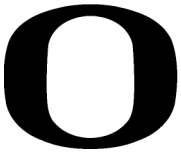

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

When Private Entities Use Video Surveillance in Public Space: Personal Benefits vs. Privacy Infringements

CAPSTONE REPORT

Michael Lasher
Chief Operations Officer
Umatilla-Morrow ESD

University of Oregon
Applied Information Management Program

March 2006

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger

Academic Director, AIM Program

Abstract

for

When Private Entities Use Video Surveillance in Public Space: Personal Benefits vs. Privacy Infringements

This study examines the most common video surveillance applications currently used by private entities in public spaces. Through literature review and content analysis (Leedy and Ormrod, 2005) the paper examines: monitoring, facial recognition, inclusion of video in larger databases, tracking, and security applications (Davis, 2005). Purported benefits of these technologies are aligned with potential privacy intrusions. A personal decision tool provides readers with a process to evaluate their own feelings about video surveillance and privacy.

Table of Contents

List of Figures

Chapter I – Purpose of Study

Brief Purpose

While the technology for video surveillance has been around since the 1950s (Beranek, 2005), a revolution in video surveillance systems is occurring with the advent of low-cost, high-resolution cameras, wireless network connectivity, and the transition from analog to digital technology, (Davis, 2005). With this transformation, a host of new software functionality has also appeared (Beranek, 2005) including motion detection, object separation, and facial recognition (Davis, 2005; CQ Researcher, 2001).

Although this study pertains to private video surveillance, as a backdrop it is important to note that the Fourth Amendment of the United States constitution prevents the U. S. government from conducting unreasonable searches (U.S. Constitution); however, government video surveillance is permitted in public spaces when no reasonable expectation of privacy exists (Blitz, 2004). The U.S. Supreme Court has repeatedly affirmed that the expectation of privacy on public streets is unreasonable and therefore, in such cases, no search is being conducted (Slobogin, 2002). Cities such as Chicago, New York, and Washington DC are installing thousands of video cameras to monitor public spaces (Douglas, 2005; Kontzer, 2005). Moreover, the U. S. constitution does not prevent private persons from spying on one another in public (CQ Researcher, 2001).

Coupled with other modalities available in the modern surveillance society including the collection of information from credit reports, credit cards, and even customer loyalty cards (Lyon, 2003), government and private parties now have an "opportunity

to amass an unprecedented amount of information about each of us" (Buderi, 2003). In 2005 alone, over 15 million video surveillance cameras were sold (Davis, 2005). Norman Siegel, of the New York Civil Liberties Union had observed five years earlier, "The explosion of video surveillance cameras around America has taken place without any public discussion about the pros and cons" (Marks, 2000).

The purpose of this study is to document a selection of applications of private video surveillance conducted in public spaces and examine the effect of this type of surveillance on personal privacy as defined by Fourth Amendment privacy rights (U.S. Constitution) and the Privacy Right of Intrusion (Restatement Second of Torts). Staples (1997) defines surveillance, in general, as the act of monitoring the activities of people (Staples, 1997). Lyon (2001) describes surveillance as the "collection and processing" of information about people "for the purposes of influencing or managing" them (Lyon, 2001). For this study, video surveillance refers to the use of digital or analog video cameras coupled with software applications to practice surveillance as described by Lyon. Examples of the use of the term "application" in this paper include facial recognition, object separation, security, etc. (Davis, 2005).

The overall method of study is literature review (Leedy & Ormrod, 2005). Literature is collected that examines the private use of video surveillance is published between 1996 and 2006. Literature is selected that addresses the question: "In what ways is personal privacy affected by the use of video surveillance systems when employed by private companies, and organizations to monitor, collect and process information about individuals in a public place?" A content analysis strategy is selected for data analysis (Leedy & Ormrod, 2005). The goal of the content analysis is to examine:

(1) selected examples of the application of digital video surveillance systems in public spaces by private entities, and (2) the personal privacy rights trade-offs with which the American public is potentially faced, as a result of the expanded use of video surveillance systems.

Results of the content analysis are presented in two tables. The first table (see Appendix A: Video Surveillance Technology Applications) documents the most commonly used private video surveillance applications with brief descriptions of each. The second table (see Appendix B: Private Use of Video Surveillance Technology, Purported Personal Benefits and Potential Personal Privacy Tradeoffs) compares the purported personal benefits of each video surveillance application with a description of potential impacts to one's individual privacy.

The results of this study are then framed into a decision tool, designed to enable an individual to conduct a self-directed assessment of their sense of privacy infringement from video surveillance (see Appendix C: Do I Think That I Am Losing My Privacy?). The tool provides a set of personal benefits for selected video surveillance technologies, which can be weighed against potential loss of personal privacy. The researcher intends that this outcome will provide American citizens with a useful tool with which to increase awareness of the potentially positive and negative aspects of the use of private video surveillance in public spaces, when examined within the context of social and personal criteria.

Full Purpose

According to the market research firm Frost and Sullivan, sales of digital surveillance cameras were expected to grow 10 fold between 2000 and 2005 (Farmer & Mann,

2003). This growth is fueled by a number of factors, including advances in surveillance technology, lower cost equipment, and new applications for marrying video information with other privately collected data (Buderi, 2003; Farmer & Mann, 2003; Davis, 2005). Digital video surveillance technologies are declining in price; at the same time they are growing in functionality and sophistication (Calvert & Brown 2000; Davis, 2005). While analog based closed-circuit television (CCTV) was once the main modality for video surveillance the technology and the marketplace are increasingly moving toward digital technologies (Davis, 2005; Farmer & Mann, 2003). Low cost, thumbnail sized cameras with high resolution lenses allow just about anyone to spy on their neighbor (Calvert & Brown, 2000).

The concept of "video surveillance systems" refers to more than the closed-circuit television (CCTV) systems that many people imagine (Cucchiara, 2005). The digitization of images received from video cameras can be stored, searched, cataloged, manipulated, and enhanced to be useable in many more ways than analog storage on a video-tape (Davis, 2005; Slobogin, 2002). These hardware and software technologies come together to create a surveillance "system" that is potentially far more intrusive than CCTV has been in the past (Davis, 2005; Dority, 2001; Buderi, 2003). Advances in video surveillance cameras and associated computer systems create the ability for a video surveillance system to engage in motion detection, object separation and tracking, facial recognition, gait recognition, and most importantly the ability to converge data from video surveillance systems into larger databases (Farmer & Mann (2003); Dority 2001).

Video surveillance has been used for many years by shop owners, banks, hospitals, shopping malls, and even schools, to discourage theft or violence (Iraola, 2003). For

example, facial recognition applications in conjunction with video surveillance are currently being used by casinos to identify card counters and other cheats as they enter the premises (CQ Researcher, 2001; Lyon 2003c). With the catastrophic events of the terrorist attacks on the World Trade Center in New York City and the Pentagon (Headquarters of the U.S. Department of Defense) on September 11, 2001, a majority of Americans have come to acknowledge video surveillance as a means of recording, and perhaps even preventing terrorism and/or crime (Nelson, 2004). Jaeger, Bertot and McClure (2003) found that, The Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act, altered many laws related to government surveillance. However, Americans are also concerned with the use of surveillance technology beyond the purpose of stopping or catching terrorists (Nelson, 2004). It is the assumption of this researcher that such concern is warranted. With the latest technological developments listed above, Farmer and Mann (2003) believe that "Ultimately, surveillance will become so ubiquitous, networked, and searchable that unmonitored public space will effectively cease to exist" (Farmer & Mann 2003, p.36).

The case evidence for concern is beginning to stack up. For example, in a widely publicized case, at the 2001 National Football League, Super Bowl in Tampa, Florida, every one of the 100,000 people attending the event was captured on video and their images compared with pictures of wanted criminals and terrorists (CQ Researcher, 2001; Iraola, 2003; Aronov, 2004). In another type of example of misuse of video surveillance, video surveillance cameras are used to "peep" up women's dresses. Unfortunately such acts are infrequently prosecuted as invasions of privacy.

Local, state, and federal laws generally do not define privacy – even of one's underwear – to be protected in any public place (Calvert & Brown).

As one way to raise public awareness about the potential problems inherent in private video surveillance in public spaces, this study is designed to examine selected digital video surveillances systems used within the public space. A literature review (Leedy & Ormrod, 2005) is conducted to identify and gather appropriate source material addressing use of video surveillance systems and aspects of individual privacy that may be abridged in the private use of video surveillance systems in public spaces. With the exception of works by Warren and Brandeis (1890) which provide a background of privacy in common law, content was selected from a period corresponding to the significant increase in digital video surveillance technology. The time period between 1996 through 2006 also corresponds to a five year window on either side of the terrorist attacks of September 11, 2001 – which has been noted as a watershed event for video surveillance systems (Davis 2005; Nelson 2004).

