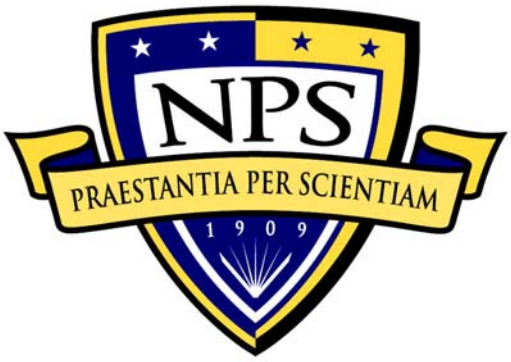
2008-03

"Someone to watch over me?" Privacy and governance strategies for CCTV and emerging surveillance technologies

Zoufal, Donald R.

Monterey, California. Naval Postgraduate School



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

"SOMEONE TO WATCH OVER ME?"
PRIVACY AND GOVERNANCE STRATEGIES FOR CCTV AND EMERGING SURVEILLANCE TECHNOLOGIES

by

Donald R. Zoufal

March 2008

Thesis Advisor:	Christopher Bellavita
Second Reader:	Diane J. Larsen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: "Someone to Watch Over Me?" Privacy and Governance Strategies for CCTV and Emerging Surveillance Technologies.		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Donald R. Zoufal			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT ***(maximum 200 words)***

Responding to concerns of terror around the world, law enforcement agencies are rapidly moving to utilize a range of surveillance technologies to address the threat. While the lead technology in this area is closed circuit television (CCTV), other technologies like radio frequency identification (RFID), global positioning satellite (GPS) technology and biometrics are also being expanded for use in monitoring human activity. These systems share common features and can be interrelated and controlled with developing computer technologies. They can also be used by government for a range of other purposes. However, use of these technologies has implications for individual privacy.

This research examines the nature of privacy and existing legal protections. It also investigates a range of approaches to govern the use of these developing technologies. It is a critical governmental function to administer the use of that technology to ensure that it is related to appropriate government purposes and that individual civil rights are protected. To be successful, that governance scheme will have to address key privacy concerns while remaining flexible enough to adapt to changing technology. Informed by this research policymakers will be better able to develop effective governance strategies.

14. SUBJECT TERMS privacy, anonymity, Panopticon, surveillance, technology, video surveillance, closed circuit television (CCTV), radio frequency identification (RFID), global positioning satellite (GPS) technology, biometrics, data collection, and data analysis.			**15. NUMBER OF PAGES** 215
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

"SOMEONE TO WATCH OVER ME?" PRIVACY AND GOVERNANCE STRATEGIES FOR CCTV AND EMERGING SURVEILLANCE TECHNOLOGIES

Donald R. Zoufal
Colonel, United States Army Reserve
B.A., University of Illinois, 1978
M.A.P.A., University of Illinois, 1980
J.D., University of Illinois, 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE OR MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2008

Author: Donald R. Zoufal

Approved by: Christopher Bellavita, Ph.D.
Thesis Advisor

Diane J. Larsen
Second Reader

Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Responding to concerns of terror around the world, law enforcement agencies are rapidly moving to utilize a range of surveillance technologies to address the threat. While the lead technology in this area is closed circuit television (CCTV), other technologies like radio frequency identification (RFID), global positioning satellite (GPS) technology and biometrics are also being expanded for use in monitoring human activity. These systems share common features and can be interrelated and controlled with developing computer technologies. They can also be used by government for a range of other purposes. However, use of these technologies has implications for individual privacy.

