RedFame

International Journal of Law and Public Administration
Vol. 2, No. 2; December 2019
ISSN 2576-2192 E-ISSN 2576-2184
Published by Redfame Publishing
URL: http://ijlpa.redfame.com

Closed Circuit Television Systems on University Campuses: Unexamined Implications for the Expectation of Privacy and Academic Freedom

Thomas W Lauer[1], Albert J. Meehan[2]

[1]Professor, Decision and Information Sciences, Oakland University, United States

[2]Professor, Sociology, Oakland University, United States

Correspondence: Thomas W Lauer, Professor, Decision and Information Sciences, Oakland University, United States

Received: June 4, 2019 Accepted: August 12, 2019 Online Published: August 13, 2019

doi:10.11114/ijlpa.v2i2.4311 URL: https://doi.org/10.11114/ijlpa.v2i2.4311

Abstract

Since 9/11 and particularly since the massacre at Virginia Tech University in 2007, many universities in the United States have begun installation of Closed Circuit Television (CCTV) systems on their campuses. What sorts of claims are being made about the use of these systems and what justifications are there for installing them? How might the pervasive use of monitoring technology affect traditional values associated with university life such as freedom of speech, freedom of assembly, privacy, and the freedom to explore? What policies are in place to ensure that whatever benefits associated with these systems justify both tangible and intangible costs?

Our analysis is partially derived from a study of university policies in the United States concerning the installation and operation of CCTV systems with the aim of gaining insight into these questions. In addition, we used a coding instrument for analyzing the corpus of policies in order to understand how the policies addressed such issues as: rationale or justification for CCTV usage, relevant personnel roles, public awareness, accountability measures, information security and data handling, routine operations of usage, and any relevant limiting measures. One aspect of our study is to interpret the corpus of policies through the lens of Nissenbaum's contextual integrity framework which is concerned with examining the effects of new technological practices (such as the installation of CCTV systems) on one's expectation of privacy.

Keywords: CCTV, privacy, surveillance, academic freedom, video surveillance policy

1. Introduction

Since 9/11 and particularly since the shootings at Virginia Tech University in 2007, many universities in the United States have installed Closed Circuit Television (CCTV) systems on their campuses. In many instances, introducing these systems is justified as a necessary security measure without much review. A number of questions arise concerning the implementation of CCTV on university campuses. For example, how might the pervasive use of monitoring technology affect traditional values associated with university life and academic freedom? Have claims made justifying the use of these systems been examined in light of possible adverse consequences of their use? Are there procedures that will ensure that whatever benefits associated with these systems justify both tangible and intangible costs? Who are the stakeholders and what are their interests in the use of CCTV? We analyzed a corpus of university policies in the United States concerning the installation and operation of CCTV systems with the aim of gaining insight into these questions.

The aim of this paper is to examine official university positions with regard to the use of CCTV systems on their campuses. To accomplish this, we analyzed official university video surveillance policies. More specifically, our objective is to understand how the installation of CCTV systems could affect the expectation of privacy on the part of members of the university community and their academic freedom. Our analysis is guided by Nissenbaum's (2010) contextual integrity (CI) framework which is concerned with examining the effects of new technological practices (such as the installation of CCTV systems) on one's expectation of privacy. The analysis proceeds along a series of steps that seek to understand how the introduction of CCTV in the university setting changes information transmissions; and ultimately how it supports or fails to support values, goals, and objectives integral to university culture.

2. Methodology

The authors of this study were part of an inter-disciplinary team consisting of five professors from the fields of information and decision sciences, sociology, law and public administration, and philosophy. The team assisted our research by participating in discussions that operationally defined a video surveillance policy and provided feedback on the coding schema for analyzing the policies devised by the authors. For our study, we used the Carnegie database of universities and colleges. The study was conducted between 2010 and 2013. Our sampling criteria yielded 1361 universities that were four year not-for-profit institutions. We excluded schools with a specialized focus, namely professional schools with a limited concentration of academic programs and service academies. We then employed a stratified random sampling procedure that resulted in a final sample of 370 schools. Within our final sample we identified 44 policies (12%); we found evidence of 172 institutions with CCTV systems but no apparent policy (46%); there were 146 schools with no evidence of CCTV (40%); and there were 8 institutions that confirmed no CCTV system (2%).