Once collected and reviewed, the chosen literature undergoes a content analysis (Leedy & Ormrod, 2005). Content analysis enables the researcher to systematically review source materials for the purpose of uncovering underlying themes or patterns (Leedy & Ormrod, 2005). The text-based nature of content analysis is useful in this study, where the goal is to evaluate the tension between applications of video surveillance systems and effects on personal privacy, as these are presented in written publications.

The content analysis results in two tables. The first table (see: Appendix A: Video Surveillance Technology Applications) presents the most frequently mentioned types

of video surveillance systems and provides descriptions of how they are often used to monitor individuals within the realm of public space. The researcher intends that this information will increase interest and understanding of both the types and applications of this technology currently in use. The second table (see: Appendix B: Private Use of Video Surveillance Technology, Purported Personal Benefits and Potential Personal Privacy Tradeoffs) is designed to describe the potential effects these video surveillance applications have on individual privacy.

The final outcome of the study is designed as a decision support tool (see Appendix C: Do I Think That I Am Losing My Privacy?) derived from the two content analysis results tables. This final table is designed to provide the opportunity to examine the potential for infringement on individual privacy that might occur as a result of the use of the selected video surveillance systems in pubic spaces. Emphasis is on those software technologies that are in wide-spread use. The intent of this tool is not to judge the efficacy of either the technology or the applications of the technology. Nor is it concerned with proclaiming privacy to be infringed. Rather, this tool is presented as a guide for an assessment process, useable by any citizen, which may facilitate personal judgments regarding the individual benefits of the selected video surveillance systems when balanced against the potential risk in loss of individual privacy.

Limitations to the Research

• Literature is explored that can help answer the question: "What are the effects on individual privacy when private individuals, companies, and organizations use video surveillance to monitor, collect, and process information within public spaces"?

• This study does not seek to explore or explain the reasons private entities install and use video surveillance systems in public spaces.

• With a couple of noted exceptions, literature for this study is limited to the five years preceding, and the five years following the terrorist attacks of September 11, 2001.

• Although much has been written about the encroachment of technology and particularly the effects of data collection on consumer privacy, the Patriot Act and its provision for extraordinary surveillance, search, seizure, and imprisonment have elevated the debate among scholars (Nelson, 2004). The last ten years also parallels the rise of digital video surveillance technology over the older CCTV technology (Farmer & Mann, 2003).

• Literature for this study is collected from a variety of sources including academic journals, law reviews, government documents, newspapers, periodicals and business and industry magazines. Emphasis is placed on evaluation of the credibility of the source, publication and/or the author. The researcher eschews writings that are clearly designed to promote or highlight a particular technology product, process, or application. Similarly, information from journals of engineering and computer science, as well as, technical journals that require a high degree of familiarity with electronics, optics, physics, etc. are avoided.

• To date, the United States courts have generally ruled that it unreasonable for individuals to expect any privacy in public spaces; thereby providing government and private video surveillance in any public spaces (Blitz, 2004; Calvert & Brown, 2000; Intille, 1999; Iraola; 2003). On the other hand, while the United States Constitution

does not contain explicit language relating to privacy, various supreme courts have interpreted privacy rights to be contained within the First, Fourth, Fifth, Fourteenth, and Sixteenth Amendments (Intille, 1999; Nelson, 2004; Iraola, 2003). Because of the difficulty in defining privacy from multiple, non-explicit amendments (Intille, 1999), for the purpose of this study the definition of privacy is limited to Fourth Amendment protections relating to unreasonable search when referring to government video surveillance activities. In addition, for situations involving the use of private video surveillance technologies, privacy will be defined by the Privacy Tort of Intrusion (Restatement Second of Torts, 1977).

• A content analysis (Leedy & Ormrod, 2005) strategy is chosen to analyze collected literature. As the data analysis seeks to identify selected examples of digital video surveillance systems by private entities, the content analysis strategy provides a way to reach this goal through the examination of text-based materials.

• Lyon's (2003) view is that "surveillance is always Janus faced", meaning to have two contrasting aspects. This view is supported in this paper. The author agrees with the position, that there are as many positive uses for surveillance as there are negative consequences (Lyon, 2003). In addition, the author supports the notion by Nelson (2004), who would have us informed by the broader policy debate and abandon "time-worn dichotomies…by entrenched political decisions" (Nelson 2004).

Definitions

The term **Application** in this study refers to a computer software or hardware/software combination that permits the processing of information obtained

through a video surveillance camera. Facial recognition, gait recognition, tracking, and object separation are all examples of applications.

Biometrics is the ability to recognize individual persons by using a computer(s) to compare physical trait(s) or characteristic(s) of a person to a database of people who share the same traits and characteristics (Iraola, 2003).

Leedy and Ormrod (2005) describe **content analysis** as "a detailed and systematic examination of the contents of a particular body of material for the purpose of identify patterns, themes, or biases" (Leedy and Ormrod, 2005, 142).

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Constitution).

A **Literature Review** is defined as a research process wherein existing literature about a topic is reviewed in an effort to gain new understanding about the topic (Leedy and Ormrod, 2005).

Personal Benefits of Video Surveillance includes such items as surveillance cameras that monitor a child's caregiver (nanny-cam), or traffic and weather conditions (Farmer & Mann, 2003). Personal benefits to video surveillance may also include a sense of safety and security one could derive from being in a monitored space. (Farmer & Mann, 2003)

Nelson (2004) describes **privacy** as "a factual condition of life…demarcated by the perception that it has been altered or lost by the actions of others. The perception that we face a loss of privacy in light of the information age is a factual condition of privacy loss and is attributable to our normative expectations of privacy" (Nelson, 2004 p. 264).

Privacy Rights, broadly defined, are the set of common law (Privacy Tort of Intrusion, 1977) and Fourth Amendment (U.S. Constitution) legal rights.

The **Privacy Tort of Intrusion** states: one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person (Restatement (Second) of Torts, 1977).

Public Space is, for the purposes of this study, defined to be any space that is free to enter without cost of admission.

Lyon (2003b) describes **surveillance** as the "routine ways in which focused attention is paid to personal details by organizations that want to influence, manage, or control certain persons or population groups (Lyon, 2003b, 5)."

Surveillance Society as described by Lyon (2003) is a function of modern life and computer power. The ability to collect and combine personal data from a variety of sources for the purpose of directing or influencing the actions of people is the hallmark of a surveillance society (Lyon 2003).

Surveillance Technologies are equipment (e.g. cameras and networks) and software applications (e.g. facial recognition) which are used to conduct visual surveillance (Davis, 2005).

Video surveillance is the use of digital or analog video cameras to conduct surveillance.

A **video surveillance system** is the combination of hardware (cameras, networks and servers) with software applications (facial recognition, object separation, gait recognition) used together to conduction video surveillance (Davis, 2005).

Problem Area

According to Nelson (2004), "Surveillance is becoming commonplace, frequent, and innocuous" (Nelson, 2004). Lyon (2001) finds all modern industrialized societies to be surveillance societies and he describes the surveillance society as one where the act of surveillance has become "societally pervasive" (Lyon 2003). For example, it is quite common to use credit and debit cards for purchases and drivers licenses and passports for identification. We readily give our personal information to retailers when we fill out a warranty card or ask for additional product information. Each of these acts leaves a trail of information about us that private companies collect and use to monitor, influence and perhaps control us. Typically we participate in this exchange of private information for convenience. Lyon (2003) makes the observation, "How inefficient and inconvenient it would be if we were obliged to pay cash for everything or to be interviewed by officials each time we crossed a border!" (Lyon 2003 p. 164).

Video surveillance is a relatively recent type of surveillance in our modern society (Lyon 2003). The growth of video surveillance installations along with the expansion in capability pose some of the greatest concern to privacy (Blitz, 2004). Private sector installations of video surveillance for commercial purposes exceed the capabilities of most national governments (Lyon, 2003). In 1998, the New York Civil Liberties Union conducted a survey of downtown Manhattan, in New York City, and found nearly 2400 cameras monitoring public spaces (Calvert & Brown, 2000; Slobogin, 2002). Today, video surveillance equipment that is tied together with computer networks has the ability to not only identify a person, but also to potentially follow their physical movements in nearly any direction (Blitz, 2004). Government and private entities have the opportunity to not only to take a picture of a person, but to also conduct an ongoing broadcast of their activities (Blitz, 2004). The implications are that tracking a persons activities in is a far greater intrusion of privacy that simply "seeing" that someone is at a particular place at a particular time (Blitz, 2004).