This research examines the nature of privacy and existing legal protections. It also investigates a range of approaches to govern the use of these developing technologies. It is a critical governmental function to administer the use of that technology to ensure that it is related to appropriate government purposes and that individual civil rights are protected. To be successful, that governance scheme will have to address key privacy concerns while remaining flexible enough to adapt to changing technology. Informed by this research policymakers will be better able to develop effective governance strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work would not have been possible without the love and support of many. My wife, Beth, and children, Jamie, Michael, and Genny, endured the long hours and endless work with love and patience. My advisor, Professor Bellavita, provided great insight and guidance in helping me find focus in the vastness of this field. My second reader, Judge Larsen, continually challenged me, helping me improve each of the many drafts. There are numerous other friends and colleagues who also provided help and support. To all, simple thanks is not enough; I know I owe more than I can repay.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Won't you tell him please to put on some speed
Follow my lead, oh, how I need
Someone to watch over me.[1]

A. WHAT IS THE ISSUE

The lyrics from the classic Gershwin tune echo the sentiment of security and comfort afforded by protective vigilance. As concerns of terror have spread across the United States and around the world, law enforcement agencies are rapidly moving to utilize a range of technologies to provide that sense of comfort and security. It is a critical governmental function to administer the use of that technology to ensure that it is related to appropriate government purposes and that individual civil rights are protected. To be successful, that governance scheme will have to address key privacy concerns while remaining flexible enough to adapt to changing technology.

One example of the use of technology to address threats is the expansion of closed circuit television (CCTV) technology. In the wake of 9/11, cities across America have been developing and implementing CCTV programs. These programs are often justified on the basis of combating terror acts. CCTV systems are, however, part of a larger trend by government to use developing technology-based surveillance solutions to address a range of purposes. In addition to CCTV, technologies like radio frequency identification (RFID), global positioning satellite (GPS) technology and biometrics are also being expanded for use in monitoring human activity. These systems can be interrelated and controlled with developing computer technologies.

The promise of surveillance technologies like CCTV is not solely, or, in some jurisdictions, even primarily, a surveillance measure designed for combating terrorism. Their uses are much broader. Technologies like CCTV can, and are, used by cities to

[1] George Gershwin and Ira Gershwin, "Someone to Watch Over Me," http://www.lyrics007.com/Gershwin%20George%20Lyrics/Someone%20To%20Watch%20Over%20Me%20Lyrics.html (accessed March 15, 2008).

address more routine crime and disorder problems. For example, CCTV has been used to secure downtown commercial areas and in high crime areas. The goals of these systems are crime suppression and building public confidence. There is also a growing movement to use a range of surveillance technologies, including CCTV, to manage traffic flow, enforce traffic laws, and for other regulatory purposes. In addition to functioning as a preventative or deterrent measure, digitized technologies like CCTV can also serve to guide response. For example, centralized CCTV systems permit greater command and control of resources deployed in response to emergencies both large and small.

While the ability to observe and monitor individual conduct in public has always been available to government, technology has developed in such a way that government's ability to efficiently monitor such conduct is greatly enhanced. As technology in the area of computers and digitization advances at an increasingly rapid pace, government can collect and analyze greater amounts of information. The convergence of technology that provides greater ability to collect information through devices like digitized CCTV systems, with greater ability to store and analyze that data makes technology enhanced surveillance programs different from surveillance conducted without the benefit of technology.

The government's expanded use of converging surveillance technologies for a range of purposes has raised concerns among privacy advocates. Those advocates contend that application of surveillance technologies in public places constitute an assault on personal privacy. At the extreme, they paint a picture of an Orwellian state where conformity is the norm and free thought and expression are repressed. The advocates contend that the law affords minimal protections for privacy. They offer a range of solutions from the prohibition of data collection tools to restrictive legislation that would place substantial burden on governmental agencies that seek to employ technology like CCTV for observation of public areas.

In response to concerns raised by the privacy advocates, proponents of the use of technology in public surveillance offer the suggestion that no real privacy interest exists for action in the public space. They point to an absence of constitutional prohibitions on visual surveillance programs in public space. They cite the long history of constitutional

jurisprudence suggesting law enforcement observations of activity in the public space is completely permissible. Much of the response focuses on challenges to data collection. Little effort is made to address what, if anything, will be done with information collected on public activity.

