thank you for participating in this survey.

Appendix C

Correlational Analyses of Survey Test Versus Retest

	Correlation	STDEV	Mean Test 1	Mean Test 2
SQ1	1.00	0.00	1.00	1.00
SQ2	0.92	1.82	3.67	3.56
SQ3	1.00	0.96	1.44	1.11
SQ4	1.00	0.43	0.78	0.78
SQ5	1.00	4.66	2007.25	2007.38
SQ6	1.00	0.96	2.13	1.83
SQ7	0.94	0.96	1.67	1.78
SQ8	0.89	1.95	4.22	3.89
SQ9	1.00	0.32	1.11	1.11
SQ10	0.89	0.70	3.67	3.56
SQ11	0.96	1.10	1.78	1.89
SQ12	0.96	1.06	1.89	2.00
SQ13	1.00	1.41	3.11	3.11
SQ14	1.00	0.49	1.33	1.33
SQ15	0.71	2.56	3.78	4.44
SQ16	0.66	0.38	1.22	1.11

SQ 17	1.00	0.51	1.56	1.50
SQ18	1.00	0.49	1.38	1.33
SQ19	1.00	0.24	1.00	1.11
SQ20	0.94	0.73	1.11	1.25
SQ21	0.75	0.38	1.89	1.78
SQ22	0.75	0.42	0.89	1.00
SQ23	0.76	0.46	1.78	1.67

Appendix D

Institutional Review Board Approval

ST. JOHN FISHER COLLEGE

January 17, 2013

File No: 3164-011713-01

Jeannine Jennette
5 North Court
Westbury, NY 11590

Dear Ms. Jennette:

Thank you for submitting your research proposal to the Institutional Review Board.

I am pleased to inform you that the Board has approved your Expedited Review project, "Analysis of Ethical Management Policies for the use of CCTV on College Campuses."

Following federal guidelines, research related records should be maintained in a secure area for three years following the completion of the project at which time they may be destroyed.

Should you have any questions about this process or your responsibilities, please contact me at 385-5262 or by e-mail to emerges@sjfc.edu, or if unable to reach me, please contact the IRB Administrator, Jamie Mosca, at 385-8318, e-mail jmosca@sjfc.edu.

Sincerely,

Eileen M Merges, PhD

Eileen M, Merges, Ph.D.
Chair, Institutional Review Board

EM:jlm

Copy: OAA IRB
IRB: Approve expedited.doc

3690 East Avenue • Rochester, New York • 14618 • www.sjfc.edu