Lyon (2003) argues that surveillance, in general, increasingly depends not only on advances in technology, but also is driven by consumerism (Lyon, 2003). The fact that many private entities gather information (surveillance) about customers and then sell it "within the vast repositories of database marketing" raises further concerns about privacy (Lyon, 2003). For example, the Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) are known to have accounts with consumer information database companies which they use to gather information on those they are investigating (CQ Researcher, 2001). By purchasing personal data in the marketplace, government agencies, step around privacy laws – "and the amount of

detail about individuals available to anyone who can afford it is staggering, if your willing to pay for it" (CQ Researcher, 2001 p. 519). One wonders, if the inclusion of data captured through video surveillance has the potential to degrade personal privacy even more dramatically?

Privacy advocates have been slow to realize the interconnected nature of surveillance in modern society (Lyon, 2003). While video surveillance technologies have been around for many years, new applications which allow still or moving images to be included in a database of other personal attributes have enabled an ability to monitor people to a much greater degree (Farmer & Mann, 2003). If private citizens are going to be watched in public spaces, it is important for the citizens to be included in the dialogue about how they will be monitored (Marks, 2000).

When a person enters a public space, it is common (and prudent) to assume that they may be observed by another person in the same space. Although the courts have regularly ruled that there can be no expectation of privacy in public spaces, Lessig (1990) points out that perhaps American's don't understand how surveillance technologies might effect their personal privacy in a public space:

"If you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if an employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were -- if any and all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible" (Lessig, 1999,p504).

The assumption underlying this study is that if video surveillance is a problem for privacy, then the problem is going to get worse with the proliferation of more video surveillance cameras. In addition, the patchwork of local, state, and federal laws combined with cultural and ethical ideas of privacy create an additional problem in defining when privacy has been violated (Nelson 2004). Without a discussion about the broader nature of privacy, Americans may lose more than they are prepared to (Nelson 2004).

Chapter II – Review of References

This chapter provides an annotated bibliography of key references used throughout this study. The chapter is divided into three sections. The first section: Video Surveillance Technologies and Applications reviews key references that describe video surveillance systems and their use. The second section: Video Surveillance and Privacy Rights, reviews key references that examine the real and potential affects on American privacy rights in relation to video surveillance systems. The final section: Relating to Method, reviews primary sources this paper uses in developing Chapter III: Method of Study.

Section 1. Video Surveillance Technologies and Applications

Blitz, M. J. (2004, May). Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity. *Texas Law Review,* 82 (6), 1349- 1481.

The author is an associate in the firm of Wilmer, Cutler and Pickering, a J. D. University of Chicago and a Ph.D. Political Science University of Chicago.

This article is especially useful to this study, providing a broad discussion of Fourth Amendment issues surrounding video surveillance and a good description of the applications of video surveillance systems, including tracking, magnification, biometric and facial recognition. However, the article is focused on the government's use of video surveillance and does not offer lengthy commentary on any use of video surveillance conducted by private individuals.

The article includes a description of the Katz v. United States Supreme Court ruling of 1967 and how this ruling has shaped the debate about rights to privacy within

public space. Blitz describes why the "expectation of privacy" is essential to effectively arguing Fourth Amendment protections against unlawful search. The author explains that the courts have been increasingly interested in defining all activities in public spaces as being free of unreasonable search because there cannot be a reasonable expectation of privacy within a public space.

The author provides examples of the video surveillance applications of tracking, magnification, and biometrics and facial recognition. Each application is then reviewed with illustrations of how the use of the application might trigger Fourth Amendment protections. This article is extremely useful in describing the Problem Area of this paper.

Cucchiara, R. (2005). Multimedia Surveillance Systems, *delivered at VSSN '05*. November 11, 2005, Singapore.

This article contains a broad description of modern video surveillance systems. The author explores biometric systems, tracking, magnification, and object separation software, in addition to coordinated camera networks. Not only is this article useful in framing the Purpose of this paper, but it is also invaluable in providing good descriptions of various video surveillance technologies currently in use, as part of the content analysis. The author makes only passing reference to privacy rights concerns. Focus is on specific application of modern video surveillance systems as compared to both the perception of video surveillance and the reality of tradition CCTV systems.

This article provides many of the video surveillance applications considered in the content analysis section of this paper. Rita Cucchiara is a professor of Computer

Engineering, University of Modena. She is a leader in the study of image processing, pattern recognition and multimedia systems in both Italy and the European Union.

Farmer, D. & Mann, C. (2003, April). Surveillance Nation: Part 1. *Technology Review*, 106 (3), pp. 34-42.

This text illustrates a number of applications for video surveillance systems currently in use along with a discussion of the potentially beneficial nature of video surveillance. The authors note how video surveillance hardware is becoming inexpensive concurrent with ever more powerful software applications that analyze data collected and incorporate it into larger surveillance databases. This article and its companion provide useful insights that assist in development of the Purpose and Problem Areas of this paper.

Without providing strict timelines, the authors posit that video surveillance systems, especially those operated by individuals, will become ubiquitous. The text goes on to illustrate how one's privacy might be affected by the advances in video surveillance technology, particularly as video surveillance data is merged with the variety of other information that is captured from retailers and government. The combining of disparate data creates problems for both the individual and for those who would seek to use the data. The classic information systems problems of "garbage in, garbage out" and "data scrubbing" mean that the compendium of data about an individual is likely to contain errors that limit the data's accuracy, and one would assume jeopardy to the individual. Like an error on a credit report, an individual may find themselves the victim of inaccurate data collected on them that becomes difficult to correct.

This text is written by Charles Mann, a contributing writer for "Technology Review" and software engineer Dan Farmer who was formerly chief of network security for such technology companies as Sun Microsystems, Silicon Graphics, and Earthlink (Buderi, 2003). It is very useful in not only providing some current applications of video surveillance systems, but in also portending how continued advancements in these systems might impact American society.

Section 2. Video Surveillance and Privacy Rights

Calvert, C. & Brown, J. (2000) Video Voyeurism, Privacy and the Internet: Exposing Peeping Toms in Cyberspace*, Cardozo Arts & Entertainment Law Journal*, 18 pp. 469-568.

The authors provide a unique perspective of how current privacy laws are lacking in regard to private surveillance of individuals within the public space. While common notions of privacy in America would seem to dictate that one's undergarments would be protected from photograph or surveillance, when being worn, the authors provide numerous examples of how the area beneath one's dress is subject to photograph or video surveillance, and how such images often end up posted on the Internet. Convictions for "up-skirting" are rare and when obtained, are commonly based on public nuisance laws.

While this article highlights a relatively pedestrian misuse of video surveillance technology, it clearly frames the concerns of many regarding the potential use and abuse of privately operated video surveillance systems within this paper's Problem Area.

At the time of writing, Clay Calvert was an Assistant Professor of Communications and Law and Co-Director of the Pennsylvania Center of the First Amendment at Pennsylvania State University. Justin Brown was doctoral candidate in Mass Communications also at Pennsylvania State University.

Intille, A. (1999). Video Surveillance and Privacy: Implications for Wearable Computing, *Suffolk University Law Review*, 32 pp. 729-765.

This article begins with a discussion of the history of Privacy Rights and common law rights to privacy law beginning with Warren and Brandeis and their seminal work on common law privacy. First and Fourth Amendment privacy rights and the Restatement (Second) of Torts and the Privacy Right of Intrusion are also discussed.

The author maintains that with any technological change new intrusions into privacy arise. At the time, Brandies was deeply concerned about the new technology of "instantaneous photographs" which allowed newspapers to publish pictures of people taken in public that might cause their embarrassment. The article proceeds to discuss how video surveillance is often treated differently than audio recordings under federal legislation. In the final pages of the article, the author discusses how privacy rights might be applied to wearable computers.

While video surveillance, particularly tracking applications is only briefly covered, this article provided a broad description of privacy rights that is valuable in informing the Purpose Area of this paper.

The Suffolk University Law Review is the product of nearly 100 years of academic excellence. Suffolk University is dedicated to providing men and women the opportunity to study law regardless of their background.

Lyon, D. (2003a). Surveillance Technology and Surveillance Society. In Misa, T., Brey, P., & Feenbert, A. (Ed.), *Modernity and Technology,* Cambridge, MA: The MIT Press.

Dr. Lyon, a noted and frequently cited researcher on the sociological aspects of surveillance, is highly influential in any discussions of surveillance. This article, and others by the author, contributes to the framing, key definitions, and context within the Problem Area of this paper.