The issue at hand is the need to develop governance strategy for use of a range of developing technology. That strategy must understand and respect the use of developing technologies for a number of permissible governmental purposes in prevention, deterrence, and response. It must also respect the power of these new tools and potential impact they may have on individual rights.

B. WHY IS THE ISSUE IMPORTANT

The competing positions of privacy advocates and proponents of use of digitized surveillance technology provide policymakers with choices for determining how to properly govern the use and deployment of CCTV and other digitized surveillance technologies. As those technologies develop and become increasingly available, more and more jurisdictions will likely come to use them for a range of purposes. Though use of some technologies will relate solely to law enforcement purposes (e.g., CCTV cameras for observation of high crime areas or attempting to identify contraband); others will have functions that can be converted to law enforcement purposes (e.g., using traffic monitoring cameras to look for a vehicle fleeing the scene of a crime).

The implementation of these technologies involves competing values. Privacy advocates seek to advance values of personal freedom threatened by technology. Proponents of these technologies contend that implementation provides greater security and efficiency in a range of government operations. The current environment lacks clear guidelines for policymakers to balance these competing concerns.

There are also financial costs as well. The capital investment in computer and related equipment and software development for operation of these systems is significant. Failure to account for privacy concerns has resulted in abandonment of several surveillance schemes after the expenditure of substantial amounts of public funds. These

experiences demonstrate the need for development of principles that can guide policymakers in their collection and use of public surveillance information. Failure to create and operate under a set of guidelines exposes policymakers to the real possibility of establishing expensive surveillance systems that cannot be utilized.

C. HOW THIS ANALYSIS WAS CONDUCTED

Development of adequate governance strategies for the governmental use of developing digital surveillance technology, like CCTV, in public areas requires an understanding of the concept of privacy and how it relates to surveillance. Certain aspects of privacy may warrant greater protection, while others may not be greatly affected by public use of enhanced surveillance technology. There also may be aspects of surveillance that can actually support and enhance privacy.

In understanding the concepts of privacy and surveillance and their interrelation, analysis should focus on existing legal safeguards. Governance guidelines must be grounded in existing laws and legal principles. This will involve primarily a constitutional analysis of the protections extended to privacy. It will also analyze other legal protection afforded to privacy at the federal and state levels.

The next analytic step in the development of a governance strategy is to understand the range of digital surveillance technologies available and the uses, capabilities, and limitations of those technologies. Understanding the relation of CCTV to a digital family of technologies that can utilize common databases will help to develop guidelines that address all aspects of the surveillance technology, not just the collection of data from one source, but the use of that data as part of a related database. Guidelines that recognize the trends in technology driven data collection and usage will be more flexible and able to address a range of differing technologies. Understanding technology can also provide insights into how the technology, itself, can be shaped to mitigate effects on privacy.

The final step in development of a governance strategy is to look at examples of how privacy concerns in the deployment of technology are and can be addressed. Examining the experience of a country like the United Kingdom which has extensively employed CCTV systems can provide insights into governance issues for CCTV use. Contrasting those experiences with countries like France and Germany where CCTV is less pronounced, can provide further insight on governance structures. In addition to looking to international experience, examining the experience of Chicago, where there has been extensive litigation and court supervised regulation of surveillance activities provides further insights.

D. KEY FINDINGS

The application of the analysis outlined above presents policymakers with substantial guidance for the development of governance strategies with respect to use of surveillance technology in public areas.

1. Understanding Privacy

While privacy plays a role in promoting human freedom, it is not a unitary concept. Deconstructing privacy into differing component parts provides insights into what limits must be drawn and where aspects of privacy may need to be compromised. For example, the states of privacy such as seclusion and intimacy, critical to human development, require substantial protection. They are, however, not greatly impacted by public surveillance.