For our research purposes, we operationally defined a *video surveillance policy* as follows:

A written document that describes a formally approved set of procedures or internal rules of operations governing the placement and/or uses of video surveillance equipment and images on a college campus, which is either a stand-alone document or embedded within other institutional structures (e.g., student services, information security, telecommunications, campus security) intended to guide and/or constrain the actions of organizational members or its constituencies/stakeholders, which may or may not entail sanctions for non-compliance, either in whole or part. Based upon this definition, a policy: a) must be written (i.e. a published document); b) must be formally approved (i.e., it has been reviewed and approved by some part of the university governance structure); c) describes procedure(s)/rules governing the placement and/or uses of surveillance equipment and/or the images it produces; d) may be a stand-alone document or a document embedded within some other document found within other operational functions of the organization (e.g., student services, telecommunications, campus police); and e) is intended to guide and/or constrain the actions of organizational members directly responsible for the implementation and enforcement of the policy and other campus constituencies/stakeholders who are the subjects of the policy.

We developed a coding instrument for analyzing the content of the corpus of policies in order to understand how the policies addressed such issues as: rationale or justification for CCTV usage, relevant personnel roles, public awareness, accountability measures, information security and data handling, routine operations of usage, and any relevant limiting measures. Within each component, questions were created to capture the relevant characteristics and/or processes mentioned in the policy. For example, under rationale and justification, the coder would read the policy and identify if the policy mentioned any of the six rationales/justifications typically mentioned in CCTV policies (e.g., deter crime, promote safety/security, protect property, regulate/standardize use of CCTV on campus, assist law enforcement investigations, create situational awareness). As a consequence for this variable (and others), the results reported may not add up to 100%. In this case, a policy could mention more than one rationale. For other policy components, more than one characteristic or process could be present. Thus for most components, the totals will not be 100%. A doctoral student performed the initial coding of the policies which were then reviewed by the entire team for accuracy.

Contextual Integrity (CI)

Understanding the context

The hardware for CCTV systems typically includes the following elements: a) video cameras, b) cables that connect to an organizational network, c) a network video recorder, d) wireless access, and e) video monitors. (See figure 1.) These are socio-technical systems, so there are social systems that are also included that make up the entire context of CCTV usage. For example, on many university campuses, video monitors are housed in a control room for viewing that is staffed by campus police personnel. The IT department may have responsibility for video data handling including archiving, encryption where employed, data release, and data destruction. All of this is part of the CCTV context.

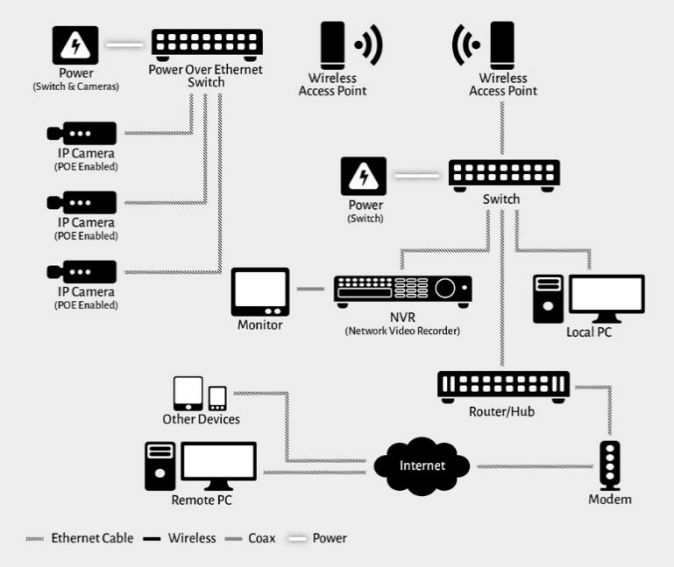

Figure 1. CCTV Hardware Configuration

Our expectation of privacy is dependent on the context in which information is shared. Privacy is "…a right to appropriate flow of personal information," that is appropriate to a specific context (Nissenbaum 2010, p. 127). Context includes roles (groups of related tasks and activities often associated with a particular function), activities (canonical activities or practices that characterize the context), norms (the range of acceptable actions, both what should and should not be done), and values (goals, purposes, or ends). There is a unity that characterizes the context so that roles and activities are in support of the context's values.