The thesis of many of Lyon's articles is that by living in a modern world, we are by definition, a part of a surveillance society. Dr. Lyon carefully explains that surveillance is not necessarily a precursor to evil intent or action; rather it may be viewed as used as a means of establishing and/or confirming trust relationships between individuals who are unknown to us. Nevertheless with the vast strides in computing power, networks, and database systems, disparate data about our lives can and is being collected by both government and private entities.

The author sees video surveillance systems as just one aspect of surveillance, yet his clearly expressed views on the perceived values and potential dangers of all types of surveillance prove invaluable to all aspects of this paper.

Nelson, L. (2004, May/June). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era, *Public Administration Review,* 64 (3) pp. 259-269.

Nelson approaches the issues surrounding video surveillance from primarily a public policy perspective. The author seeks to provide a balanced view of video surveillance by taking into account not only public safety and security concerns, but also issues of culture, ethics and perception. While the author discusses Fourth Amendment and

other privacy rights, she focuses on the tension between individual privacy and video surveillance conducted by both government and private entities.

Nelson's work is particularly useful in framing the larger societal debate about video surveillance in this paper's Problem Area section. Along with Lyon, Nelson believes that a broader discussion of the surveillance technology, security, and privacy must take place within society, both to inform the public and direct legislative action.

The author, Lisa Nelson, is an Assistant Professor in the University of Pittsburgh, Graduate School of Public and International Affairs and a fellow at the Philosophy of Science Center of the University of Pittsburgh.

Privacy under attack. (2001, June 15). *CQ Researcher,* 11 (23), pp. 505-528.
This issue of the Congressional Quarterly, provides a number of articles exploring American notions of privacy and their erosion under the influence of electronic surveillance technologies.

The issue states that privacy is a relatively current concept within the American psyche, having developed after the colonial period when many communities had laws prohibiting persons from living alone. The issue further discusses the many opportunities for government, private entities, and employers to monitor an individual's actions without violating what the courts or Congress have deemed as privacy. In addition, the issue also provides an outline of past legislative action (or lack thereof) regarding protection of individual privacy rights.

The articles contained within this issue are useful to this study both in providing specific examples of questionable surveillance activities, as presented in the Purpose and Problem Areas in this paper.

Section 3: Relating to Method

Leedy, P.D. & Ormrod, J.E. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Pearson Education Inc.

The eighth edition of this book is divided into five parts that guide the researcher from the fundamentals of research through descriptions of various research methodologies to the final preparation of the research report.

Of particular value to this study, is the assistance this book provides in outlining the literature review process described in both the Problem Area and the Methodology sections.

Paul Leedy was a Professor at American University until his death in August 2002. Jeanne Ormrod is an affiliate Professor of Education at University of New Hampshire and a Professor Emeriti of Educational Psychology at the University of Northern Colorado. The book is an accepted standard text in college research methods courses.

Palmquist, M., (2005). *Content Analysis*. Retrieved January 24, 2006, from Colorado State University Department of English Web site: http://writing.colostate.edu/guides/research/content/

The author and his students at Colorado State University have developed a useful website as a resource for anyone conducting a content analysis as a part of their research project.

The website provides information on the history of content analysis, the uses of content analysis, and a description of various types of content analysis strategies. Of particular use to this paper is the description of the "conceptual analysis" and the eight-step process recommended for coding one's research. The application of this process to this paper is presented in the Methodology section.

Mike Palmquist is a Professor and Co-Director of the Center for Research on Writing and Communications Technologies at Colorado State University. A specialist in rhetoric and composition, Palmquist received his PhD from Carnegie Mellon University.

Chapter III -- Method of Study

The primary method employed for this study is the literature review (Leedy & Ormrod, 2005); specifically concerning the use of video surveillance technologies, their deployment by private entities, and the potential impact on personal privacy. The literature review is chosen as the primary method of study for the benefits it exhibits for exposing "new ideas, perspectives and approaches", (Leedy & Ormrod, 2005, p 64.) into the research problem. In addition, the opportunity to explore the research question broadly, though the ideas of individuals in a variety of disciplines, offers a unique perspective on the topic – one that provides an opportunity for unexpected observations. A conceptual analysis as defined by the Colorado State University Department of English (Palmquist 2005), provides the format for relevant data analysis. By reviewing literature in both the fields of video surveillance systems and privacy law, the researcher attempts to build a relationship between the two.

Palmquist's (2005) conceptual analysis strategy is employed to further define the research process. The strategy begins by identifying a research question. As discussed, the primary research question for this study is: "In what ways is personal privacy affected by the use of video surveillance systems when employed by private companies, and organizations to monitor, collect and process information about individuals in a public place?" From this overarching question, other more specific questions follow that help frame the study:

- What types of private video surveillance technologies are most frequently used in public spaces?
- In what ways are these technologies being used; and

- How is personal privacy potentially affected by the use of these technologies?

Data Collection

The data collection plan includes the determinations of the search criteria and the locations where the search should be conducted. For this study a variety of materials within an equally diverse resource base are collected. Literature for this study is gathered from academic, business, government, and legal databases, and http://scholar.google.com. Books and Databases available through the University of Oregon Library (libweb.uoregon.edu) are chosen for their ease of access and the variety of content they possess. The cross disciplinary nature of this study requires a search for material in areas beyond just technology, including public policy, privacy rights, business and commerce, and sociology. Figure 1, lists the databases and keywords utilized in literature collection.

Figure 1: Literature Collection Plan

Locations Searched:	*Search Criteria/Keyword Used:*
Academic Databases: Business Source Premier Academic Search Premier, Worldwide Political Abstracts Public Affairs Information Service Lexis-Nexis Academic National Criminal Justice Service Abstracts Sociology Abstracts	**Database search criteria:** Electronic surveillance Video surveillance Privacy, Right of Image analysis and video Computer vision Electronic monitoring in the workplace Visual electronic surveillance
Google Scholar	Electronic surveillance and visual or video
University of Oregon Library	Electronic surveillance

The results of initial literature collection return approximately 300 hundred prospective sources. The next step is to evaluate and determine relevance to the

main study question. This winnowing process uses additional criteria to eliminate materials that are not deemed relevant including:

- Eliminate articles that do not contain information on video or visual surveillance;
- Eliminate articles that are not sufficiently detailed in description of video surveillance systems to be meaningful;
- Eliminate articles that are marketing related with a primary focus on a specific products sale;
- Eliminate articles that are product comparisons;
- Eliminate all articles on employee surveillance;
- Eliminate articles that are not detailed enough to provide anything more than general information;
- Eliminate articles/books that are over 10 years old;
- Eliminate articles that deal primarily with foreign experiences;
- Eliminate duplicate articles.

Data Analysis

Once the literature is collected and selected, an eight-step conceptual analysis process, outlined on the Colorado State University Writing Lab website (Palmquist, 2005) is applied. The first step in the conceptual analysis process is deciding upon the "level of analysis" (Palmquist, 2005). Coding is conducted to identify specific words and phrases. A two phase process is employed to achieve a complete data analysis for this study. The first phase includes a reading of selected literature to address the concept of video surveillance technologies (hardware) and applications

(software) in use. The second phase identifies individual benefits in the use of video surveillance and the personal rights that may be impinged.

The next step in the conceptual analysis is determining the number of concepts to code for. In this study an interactive coding mechanism is employed to include concepts such as: "camera surveillance" in lieu of "electronic surveillance" or even "video surveillance". Figure 2 provides a list of pre-determined specific words and phrases that are used to code for the larger concept, in each phase of this step. Words and phrases are selected from a preliminary reading of source materials that describe the two larger concepts under investigation in this paper: (1) video surveillance technologies and their purported benefits; and (2) the potential infringements on privacy rights. These words and phrases are used as a departure point in the coding process. Similar terms and phrases that emerge during the initial exploration of the topic across disparate areas of inquiry (including sociology, public policy and law) are also noted. The final list of words and phrases used to guide the content analysis in relation to the two larger concepts is presented in Figure 2.