Other aspects of privacy are affected by developing technology. Reserve, the ability of an individual to control disclosure of personal information, is potentially impacted by growth of computer managed databases of digitized information. Unless that data is safeguarded the ability of individuals to control access to information about themselves is impaired. Similarly affected is that aspect of privacy referred to as anonymity, moving in public without being known. Anonymity has both positive and negative, even dangerous, implications. Social psychology research has established some

of the negative values that privacy brings. On the other side of the ledger, there are positive values of anonymity in fostering political and cultural critique and discussion.

Policymakers armed with an understanding of the differing aspects of privacy can better modulate their governance strategies to mitigate adverse effects. In some circumstances, applications of some technology that may affect only limited aspects of privacy may be acceptable. Technology that interrupts other aspects of privacy may not be accepted.

2. Understanding Surveillance

Important issues are raised by examining in greater depth the concept of surveillance. For example, with regard to CCTV usage in public places, it is unclear exactly what is properly considered surveillance. Some definitions suggest that surveillance only occurs when the techniques are individuated. Thus, the general observations of crowds are not surveillance. Whether or not this definition of surveillance is accepted, it suggests that it is the individuation of the activity of observation that should cause concern. Without individuation, the impact on privacy is much more limited. This line of thought should suggest differing rules of governance based on the use of the surveillance technology with enhanced protections where the observation activity is individuated.

Contrasted with general observation that is not individuated is the perfect surveillance state raised by the concept of the "Panopticon." The Panopticon is a form of prison design that allowed for individuated observation and management of information about all the individuals residing a particular cell house. All the activities of individuals were observed and recorded. The purpose of this perfect surveillance was to raise he specter of potential discipline, thereby ensuring conformity. Creating the perception of continual government observation and knowledge of individual activity was a key to this control.

The Panopticon effect raises important considerations for governance strategies regarding a range of aspects of the operation of public surveillance programs. The issue

of notice, for example, should be addressed in a way that it informs individuals without becoming oppressive. General observation should not be equated with individual observation to look for infractions requiring the imposition of discipline. This permits the individual to operate with some aspect of anonymity.

Moreover, understanding the concept of total surveillance demonstrated by the Panopticon should lead governance strategies to address the issues regarding the operation and use of databases containing surveillance information. It is the recording of this data that directly impacts the reserve aspect of privacy. Controls on dissemination and use of collected data may mitigate concerns over the impact on this state of privacy.

A final conclusion drawn from the analysis of the Panopticon is the notion that surveillance technology can actually serve to provide a check on government itself. Where surveillance programs are operated in a transparent fashion subject to public oversight, the operation of the government can be understood and examined. Accordingly, public accountability should be addressed in system governance.

3. Understanding Constitutional Protections

Analysis of existing constitutional jurisprudence demonstrates that significant protections are afforded to certain aspects of privacy. For example, there are substantial constitutional protections for seclusion and intimacy. Though protections for seclusion are largely restricted to the protection of areas like homes and residences, they extend to other areas and even public areas where bodily integrity and private communications are concerned.

Privacy states of anonymity and reserve have received lesser protections. Anonymity is protected only to the extent that impacting it affects the exercise of free speech or assembly. As to reserve, while there is some expression of concern over impacts on this value by large and complex compilations of computerized data, there is not definitive protection as of yet recognized under the Constitution for this value.

However, there is strong suggestion that concerns about reserve, if not appropriately addressed by government, may give rise to future court intervention to provide protections.

Constitutional protections are important considerations in development of governance strategies. Use of collection devices must be consistent with constitutional protections extended to seclusion and intimacy. Anonymity must be assured for the exercise of protected association and expressive activity. Moreover, safeguards should be employed to protect surveillance data collection consistent with respect for the privacy value of reserve.

4. Considering Other Legal Protections and Issues

In addition to constitutional protections for privacy, there are also protections that apply through federal statutes, state law protections and private rights of action. Most all these legal protections do not to extend to public surveillance activities, except those related to private communications. They do, however, provide some helpful principles for review in developing governance strategies. Federal statutes addressing the government's electronic surveillance of communications provide models for governance of individualized public surveillance activity. They address important concepts like authorization, oversight, notice and retention of information. Moreover, some recent state law cases raise the specter of a growing body of state law providing greater protection from individuated surveillance in public. These cases demonstrate a concern for surveillance directed at individuals without standards and oversight.