The CI framework is primarily concerned with changes to informational integrity that occur as a result of incorporating a socio-technical change, in this case, the introduction of CCTV systems in the context of university life. Informational norms are a subset of a context's norms that concern the flow of personal information from collection to use. "The framework of contextual integrity maintains that the indignation, protest, discomfit, and resistance to technology-based information systems and practices … invariably can be traced to breaches of context-relative informational norms." (Nissenbaum 2010, p. 140).

Beginning with a defined context that includes informational norms, the CI framework examines changes to actors, attributes, and information flows with the introduction of the new information system. The university context includes a range of roles, locations, and activities. With no attempt to be exhaustive, roles include student, instructor, researcher, administrator, and staff roles associated with various operational activities such as secretary, information technology (IT) specialist, police, and legal staff. Some locations and activities relevant to the university context are: classrooms for teaching, private offices, dormitories, common social spaces within buildings and outside, administrative spaces for the performance of a variety of operational functions, facilities for entertainment including athletic contests, musical performance venues, etc.

In addition, norms and values associated with university life are relevant to understanding the context. A number of authors have characterized the American university as one that supports various democratic values (Bird and Brandt 2002; Cole 2009; Wildavsky and O'Connor 2013). Cole identifies a set of core values some of which are: free and open communication of ideas, free inquiry and academic freedom, knowledge creation and the spirit of discovery, support for a community of scholarship, and intellectual progeny (an environment for fostering student intellectual development). In order to foster free and open communication, it is necessary that public places be amenable to the exchange of ideas without barriers to self-expression. Free inquiry and academic freedom distinguish universities from other types of institutions. Traditionally tenure for faculty supports academic freedom by removing fear of reprisal and interference by internal or external entities. Intellectual progeny serves as a protection for the developmental process most conducive to the intellectual maturation of students.

Changes Stemming from Introducing CCTV Systems

In order to understand the effects of introducing a new technology, the CI framework compares a baseline context (one absent the new technology) with a context where the technology has been introduced. An initial examination of our corpus of CCTV policies gives insight into where cameras are used, and how those decisions are made. As the aim of the CI framework is to understand threats to privacy, these results provide insight into areas of ambiguity and potential concern with where CCTV is used. It should be noted that there was considerable variation among universities, some

having well thought out policies while others were cursory consisting of a single page of vague and general statements.

The policies analyzed in our sample provided negative inferences about where there may be camera location, mostly by statements explicitly prohibiting camera usage in certain locations or circumstances and not others, and by describing where authority resides for locating cameras. Locations most often explicitly restricted from CCTV coverage included: residence hall rooms (66%), windows of private residential space/office on campus (51%), bathrooms (39%), locker rooms (33%), and private offices (29%). Beyond these specific references, 73% of policies restricted CCTV in "areas with a reasonable expectation of privacy." Notably missing from this list are classrooms. Prohibitions on CCTV usage included: a) 30% restricted CCTV from capturing images of "persons being intimate in public places", b) 43% prohibited camera use for the targeting of individuals protected by law (i.e. profiling), c) 17% prohibited the use of CCTV images/data in disciplinary proceedings against faculty, staff or students, and d) 14% of the policies prohibited or restricted audio monitoring.

Final decision on camera placement typically resides with the campus police chief or a single administrative authority, e.g. Legal Counsel, Director of Risk Management, or University President. Although 32% of our sample had a representative committee concerned with CCTV usage, committee membership was weighted toward administrative representation while also giving the committee limited decision making authority concerning camera placement and other critical matters. The vast majority (90%) of policies did not require that camera placement decisions be subject to public comment. With no participation from important stakeholders (e.g. students and faculty), there are few barriers to locating cameras in places that could raise objections. The CI framework requires that we identify how changes (the introduction of CCTV) affect actors, attributes of information, and information transmission principles. Each of these will be taken up in turn.

Actors

For the roles and the locations in the baseline context, the actors include a sender, a receiver, and a data subject. Absent a recording device, the sender and the data subject may be the same individual. For example, in an office visit, the student and professor may alternate between being the data subject and receiver. In an instructional setting, the student may be the data subject and the instructor the receiver or vice versa. During a casual encounter in the public spaces of the campus, the data subject and sender are the same person; the receiver is anyone who is encountered.