Figure 2: Concepts Aligned with Coding Words and Phrases

Larger Concepts:	**Words and Phrases used in Coding:**
Phase 1 – Technologies/Applications and Purported Benefits:	Video/Camera/Digital/Visual/Electronic Surveillance Object Separation Facial Recognition Gait Recognition Tracking Security Databases Monitoring Biometrics
Phase 2 - Potential Infringements on Personal Privacy Rights:	Personal/Individual/Private Liability/Infringement/Impingement Privacy, Right of Privacy Rights Privacy Expectations Public Interest/Public Good Public Space Public Surveillance Panopticon Loss of Privacy

Step three of the process requires a determination as to "whether to code for existence or frequency of a concept" (Palmquist, 2005). In this study both approaches are used – first to determine the existence of various kinds of video surveillance technologies and applications in phase one and also potential personal benefits and personal privacy liabilities in phase two, and then to determine the frequency of the appearance of each concept, as a way to understand "emphasis" as presented in the literature.

The fourth step of the conceptual analysis process demands an ability to distinguish between concepts. Digital video surveillance is a more specific subset of video surveillance which also includes CCTV (Davis, 2005). However, both types of surveillance are relevant to discussion to the primary research question. On the other hand, the appearance of the term "surveillance" without qualifier may imply both human, non-electronic surveillance, or perhaps, audio surveillance technologies, neither of which are especially relevant to this study. The notion of personal privacy is bounded for the conceptual analysis process by a definition, which emphasizes that privacy is a condition that is perceived by our normative expectations. One's feelings about the loss or gain of personal privacy are dependent on how we imagine the actions of others affect our privacy and can be very different from legal definitions of privacy (Nelson, 2004).

By step five, rules are established for coding and translation rules for source information. In this study, translation rules appear for such terms as: camera and video, privacy rights and right to privacy, as well as, applications and software. As formerly mentioned, the term "surveillance" has many meanings depending upon the source of material e.g. public policy, or law enforcement. The terms "personal" and "individual" are used interchangeably when related to privacy and privacy rights.

Step six deals with information that is deemed irrelevant. This researcher generally chooses to disregard terms and concepts that did not directly impact the main study question or the secondary questions that pertained to the central purpose of this paper. The set of criteria used to select data for analysis reveals the initial strategy.

Actual coding of the texts, step seven, is greatly eased by the use of computers software able to scan documents for words and phrases. By coding for the occurrence of explicit terms, (see: Figure 2: Concepts Aligned with Coding Words and Phrases), source literature is divided into two categories: video surveillance technologies and concerns for privacy.

Data Presentation

The final stage in the conceptual analysis process requires an analysis of results. As a result of the content analysis, two tables are developed. Tables present information on the selected types of video surveillance technologies used by private entities within the public space and a comparison of purported benefits of private video surveillance systems and the potential detriments to personal privacy that may result.

The first table is presented in Appendix A: Video Surveillance Technology Applications, which is formatted to provide the reader with a clear representation of the most common types of video surveillance technologies in use today as noted in the selected literature (see column one), followed by a brief description of each selected application in column two. In this case the term "application" refers to computer software or software/hardware combinations which process or enhance data from video surveillance cameras. A template for this table is presented in Figure 3.

Figure 3: Template for Appendix A: Video Surveillance Technology Applications

Video Surveillance Technology Applications	Description
Facial Recognition:	A biometric technology that analyzes features of a person's face, e.g. (skin shade, eye spacing, cheekbone width, mouth shape, etc…) and compares these attributes with attributes of facial pictures from a database.

The second table is presented in Appendix B: Private Use of Video Surveillance Technology, Purported Personal Benefits and Potential Personal Privacy Tradeoffs, which lists the same selected video surveillance applications (from Appendix A, column one) and aligns these with purported individual benefits of the video surveillance and potential personal privacy infringements that could transpire. A template for this table is presented in Figure 4.

Figure 4: Template for Appendix B: Private Use of Video Surveillance Technology, Purported Personal Benefits and Potential Personal Privacy Tradeoffs

Video Surveillance Technology Application	Purported Individual Benefits	Potential Personal Privacy Tradeoffs
Facial Recognition:	Identification of customers in retail setting. Ability to greet customers by name and recall previous purchases or preferences. Can be used to recognize shoplifters or individuals who are undesirable to the business.	Customers are unable to shop anonymously.

The final document of this study is presented in Appendix C: Do I Think That I Am Losing My Privacy? This document is designed to serve as a personal decision tool for citizens to use in their own evaluation of the potential purported personal benefits of video surveillance in comparison with potential personal privacy infringements. The tool is presented as a matrix wherein the user is able to rate each side of the video surveillance vs. privacy equation and develop a personal sense of risk vs. reward for each new technology. A template for this tool is presented in Figure 5, with sample data points included for demonstration.

Figure 5: Template for Appendix C: Do I Think That I Am Losing My Privacy?

	Purported Individual Benefits	X	**Potential Personal Privacy Intrusion**	Y
Video Surveillance Technology Application	Rating 1-10 1 = very little personal benefit 10 = very direct personal benefits	RATING	Rating -1 thru -10 -1 = little or no intrusion -10 = massive intrusion	RATING
Facial Recognition	• Prevents Crime • Prevents Terrorism • Shopkeepers know me instantly	8 2 4	• Face is recorded without my permission • My name and picture could be put on the Internet without my permission	-5 -1 -10
	Total	+14	**Total**	-16

Directions:

List each personal benefit/potential intrusion and assign a numeric value.

Total columns +X and -Y

How to Interpret Results:

The more positive the number, the greater the benefit in comparison to imposition on individual privacy. The more negative the sum, the more one's privacy is likely to be impinged.

Chapter IV – Analysis of Data

This chapter presents a description of the data analysis process and the results of the content analysis. The 12 selected literature sources used as a basis for the content analysis are:

1. Blitz, M. J. (2004, May). Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity. *Texas Law Review,* 82 (6), 1349- 1481.

2. Calvert, C. & Brown, J. (2000) Video Voyeurism, Privacy and the Internet: Exposing Peeping Toms in Cyberspace*, Cardozo Arts & Entertainment Law Journal*, 18 pp. 469-568.

3. Cucchiara, R. (2005,). Multimedia Surveillance Systems, *delivered at VSSN '05*. November 11, 2005, Singapore.

4. Dority, B. (2001, May/June). Big Brother is Watching. *The Humanist*, 61 (3) pp. 9-13.

5. Farmer, D. & Mann, C. (2003, April). Surveillance Nation: Part 1. *Technology Review*, 106 (3), pp. 34-42.

6. Farmer, D. & Mann, C. (2003, May). Surveillance Nation: Part 2. *Technology Review*, 106 (4), pp. 46-52.

7. Intille, A. (1999). Video Surveillance and Privacy: Implications for Wearable Computing.*Suffolk University Law Review*, 32 pp. 729-765.

8. Lyon, D. (2002, April). Everyday Surveillance: Personal data and social classifications. *Information, Communications & Society,* 5 (2), pp. 242-257.

9. Lyon, D. (2003a). Surveillance Technology and Surveillance Society. In Misa, T., Brey, P., & Feenbert, A. (Ed.), *Modernity and Technology,* Cambridge, MA: The MIT Press.

10. Nelson, L. (2004, May/June). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era. *Public Administration Review,* 64 (3) pp. 259-269.

11. Privacy under attack. (2001, June 15). *CQ Researcher,* 11 (23), pp. 505-528.

12. Slobogin, C. (2002, Fall) Symposium: Public Privacy: Camera Surveillance of Public Spaces and the Right to Anonymity. *Mississippi Law Journal,* 72, (1) pp. 213-315.

The content analysis is conducted in two phases using the words and phrases presented in Figure 2: Concepts Aligned with Coding Words and Phrases, as seen in the Chapter III – Method. The results of the coding process are displayed in Figure 6: Data Analysis Coding Tally Results. The first phase of coding uses the words and phrases from the Technologies/Applications and Purported Benefits section of Figure 2. The second phase of coding uses words from the Potential Infringements on Personal Privacy Rights section of Figure 2.

In the first phase of coding, the word or phrase, e.g. "facial recognition", is inserted into a text search tool. The search tool then displays the number of times that word or phrase occurs within each of the literature sources. The usage of each word in the sentence is visually scanned before inclusion in an effort to ensure that the usage of the word is germane to this study and not an aberrant reference. For example, when scanning the document for the word "security", the word "security guard" was returned. This usage is not deemed by the researcher to be relevant to the goals of the content analysis; therefore any use of the word "security guard" is ignored, as noted in Step 6 of the content analysis plan, on how to handle irrelevant information.

In addition to the words and phrases listed in Figure 2, similar words and phrases are also inserted into the text search tool for location within the documents, e.g. "face" and "recognition", as noted in Steps 4 and 5 of the content analysis plan, addressing how to distinguish between concepts and translation rules, respectively.

In the second phase of coding, words and phrases from the Potential Infringements on Personal Privacy Rights section of Figure 2 are inserted into the text search tool in the same manner as described in phase one coding. The incidents of similar words and phrases to those presented in

Figure 2, Phase 2 are also searched for in the same manner as described above with one exception. The usage and context of the words "personal", "individual", and "private" are not evaluated for efficacy within the documents; instead, every occurrence of these three words is counted without regard to how they were used within the scanned document. The researcher's intent in not evaluating the usage of these words is to gather an impression of whether the document is generally concerned with issues of personal or individual privacy. When one of these search words or phrases is located during the coding process, the researcher returns to the specific text and the detailed context surrounding the search word or phrase is further examined as a way to identify examples of how video surveillance technologies are commonly used, why they are used, and/or in some cases where there may be areas of concern for personal privacy. Documents with a higher tally of keyword incidents, within either phase one or phase two coding, are generally more productive ground for descriptive materials.

The product of phase one of the coding process is a list of the most common video surveillance applications identified in this set of literature. The five most frequently mentioned video surveillance applications are presented and defined in Appendix A. They include: Monitoring a sub-set of the security application), Facial Recognition (the ability to compare captured video facial images to a database of known faces), Merging Video Surveillance with Larger Databases (the inclusion of captured video images with other personal identifying information), Tracking (the ability to follow an individual's activities across a broad area, and Security (which includes protecting and defending a place or persons within a space or deterring inappropriate or illegal actions). Appendix A includes a brief description of each of these technology applications in relation to use by private entities, within public spaces.

The product of phase two of the coding process (see Appendix B) is a list of purported personal benefits to each of the types of video surveillance technology applications (identified during phase one coding), aligned with a list of potential personal privacy tradeoffs. The two lists in Appendix B are derived from an examination of the text surrounding each occurrence of the keywords used in both stages of the coding process, when a discussion of personal benefits or privacy concerns in the use of video surveillance technologies is revealed. In an effort to simplify the presentation of this information, the lists in Appendix B are generalized descriptions of the purported personal benefits and potential privacy concerns. These descriptions were synthesized from examples presented in the content analysis source material. While this is a relatively complete list developed from the content analysis, purported benefits and potential privacy concerns are best judged independently by each individual; therefore the reader is encouraged to think broadly and imaginatively in using the evaluation tool contained in Appendix C.

Many of source materials used in the content analysis process contain substantial discussion of the government's (particularly law enforcement's) use of video surveillance and the resulting privacy concerns. While some of this conversation on privacy is useful in informing this study, as many of the privacy concerns are analogous, privacy concerns revolving around constitutional issues do not apply to private sector uses of video surveillance (CQ Researcher, 2001). As this study is concerned with the use of video surveillance technologies by private entities, Appendix B omits references to government use of video surveillance or the privacy concerns that may result solely from governmental use.

Nelson (2005) aptly argues that personal privacy is a function of one's perceptions; what one person may find an intrusion, another finds as a benefit (Nelson, 2004). Appendix B seeks to align the video surveillance applications and their purported benefits, as noted in the literature, with potential

personal privacy tradeoffs in a manner that is easy to compare. It should be noted that this alignment is based on the researcher's own perceptions, following the insight provided above by Nelson (2004). In general, the purported benefits of video surveillance usually focus on issues of deterrence of actions, or protection from harm. The predominant concerns for privacy revolve around loss of anonymity and the fear of unauthorized influence and control (Lyon, 2003).

Figure 6: Data Analysis Coding – Tally Results **Figure 6: Data Analysis Coding – Tally Results**

Data Analysis Coding Tally	Farmer & Mann, Apr 2003	Farmer & Mann, May 2003	Lyon, 2002	Blitz, 2004	Calvert & Brown, 2000	Intille, 1999	Slobogin, 2002	CQ Reseacher, 2001	Lyon, 2003	Nelson, 2004	Dority, 2001	Cucchiara, 2005	**Totals**
Video Surveillance Technologies:													
Phrase/Keyword							Incidents/	Frequency					
Video Surveillance/Surveillance													
Video	2	1	1	99	5	50	10	13	2	0	4	25	**212**
Camera Surveillance/Surveillance													
Camera	8	1	3	0	12	3	64	13	2	0	10	3	**119**
Digital Surveillance	3	0	0	4	0	0	0	0	0	0	0	0	**7**
Visual Surveillance	0	0	0	4	0	0	1	0	0	0	0	0	**5**
Electronic Surveillance	0	2	2	4	1	0	2	0	1	0	0	0	**12**
Biometrics	0	1	1	61	0	0	2	1	5	2	1	13	**87**
Object Separation	0	0	0	0	0	0	0	0	0	0	0	9	**9**
Facial Recognition	1	1	0	65	0	1	3	9	0	1	7	27	**115**
Gait Recognition	0	0	1	0	0	0	0	0	0	0	5	0	**6**
Tracking	0	0	0	45	0	6	4	1	0	1	0	23	**80**
Security	4	3	4	22	12	2	4	0	8	4	4	4	**71**
Databases	19	29	1	32	0	1	1	9	8	0	4	1	**105**
Monitoring	15	5	1	41	3	5	14	13	12	2	4	2	**117**
Concerns of Privacy:													
Phrase/Keyword							Incidents/	Frequency					
Personal	4	3	1	21	6	12	9	43	25	27	0	2	**153**
Individual	2	0	0	161	35	20	61	28	11	40	6	1	**365**
Private	2	1	0	121	52	37	23	26	7	29	5	2	**305**
Liability/Infringement/Impingement	3	0	0	1	5	1	1	1	0	2	1	0	**15**
Privacy, Right of	0	0	6	5	2	23	0	0	0	2	0	0	**38**
Privacy Rights	0	0	0	7	3	34	1	6	0	1	4	0	**56**
Privacy Expectations	0	4	0	76	67	15	20	1	0	21	1	0	**205**
Public Interest / Public Good	0	1	0	2	0	3	1	0	0	4	0	1	**12**
Public Space	1	0	1	92	1	5	2	0	2	1	1	0	**106**
Public Surveillance	0	0	0	8	0	0	24	0	2	0	0	0	**34**
Panopticon	0	4	1	1	0	0	0	0	3	0	0	0	**9**
Loss of Privacy	0	1	0	1	0	0	0	1	0	8	0	0	**11**

Chapter V – Conclusions

With the growth in sales and use of video surveillance cameras and equipment, Americans are subject to more surveillance than ever before (Buderi, 2003; Farmer & Mann, 2003). While this trend puts pressures on our perceptions of personal privacy, the perceived benefits in terms of service and/or security may outweigh an individual's privacy concerns. However, making such a determination is difficult. As noted by Nelson (2004) whether individuals consider their privacy to be endangered by this increase use of video surveillance depends largely on their normative perceptions of their privacy. It remains to be seen whether the public's expectation of privacy will change with the increased use of this technology (Nelson, 2004).

The courts have been reluctant to view any private video surveillance in public spaces as an invasion of privacy largely based on the argument that one cannot have an expectation of privacy within a public space (Blitz, 2004; Calvert & Brown, 2000; Intille, 1999; Iraola, 2003). As new video surveillance technologies become widely available, one wonders whether they will continue to maintain that view.

Unfortunately, there has been limited public debate concerning the use of private video surveillance and its effect on privacy (Marks, 2000). Absent a larger public discourse, state legislatures and Congress have largely been seen as reactive in their approach to privacy legislation. The Video Privacy Protection Act following the Judge Bork nomination to the U.S. Supreme Court is but one example (CQ Researcher, 2001).

While waiting for this public discourse to begin in earnest, Appendix C is presented as a personal decision tool for citizens to use in their own evaluation of the purported personal

benefits of video surveillance in comparison with potential personal privacy infringements. The tool is designed in the form of a matrix, allowing examination of five key video surveillance technologies. Each is described in some level of detail, below:

- ***Monitoring*** is the sustained attention directed toward the actions of an individual or group. Individuals are most likely to encounter monitoring in shopping centers, parking lots, city sidewalks, store aisles, and in many other locations where people are in motion. Perhaps the most heavily monitored private areas are casinos. It's important for individuals to realize that the proliferation of inexpensive networked video surveillance and web sites such as video.google.com, video.yahoo.com and youtube.com allow video surveillance footage, recorded in a public space, to be uploaded for anyone's viewing.
- ***Facial Recognition*** is the ability to compare a person's facial features to those in a database of faces. While the application is analogous to being recognized by a fellow human, the fact that one could be recognized anywhere by people one does not know should be a concern. For example, visiting a local department store and receiving personal recognition by a clerk may make one feel special; however, visiting another branch of the same department store chain in a distant city and receiving the same kind of personal recognition may seem a bit unnerving.
- ***Video Merged into Other Databases*** is the inclusion of video information into databases of other collected surveillance information. As Lyon's (2003) describes, we freely give up our personally identifying information for the sake of convenience (Lyon, 2003), such as customer loyalty cards. However, video surveillance records of our movements, our actions, our facial characteristics may

all be included into "customer" databases with other personal information. The impact on privacy from the collection of these discrete pieces of information may seem minimal, but the picture tends to change when all of these sources are compiled into a dossier.