With the introduction of CCTV, new actors include the university police, the IT department, and any university administrators who have decision making authority over the CCTV system. As with the previous examples, the data subject is the same, but new senders are those who installed and operate the CCTV camera, possibly university police, IT personnel, and university administrators. New receivers are those who monitor live feeds, and those who review archived material, most obviously the same three sender groups, but depending on policies for releasing camera footage, there may be additional receivers.

Attributes

Attributes in the framework refers to the type or nature of information that is sent or received and can be thought of as a data field. What is important is the change in the attributes introduced by the CCTV system. Absent CCTV, for the data subject in a face to face encounter, the attributes are the set of sensory data about the subject available to the observer. Some of the data may be salient, but most won't, and most will not be remembered (Strahilevitz 2005). With the introduction of CCTV, all data undergoes some change – smell data is omitted, visual data is transformed from three dimensions to two, and audio may or may not be omitted. In addition, once the CCTV footage is recorded, video images may be isolated and editorially manipulated in various ways. The feeds from these systems can be combined with facial recognition software so that individuals can be isolated. Additional interpretive information may be added from other data sources to create a new aggregated record. In addition editorial manipulation enables sections of the feed to be slowed and analyzed frame by frame with enhancements or enlargements applied to sections of an image.

Transmission Principles

The third important consideration in judging whether information integrity has been compromised is to examine changes in transmission principles. Nissenbaum (2010, p. 145) defines transmission principles as constraints on the flows of information among parties in the relevant context. She considers transmission principle to be the most distinguishing feature of the contextual integrity framework. A key transmission principle in casual face to face encounters in public spaces where CCTV is not present is reciprocity or bi-directionality. How does CCTV alter transmission principles for typical public encounters? Among those that have changed are: reciprocity – completely missing with CCTV and onward transfer and secondary use – both unlikely in a face-to face setting unless there is something extraordinary about the encounter. In contrast, with CCTV, onward transfer is enabled since the record is now digitally stored and secondary usage may occur if administrators imagine new uses for the data.

The CI framework is a two-step process. The first step examines actors, attributes, and transmission principles. Since at this point, since there is a change in all three (actors, attributes, and information flows) there is a *prima facie* judgment that introducing CCTV constitutes a violation of contextual integrity. The next steps in the CI framework require further analysis to understand 1) the effects of introducing CCTV on political or moral factors, and 2) whether the use of CCTV supports or fails to support values, goals, or objectives of the original context, namely university education. It is possible that the further analysis will support the notion that 1) and/or 2) may mitigate changes to actors, attributes, and transmission principles.

Political and Moral Factors

Effects on political or moral factors, include threats to autonomy and freedom, changes to the power structure, and changes to our notion of justice and fairness. A number of findings from the policy descriptions are relevant here. The roles and responsibilities that different personnel have for administering the CCTV system have implications for understanding the university power structure. For example where there were representative committees with responsibilities regarding the CCTV system (1/3 of the policies) they did not have decision making authority regarding camera placement and usage. This rested with the Chief of Police or another administrator. Respect and protection of privacy was included as a rationale or justification in approximately 5% of the policies. Where privacy fits in can also be understood by implication where data handling procedures are specified. Information Services personnel were only mentioned in about 1/3 of the policies. This would suggest that for the other 2/3 little thought has gone into protecting the personal information contained in the CCTV feeds.

Data Handling

With the introduction of CCTV comes the introduction of a new role for the IT specialist as one responsible for: a) transfer of camera feeds across the network, b) storage of data, c) any processing of data that may be required by the university, d) data security, e) data archiving, f) data destruction, and g) release or transfer of data. In order to understand potential harms related to these IT activities, it is useful to consider Solove's (2008) privacy taxonomy. The taxonomy is essentially a process model that includes broad life-cycle categories of information: h) information collection, i) information processing, j) information dissemination, and k) invasions. Subcategories within the taxonomy include insecurity (resulting in data breaches) and several having to do with uses that go beyond the purposes for which the information was originally collected such as aggregation and secondary usage.