- ***Tracking*** is analogous to being visually followed. While the federal law prohibits the recording of an individual's voice without their consent, there is no prohibition on recording a person's movements (Blitz, 2004). This omission in the law may create a privacy concern regarding freedom of association and movement.
- ***Security*** is the original video surveillance application. Any security application seeks to protect people and property through deterrence or subsequent prosecution. Most people accept the use of this application around or within group residences (such as apartment buildings) or a place of business. The growing use of security applications to monitor purely public spaces (sidewalks, streets, parks, etc), is now raising the most concern.

Do I Think That I Am Losing My Privacy? (see Appendix C) is a decision support tool, designed to enable the user to rate each side of the video surveillance vs. privacy equation and develop a personal sense of risk vs. reward for each video surveillance application. The intent of this tool is to help individuals determine their own views of a particular application of video surveillance technology in hopes of stimulating the public discussion of the private use of video surveillance. An example is provided within Appendix C, concerning the use of a video camera to monitor the entrance lobby of an apartment building. This application is a common form of security technology, and while it offers a sense of safety, at the same time it creates a sense of intrusion into personal affairs. These benefits/concerns are briefly

articulated in the body of the matrix, as a way to demonstrate its use. The rating of each benefit/concern is left for the reader to fill in.

Once the reader has rated and tabulated each of the gray columns (X and Y), the negative number from column Y (potential privacy infringements) can be subtracted from column X (purported technology benefits). A positive sum of the two columns would indicate that on balance the reader sees the video surveillance application as a net benefit; a negative sum would indicate that the reader would feel their privacy to be at greater risk than the benefits derived. The reader is encouraged to use this tool to rate other examples of video surveillance, within their own experience.

The video surveillance applications presented in this paper are those in common use today. However more sophisticated technologies, including those that use high magnification and infrared and microwave radiation, may soon be available which will further challenge our perceptions of privacy.

Appendix A: Video Surveillance Technology Applications

TECHNOLOGY	DESCRIPTION
Monitoring	The term "monitoring" can be applied to either a space or an individual. When applied to a space, the application of monitoring is often a subset of the security application. As applied to a person, monitoring implies the ability to target an individual for observation by video surveillance.
Facial Recognition	A biometric technology that analyzes features of a person's face, e.g. (skin shade, eye spacing, cheekbone width, mouth shape, etc…) and compares these attributes with attributes of facial pictures from a database.
Merging Video Surveillance into Larger Databases	With video surveillance moving from analog to digital technology, it is possible to capture images from video surveillance and insert those images into databases that contain other information.
Tracking	As with monitoring, tracking requires that an object or person is targeted. Once the intended object is targeted a tracking application will follow the object from one camera to another across a distance.
Security	Security is the original video surveillance application. Real time security monitoring is less frequently used than the ability to review a record of events from a particular camera. Primarily acts as a deterrent if well advertised within an area.

Appendix B: Private Use of Video Surveillance Technology, Purported Personal Benefits and Potential Personal Privacy Tradeoffs

TECHNOLOGY/ APPLICATION	PURPORTED TECHNOLOGY BENEFITS	POTENTIAL PRIVACY TRADEOFFS
Monitoring	Monitoring of a space may enhances security by deterring misdeeds Monitoring of an individual through a space may increase the safety of the person monitored. Monitoring to provide status information about road, construction, weather or other events visually to the public. Ability to monitor children or family at school, home, or in care facilities.	Monitoring of space does not allow persons to enter unobserved. Desire to move freely may be inhibited, if one is aware of monitoring. Difficult to feel alone or "unobserved" if video surveillance is present. Can be used to casually identify persons, if individual is identified, how long will one's image be stored? Notification of monitoring is not typically required in public spaces
Facial Recognition	Identification of customers in retail setting. Ability to greet customers by name. Ability to eliminate other forms of identification and move more quickly through airports and other lines. Ubiquitous use would make it difficult to become lost.	One cannot be in a public space with anonymity. Little legal defense to prevent dispersal of personal image to others private or governmental entities.

Merging Video Surveillance into Larger Databases	If retailers and other marketers know more about you, the argument goes; they are better able to meet your needs.	Aggregated data about one, may intrude into privacy more so than data that is dispersed. Erroneous data may lead to embarrassing or difficult situations. Difficult to correct bad data. If database is compromised, personal information and images could be used inappropriately.
Tracking	May ensure security of person tracked, e.g. from kidnapping. Ability to track one's belongings visually and apart from oneself.	Analogous to being followed through public spaces.
Security	Most common current application for video surveillance. May ensure safety of area through deterrence. Can be used to identify and/or prosecute suspects after a crime or misdeed.	Limited expectation of privacy of association, action, or movement, when one is in a public space.

Appendix C: Do I Think That I Am Losing My Privacy?

	Purported Individual Benefits	X	Potential Personal Privacy Intrusion	Y
Video Surveillance Technology Application	**Rating 1 -10** **1** = very little personal benefit **10** = very direct personal benefits	RATING	**Rating -1 thru -10** **-1** = little or no intrusion **-10** = massive intrusion	RATING
	Describe potential benefit….		**Describe potential intrusion…..**	
Monitoring For example, the new video camera mounted in the apartment lobby.	• Deters misdeeds • Increases safety of people in the complex. • Provides information about who is in the lobby. • Other (list your own)		• No one can enter lobby unobserved. • Actions may be inhibited. (e.g. kissing my partner). • Identity is noted and stored for an unknown period of time. • I don't know who's watching me. • Other (list your own)	
Facial Recognition Safeway grocery store begins using.	• I'm always greeted by name. • No longer need ID when cashing a check or using credit cards.		• Cannot shop at any Safeway anonymously. • I don't know people who seem to know me.	
Video Merged Into Other Databases Video included in customer rewards program database.	• Don't know how I benefit.		• Who else is my image being shared with? • What else do they know about me? • Is my information secure from theft?	
Tracking Private School uses tracking to watch children	• My children are monitored all day. • I can see what my child is doing anytime from my office.		• Is this changing my child's behavior?	
Security Private School installs security cameras	• Wrong-doing deterred. • Bullies are easily caught. • Safer school for my children.		• Are the video kept indefinitely? • Are children afraid of being recorded?	
	Total	**+**	**Total**	**-**

	Directions: List each personal benefit/potential intrusion and assign a numeric value. Total columns +X and -Y		**How to Interpret Results:** The more positive the number, the greater the benefit in comparison to imposition on individual privacy. The more negative the sum, the more one's privacy is likely to be impinged.	

References

Aronov, R.F. (2004). Privacy in the Public Setting: The Constitutionality of Street Surveillance. *Quinnipiac Law Review*, 22 pp. 769-810.

Beranek, B. (2005, August/September). Internet Protocol (IP) video surveillance. *Canadian Consulting Engineer,* 46 (5), p. 63.

Blitz, M. J. (2004, May). Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity. *Texas Law Review,* 82 (6), 1349- 1481.

Buderi, R. (2003, April). Our Surveillance Nation. *Technology Review,* 106 (3), p. 11.

Calvert, C. & Brown, J. (2000) Video Voyeurism, Privacy and the Internet: Exposing Peeping Toms in Cyberspace*, Cardozo Arts & Entertainment Law Journal*, 18 pp. 469-568.

Cucchiara, R. (2005,). Multimedia Surveillance Systems, *delivered at VSSN '05*. November 11, 2005, Singapore.

Davis, J. (2005, June). Surveillance Mini-boom. *Electronic Business,* 31(6), p. 23.

Douglas, M. (2005, February). City that works now the city that spys. [sic] *Mobile Radio Technology,* 23 (2), pp. 24-25.

Dority, B. (2001, May/June). Big Brother is Watching. *The Humanist*, 61 (3) pp. 9-13. Farmer, D. & Mann, C. (2003, April). Surveillance Nation: Part 1. *Technology Review*, 106 (3), pp. 34-42.

Farmer, D. & Mann, C. (2003, May). Surveillance Nation: Part 2. *Technology Review*, 106 (4), pp. 46-52.