Analysis of our corpus of policies was informative as to universities' sensitivity to potential privacy infringements that could stem from privacy harms resulting from the use of CCTV. For example, just over half of the policies required minimal data security measures such as locked facilities or password access. Only 7.5% required the use of encryption for stored data. This leaves open the possibility of a security breach where the perpetrator is either an insider or someone external to the university. Most CCTV systems can be breached by trivial means, namely through the use of default settings that are often not changed prior to usage (Slashdot 2013). A security researcher going by the name of SomeLuser reported a vulnerability that enables remote access to CCTV recording systems and revealed 58,000 unique IP addresses that were running vulnerable systems (Leyden 2013; Moore 2013). Certainly the potential loss from such vulnerabilities emphasizes why for personally identifiable information captured by CCTV, encryption is advisable.

Access and release of CCTV images and data may also be the source of privacy harms. Close to 2/3 of all policies prohibit unauthorized access to CCTV images/video. Similarly, about 2/3 of all policies allow for release of images/data, typically with the approval of the police chief and/or some other administration official. When release of images/data is allowed in a policy, the representative committee has very limited approval authority in such matters: approximately 13% of these policies empower committees with this decision. This insures that in most cases, release of data will be primarily motivated by law enforcement or organizational issues. The majority of policies (56%) do not stipulate a time period for which data must be retained nor do they stipulate a time period after which data must be destroyed. Archival data offers many possibilities for secondary usage as it just waits for someone who has an interesting idea.

Power Dynamics

Not only are there new actors who are relevant to the context, but their relationships have changed by altering the power dynamics between the watcher and the watched. An essential feature of the power change is due to a knowledge asymmetry inherent to surveillance. The data subject has no way to know how information derived from camera footage may be used or by whom. There are many ways it may be used such as; to directly persuade, influence, or control, or to be retained for later use or no use. This is true whether or not the data subject is aware of the presence of video cameras. This power accretes over time, because the accumulation of digital records results in a temporal panopticon rather than one that is instantaneous and spatial (Mayer-Schönberger 2009). Contemplation of a temporal panopticon is particularly chilling. Rather than considering immediate consequences of being observed in the present, one must be wary of accounting for the entire permanent record. What of the trends in one's behavior and associations over time derived from cutting and pasting snippets of past video?

Two important ways of conceptualizing privacy are in terms of access and control. One that uses access defines privacy as "the condition of being protected from the unwanted access of others – either physical access, personal information, or attention" (Bok 1982, 10 – 11). For Westin (1967, 7), "Privacy is the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others." With our CCTV example, the direct recording of footage violates our sense of access. In addition, combining archival footage with other personal information violates both our sense of access and control. The potential for the onward transfer or release of CCTV footage and images violates our sense of control. Both concepts capture aspects of our sense of privacy, but as Nissenbaum (147 – 8) points out, by analyzing changes to information transmission principles from the standpoint of access and control, we are able to gain a more finely nuanced understanding of why we are made uncomfortable.

Support for Values, Goals, or Objectives of University Education and University Life

The final consideration is whether the new practice supports or fails to support values, goals, or objectives of the original context. If the introduction of CCTV, even if it results in the loss of privacy and is unfavorably evaluated in the previous steps, provides better support for the values, goals, and objectives of university education, that improved support could justify its installation and use. For example, if the threats to the security of university stakeholders are sufficiently grave, and if CCTV can mitigate these threats, then its use could be justified, even if the previous analysis shows CI violations. To understand this, we examine the corpus of policies to see if they include claims of improvement to either student learning, scholarly activity, or that they provide a secure environment. We further consider likely effects on traditional university values such as academic freedom, intellectual privacy, and the opportunity for exploration of unpopular ideas and alternative lifestyle choices.

Rationales for CCTV Use

Policies typically indicated multiple rationales and justifications and were coded for each given rationale or justification. The most frequently cited rationales were: a. preventative (i.e. promote security [90%], protect property [70%], deter crime [68%]), b. investigative (i.e. assist law enforcement investigations [68%]), and c. regulatory (i.e. standardize camera use on campus [56%]). Using Clery data, we conducted a separate analysis of campus crime data and CCTV and found there was no difference in crime rates for campuses with CCTV systems vs. campuses with no evidence of CCTV systems (Liedka, Meehan, and Lauer 2016). Thus the most frequently cited rationales for CCTV do not seem to be supported by the presence of high crime rates on campus or by their reduction through the use of CCTV systems. Other researchers and privacy advocates have noted the ineffectiveness of CCTV systems for crime prevention (bigbrotherwatch.org 2012; Bowe 2012; Franklin 2008; Sasse 2010; Welsh and Farrington 2009) and note further that they may induce a false sense of security. It is also interesting to note that a significant majority (76%) of policies do not require that public notice/signage be located at each camera site, thus further weakening any claim of deterrence.

University Values

As mentioned above, core university values are democratic and include the freedom to develop and express ideas. Freedom of thought and belief is the closest thing to an absolute right guaranteed by the U.S. Constitution. It is the precursor to other freedoms, for example those enumerated in the U.S. Bill of Rights such as the First Amendment that guarantees freedom of speech, freedom of expression, and freedom of association. Thus it could also be considered to be foundational with respect to the core values of universities such as academic freedom (Richards 2013). A number of writers have noted the 'chilling effect' that surveillance and lack of privacy can have on these First Amendment values (Reiman 2004, Solove 2008).

One way this manifests is by producing compliance and conformity. According to Gilliom (2001, 130 – 1), surveillance operates such that "under its power, we will almost inevitably succumb to the normalizing process which denies us any chance for truly autonomous existence." While chilling effects may affect a minority, those who may engage in non-conformist speech or behavior, harms extend beyond the individuals. The net result can reduce the number and variety of expressions and viewpoints within the community at large (Solove 2008). For example, the use of video analytics based on cognitive science that enable algorithmic determination of normal patterns of movement in public spaces and the identification of anomalies could pressure university stakeholders to conform so that they don't call attention to themselves through their physical actions. In contrast, "when there is protection from surveillance, new ideas can be entertained, even when they might be deeply subversive or threatening to conventional or orthodox views. If we value a pluralistic society or the cognitive processes that produce new ideas, then some measure of intellectual privacy, some respite from cognitive surveillance, is essential." Richards (2008)

The Threat of Scope Enlargement

Solove's taxonomy is a process model that provides insight into further harmful uses of personal data after it is collected. In this way, it complements Nissenbaum's CI framework. As noted above, most CCTV policies are generally lax or

silent with respect to procedures for protecting the privacy of data subjects whose images appear in the recorded CCTV footage. Much potential mischief can occur as a result of having data archives that can be repurposed. Vagueness regarding the justification and purpose for operating the systems in the first place provides room for new experimental uses. The lack of data destruction rules means that there may be available data for such uses. One harm noted in Solove's taxonomy is exclusion, the lack of notification to the subject that data are collected about her, and the concomitant bar to participate in data handling and use. There is no possibility for the subject to weigh in on any subsequent aggregation of the data with other data, secondary uses by third parties, or subsequent dissemination of the original data or products that combine the original data with other material.

There are particular factors that increase the plausibility of scope expansion. The first is the continued increase in the functional capability of video cameras and CCTV systems. Another factor is the growing militarization of campus police and influence of federal agencies such as the FBI, the NSA, and the Department of Homeland Security on campuses. A third is the propensity for operators of these systems to play around with them especially where there is little transparency or accountability.

Among the predicted trends for CCTV system functionality for 2014 are: Increased use of video analytics, power over Ethernet (PoE) products, and combining video with 'big data' (securityinfowatch.com 2013). Video analytics includes video content analysis that uses algorithms to predict potentially hazardous situations. Similar to facial recognition systems, the analysis and interpretation of complex and subtle human social spaces is error prone. The tendency to produce false positives depends on both the incidence of true positives and the sensitivity of the test (Majeske, Lauer 2012). As we have seen with such applications as TSA screening, the only individuals who were flagged were false positives and we can expect much the same from video analytics. Of course the use of video analytics requires combining video feeds with additional data, raising issues such as secondary use and aggregation, and the potential for disseminating a production vastly different from the original video image; one that includes personally identifiable information. PoE video cameras enable security personnel to plug a camera into any vacant Ethernet port connecting it to the campus network. This *ad hoc* addition of new camera feeds makes it easy to bypass any checks and balances that may exist regarding camera placement. By adding more points of vulnerability, it introduces a greater risk of security breaches. Finally, using CCTV images and feeds to enrich data from social network sites and other data stores is described under the rubric 'big data'. Using facial recognition software to produce an identified record and then linking that record to other data sources is no longer a discrete act of surveillance consonant with the purposes typically included in CCTV policies, but rather a part of a surveillance assemblage that consolidates power within the university administration at the expense of other stakeholders who become the data subjects.