Intille, A. (1999). Video Surveillance and Privacy: Implications for Wearable Computing. *Suffolk University Law Review*, 32 pp. 729-765.

Iraola, R. (2003, Winter). Lights, Camera, Action! - Surveillance Cameras, Facial Recognition Systems and the Constitution. *Loyola Law Review*, 49 pp. 773-808.

Jaeger, P.T., Bertot, J.C., & McClure C.R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. Government Information Quarterly, 20, pp. 295-314.

Kontzer, T. (2005, August 29). New York Spends $212M on Transit Security. *Information Week*, p. 24.

Leedy, P.D. & Ormrod, J.E. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Pearson Education Inc.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, 113 pp. 501, 504-05.

Lyon, D. (2001). *Surveillance society: monitoring everyday life.* Philadelphia, PA: Open University Press.

Lyon, D. (2003). Surveillance Technology and Surveillance Society. In Misa, T., Brey, P., & Feenbert, A. (Ed.), *Modernity and Technology,* Cambridge, MA: The MIT Press.

Lyon, D. (2003b). *Surveillance after September 11.* Malden, MA: Blackwell Publishing Ltd.

Lyon, D. (Ed.). (2003c). Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination New York: Routledge.

Marks, A. (2000, December 22). Smile! You're on hidden camera. *Christian Science Monitor*, 93 (21), p1.

Nelson, L. (2004, May/June). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era. *Public Administration Review,* 64 (3) pp. 259-269.

Palmquist, M., (2005). *Content Analysis.* Retrieved January 24, 2006, from Colorado State University Department of English Web site: http://writing.colostate.edu/guides/research/content/

Privacy under attack. (2001, June 15). *CQ Researcher,* 11 (23), pp. 505-528.

Slobogin, C. (2002, Fall) Symposium: Public Privacy: Camera Surveillance of Public Spaces and the Right to Anonymity. *Mississippi Law Journal,* 72, (1) pp. 213-315.

Staples, W. G. (1997). The Culture of Surveillance: Discipline and Social Control in the United States. New York: St. Martin's Press.

U. S. Constitution, Amend. IV

Bibliography

Aronov, R.F. (2004). Privacy in the Public Setting: The Constitutionality of Street Surveillance. *Quinnipiac Law Review*, 22 pp. 769-810.

Beranek, B. (2005, August/September). Internet Protocol (IP) video surveillance. *Canadian Consulting Engineer,* 46 (5), p. 63.

Black, J. (2002, September 27). When Cameras Are Too Candid. *Business Week Online,* Retrieved January 3, 2006, from http://www.businessweek.com/technology/content/sep2002/tc20020926_9020.htm

Blitz, M. J. (2004, May). Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity. *Texas Law Review,* 82 (6), 1349- 1481.

Buderi, R. (2003, April). Our Surveillance Nation. *Technology Review,* 106 (3), p. 11.

Burrows, Q. (1997, Summer) Scowl Because You're on Candid Camera: Privacy and Video Surveillance. *Valparaiso University Law Review,* 31, pp. 1079-1139.

Calvert, C. & Brown, J. (2000) Video Voyeurism, Privacy and the Internet: Exposing Peeping Toms in Cyberspace*, Cardozo Arts & Entertainment Law Journal*, 18 pp. 469-568.

Cucchiara, R. (2005,). Multimedia Surveillance Systems, *delivered at VSSN '05*. November 11, 2005, Singapore.

Davis, J. (2005, June). Surveillance Mini-boom. *Electronic Business,* 31(6), p. 23.

De George, R.T. (2005). *Business Ethics,* (6th ed). Upper Saddle River, NJ: Pearson Education Inc.

Douglas, M. (2005, February). City that works now the city that spys. [sic] *Mobile Radio Technology,* 23 (2), pp. 24-25.

Dority, B. (2001, May/June). Big Brother is Watching. *The Humanist*, 61 (3) pp. 9-13.

Farmer, D. & Mann, C. (2003, April). Surveillance Nation: Part 1. *Technology Review*, 106 (3), pp. 34-42.

Farmer, D. & Mann, C. (2003, May). Surveillance Nation: Part 2. *Technology Review*, 106 (4), pp. 46-52.

Fay, S.J. (1998, July). Tough on crime, tough on civil liberties: Some negative aspects of Britain's wholesale adoption of CCTV surveillance during the 1990s. *International Review of Law, Computers & Technology,* 12 (2), pp. 315-47.

Guirguis, M. (2004, December). Electronic Visual Surveillance and the Reasonable Expectation of Privacy. *Journal of Technology Law & Policy*, 9 pp. 143-181.

Hawkins, D. (2000, January 17). Cheap video cameras are monitoring out every move. *U.S. News & World Report,* 128 (2), pp. 52-54.

Here's Looking at You. (2001, December). *Scientific American,* 285 (6), p. 8.

Intille, A. (1999). Video Surveillance and Privacy: Implications for Wearable Computing. *Suffolk University Law Review*, 32 pp. 729-765.

Iraola, R. (2003, Winter). Lights, Camera, Action! - Surveillance Cameras, Facial Recognition Systems and the Constitution. *Loyola Law Review*, 49 pp. 773-808.

Jaeger, P.T., Bertot, J.C., & McClure C.R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. Government Information Quarterly, 20, pp. 295-314.

Katz v. United States. 389 U.S. 347 (1967) [Online] Available: http://www.lexisnexis.com/universe

Kontzer, T. (2005, August 29). New York Spends $212M on Transit Security. *Information Week*, p. 24.

Leedy, P.D. & Ormrod, J.E. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Pearson Education Inc.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, 113 pp. 501, 504-05.

Lyon, D. (2001). *Surveillance society: monitoring everyday life.* Philadelphia, PA: Open University Press.

Lyon, D. (2002, April). Everyday Surveillance: Personal data and social classifications. *Information, Communications & Society,* 5 (2), pp. 242-257.

Lyon, D. (2003a). Surveillance Technology and Surveillance Society. In Misa, T., Brey, P., & Feenbert, A. (Ed.), *Modernity and Technology,* Cambridge, MA: The MIT Press.

Lyon, D. (2003b). *Surveillance after September 11.* Malden, MA: Blackwell Publishing Ltd.

Lyon, D. (Ed.). (2003c). Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination New York: Routledge.

Marks, A. (2000, December 22). Smile! You're on hidden camera. *Christian Science Monitor,* 93 (21), p1.

McGrath, J. E. (2004). *Loving Big Brother.* New York: Routledge.

Milligan, C. S. (1999, Winter). Facial Recognition Technology, Video Surveillance and Privacy. Southern California Interdisciplinary Law Journal, 9 pp. 295-333.

Murphy, D. E. (2002, September 9). As Security Cameras Sprout, Someone's Always Watching. *New York Times,* p1.

Nelson, L. (2004, May/June). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era. *Public Administration Review,* 64 (3) pp. 259-269.

Palmquist, M., (2005). *Content Analysis.* Retrieved January 24, 2006, from Colorado State University Department of English Web site: http://writing.colostate.edu/guides/research/content/

Privacy under attack. (2001, June 15). *CQ Researcher,* 11 (23), pp. 505-528.

Public spaces have eyes. (2003, March). *PC Computing,* 13 (3), p.100.

Restatement (Second) of Torts 652. (1977), Retrieved January 18, 2006, from Havard University Law School website: http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm

Slobogin, C. (2002, Fall) Symposium: Public Privacy: Camera Surveillance of Public Spaces and the Right to Anonymity. *Mississippi Law Journal,* 72, (1) pp. 213-315.

Staples, W. G. (1997). The Culture of Surveillance: Discipline and Social Control in the United States. New York: St. Martin's Press.

Steel, K. (1998, June 22). Say cheese and keep on walking. Alberta Report/Newsmagazine, 25 (27), p. 31.

U. S. Constitution, Amend. IV

Warren, S. & Brandeis, L. D. (1890). *The Right to Privacy*, Retrieved January 17, 2006, from University of Louisville, Louis D. Brandeis School of Law Library website: http://www.louisville.edu/library/law/brandeis/privacy.html

Woodward Jr., J. D. (2002, March) Privacy vs. Security: Electronic Surveillance in the Nation's Capital. Testimony before the Subcommittee on District of Columbia of the Committee on Government Reform, United States House of Representatives, on March 22, 2002, p. 1-9. Santa Monica, CA: RAND.

Yang, C., Capell, K., & Port, O. (2005, August 8). The State of Surveillance. *Business Week*, pp 52-59.

Zerubavel, E. (1999). *The Clockwork Muse.* Cambridge, MA: Harvard University Press.