The second potential threat of scope enlargement comes from the militarization of police and in particular campus police. Over 50% of campus police forces have intelligence sharing agreements with Department of Justice or Department of Homeland Security agencies (Gould-Wartofsky 2012). In addition, there are a number of collaborations between commercial organizations and universities that concern security. Twelve universities have DHS Centers of Excellence that are generously funded research institutes with participation by university researchers, the DHS, and various corporations. For example, Purdue University is home to VACCINE (Visual Analytics for Command Control and Interoperability Environments). They are a DHS center of excellence and list 27 university partners and 17 corporate partners. Their description includes the following: "The amount of information gathered during a crisis can be crushing if not managed correctly. DHS views this new Center's research and education in visualization as critical to the protection and security of America and her allies. In the event of a catastrophe such as a chemical spill, natural disaster, disease outbreak or a terrorist attack, information will be coming from many sources, such as camera images, data from sensors and simulations, and text documents from police and health-care agencies. VACCINE will focus on education, research, development, and deployment of interactive visual analytic environments for communicating and disseminating information and deriving insight from the massive homeland security data deluge." (VACCINE 2016)

Fusion centers, another DHS initiative are set up for the explicit purpose of enabling data sharing among different law enforcement entities. While the original justification for establishing fusion centers was to facilitate data sharing as it related to counter terrorism, a number of authors have noted a scope creep to include all crimes and all hazards (Monahan & Palmer 2009; Richards 2013; Slobogin 2009). Fusion centers have become a repository for all sorts of data (Cushing 2013) and in many instances have focused attention on demonstrations. The clear intent of this DHS program is to involve university police in the collection and sharing of data. While beyond the scope of this research report, there is a question as to whether FERPA (Federal Education Records Protection Act) provides a barrier to sharing video records keyed by personal identifiers. However, there is ambiguity since there is an exception for law enforcement records. Is the video record an educational record or a law enforcement record?

Given this platform for scope expansion can one trust the administrators of these systems to protect individual privacy? Realistic expectations are that there will be further harms resulting from aggregation (to produce or add to a dossier on

individuals), secondary use, breach of confidentiality (if one believes that a university has a fiduciary responsibility to students, faculty, and staff there should be confidentiality), additional harms from dissemination (disclosure, exposure, distortion and even blackmail), and invasions such as intrusion and decisional interference. (All of these harms are from Solove's taxonomy). Specific instances of these abuses by those charged with operating CCTV systems are documented in Nestel (2006).

3. Conclusion

The introduction of CCTV systems on university campuses should raise a number of red flags. The CI analysis reveals alteration of the context of information use; change to actors, attributes, and information transmission norms. It does so in a way to tilt the balance of power away from students and faculty and toward university administration, with special emphasis on legal counsel and the police. In addition, its use inhibits the expression of important values of the university, e.g. freedom of inquiry, freedom of speech and association, and enabling students to try out new ideas and life choices. Particularly troubling is the potential for scope expansion well beyond any original justification for these systems. One could argue that the DHS with the complicity of university administrations has used tragic events like 9/11 and the Virginia Tech murders as a cover for action; that their motivation has been the consolidation of power and their various grants and programs include an incursion on the institution of higher education.

This should give us pause. There is a body of experience that teaches that universities are unlikely to remain healthy and free if there is undue meddling from external entities (Rorty 1996). The widespread introduction of CCTV to university campuses without adequate checks and balances may be only a symptom, but it is not a harbinger of a vibrant intellectual environment for American universities.

References

Bigbrotherwatch.org (2012). The Price of Privacy: Councils Spend Half a Billion Pounds on CCTV in Four Years. https://bigbrotherwatch.org.uk/2012/02/price-privacy-councils-spend-521m/ Accessed at 5/31/2019

Bird, R. K., & Brandt, E. B. (2002). Academic freedom and 9/11: How the war on terrorism threatens free speech on campus. *Communication Law & Policy*, *7*(4), 431-459. https://doi.org/10.1207/S15326926CLP0704_05

Bok, S. (1982). *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon Books.

Bowe, R. (2012). Freedom not Fear: CCTV Cameras in Focus. Accessed at https://www.eff.org/deeplinks/2012/09/freedom-not-fear-cctv-surveillance-cameras-focus 5/31/2019

Cole, J. (2009). *Great American University*: *Its Rise to Preeminence, Its Indispensable National Role, Why It Must Be Protected*. New York: Public Affairs.

Cushing, T. (2013). 'See Something, Say Something' Campaign Creates Massive Database of Useless Info From Citizens Spying On Each Other, techdirt.com, accessed 3/23/14

Franklin, S. B. (2008). Watching the Watchers: Establishing Limits on Public Video Surveillance, *The Champion*, www.nacdl.org, accessed 3/20/2014

Gilliom, J. (2001). *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.

Gould-Wartofsky, M. (2012). Repress U, Class of 2012: Seven Steps to a Homeland Security Campus, http://www.tomdispatch.com/post/175519/tomgram%3A_michael_gould-wartofsky_class_of_2012_meet_the_class_of_1984/ accessed 5/31/2019

Leyden, J. (2013). Hackers squeeze through DVR hole, break into CCTV cameras. *The Register*. http://www.theregister.co.uk/2013/01/29/cctv_vuln/. Accessed 5/31/2019

Liedka, R., Meehan, A. J., & Lauer, T. W. (2016). *CCTV and Campus Crime: Challenging a Technological "Fix"*. Criminal Justice Policy Review, First published September 1, 2016. https://doi.org/10.1177/0887403416664947

Majeske, K. D., & Lauer, T. W. (2012). Optimizing airline passenger prescreening systems with Bayesian decision models, *Computers and Operations Research, 39*, 1827-1836. https://doi.org/10.1016/j.cor.2011.04.008

Mayer-Schonberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press, 2009.

Monahan, T., & Palmer, N. A. (2009). The Emerging Politics of DHS Fusion Centers, *Security Dialogue*, *40*(6), 617-636. https://doi.org/10.1177/0967010609350314

Moore, H. D. (2013). Ray Sharp CCTV DVR Password Retrieval Remote Root. https://community.rapid7.com/community/metasploit/blog/2013/01/28/ray-sharp-cctv-dvr-password-retrieval-remote-root, Accessed 5/31/2019

Nestel, T. J. III (2006). Using Surveillance Cameras to Monitor Public Domains: Can Abuse Be Prevented? (March 2006) (unpublished M.A. dissertation, Naval Postgraduate School)

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford University Press.

Reiman, J. H. (2004). Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future. In *Privacies: Philosophical Evaluations*, edited by Beate Rossler, Stanford, CA: Stanford University Press.

Richards, N. M. (2008). Intellectual Privacy, *Texas Law Review*, *87*, 387-445.

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*, vol. 126, 1934 – 1965.

Rorty, R. (1996). "Does Academic Freedom Have Philosophical Presuppositions?" in *The Future of Academic Freedom*, Louis Menand, Ed. Chicago: University of Chicago Press.

Sasse, M. A. (2010). Privacy and Security: Not Seeing the Crime for the Cameras, *Communications of the ACM*, *53*(2), 22-25. https://doi.org/10.1145/1646353.1646363

Securityinfowatch.com (2013). IHS: Top 10 Video Surveillance Trends 2014. Accessed 3/23/2014

Slashdot (2013). Most CCTV systems come with trivial exploits. http://yro-beta.slashdot.org/story/12/05/17/1321257/most-cctv-systems-come-with-trivial-exploits Accessed 5/31/2019

Slobogin, C. (2009). Surveillance and the Constitution, *The Wayne Law Review*, *55*, 1105.

Solove, D. J. (2008). *Understanding Privacy.* Cambridge, Massachusetts: Harvard University Press.

Strahilevitz, L. J. (2005). A social networks theory of privacy, *University of Chicago Law Review, 72*, 919-974.

VACCINE (2016). https://www.purdue.edu/discoverypark/vaccine/about/ accessed 5/31/2019

Welsh, B., & Farrington, D. (2009). Public area CCTV and crime prevention: An updated systematic review and meta analysis. *Criminal Justice Quarterly*, *26*(4). https://doi.org/10.1080/07418820802506206

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Wildavsky, R., & O'Connor, E. (2013). *Free to Teach, Free to Learn: Understanding and Maintaining Academic Freedom in Higher Education*. New York: ACTA.