With respect to state law, certain provisions may actually pose impediments to protecting privacy interest, particularly with respect to compiled databases. State open records and freedom of information laws, designed to provide protections for transparency in government and citizen access to information, can actually serve to impair privacy rights. Unless appropriately addressed in governance strategies, these laws may require collection of data that is not required for system operation and unacceptably wide dissemination of data to third parties.

A final area of legal analysis concerns the right of remedy for impermissible intrusion on privacy rights. While many states have private remedies available for privacy right violations those rights are largely inapplicable to publicly observed conduct. In contrast, there is a robust body of federal remedies for privacy violations that implicate constitutional protections. Availability of remedy to individuals whose rights are violated should be part of a comprehensive governance strategy.

5. Assessing Technology

The assessment of technology reveals that CCTV is one of a wide array of developing digital technologies that can be used by government to observe human conduct. The purposes for and the ways in which those technologies are applied vary widely. In gross terms they can be analyzed in three groups of uses: detection of dangerous items and individuals; area observation and monitoring; and tracking individuals. The use of CCTV technology pervades all three groupings.

In the first group of uses, technologies, to the extent they can be focused solely on unlawful items or persons with a limited liberty interest, do not raise significant cognizable privacy concerns. These technologies can be highly intrusive. Additionally, the technologies that drive these surveillance systems are, as yet, unable to operate with sufficient accuracy and reliability to be employed. However, if and when these technologies can be employed with sufficient reliability to show in a binary fashion, the presence or absence of contraband, or the presence or absence of a person wanted on a warrant, they may be able to be employed with little concern over privacy implications. The lesson from these technologies for governance is to attempt to reduce surveillance technologies to binary outputs that indicate only the presence or absence of a person or material in which there is legitimate government interest. Additionally, the use of this technology has implications for data storage and subsequent use. This technology should only be employed in areas where detection is of critical importance (airports, public building and the like). Moreover, there is little reason for lengthy retention of this type of data.

The second group of uses embraces a wide number of visual and other sensor technologies that can be used to monitor human conduct in a given space. These technologies are not generally concerned with the identity of individuals. Instead, focus is on conduct and acts within areas that require some form of supervisory attention. Those areas may include: the surroundings of critical infrastructure; high crime areas; commercial areas or streets; and roadways. The purposes for observation may also vary. It may be to prevent crime, reduce traffic congestion, or direct response activities. Whatever the purpose, the government interest is principally satisfied in real time so there is little need to maintain data for lengthy periods of time. Unless the data is stored for long periods and individuated for some purpose, there seems to be little privacy impact to its collection.

In the third group of uses, technologies include a number of digital systems, CCTV, RFID, GPS, biometrics and cyber tracking, which are directed to track human activity. All these systems can be interrelated through computerized databases. Moreover, even where the primary purpose of the system is not law enforcement, the data can be analyzed and used for law enforcement purposes. For example, data from traffic observation CCTV cameras in the vicinity of a bank robbery may be used to determine the identity of persons in a getaway car, or RFID and CCTV information from a toll way pass system may be used to track a suspect. It is this concept of tracking individual activity in public space that impacts significantly the privacy states of anonymity and reserve. Given that fact, addressing this type of collection activity may warrant special consideration in the development of governance strategy. In developing such strategies, policymakers should consider heightened standards for initiating tracking activities, the duration and conduct of those activities, and greater supervisory oversight. Additionally, there should be considerations regarding notice and redress for the subject of such tracking.

Much of the use of CCTV and other digitized surveillance technology for human tracking turns on the use of large computerized data bases. It is perhaps the storage and use of digitized surveillance data bases that raises the most substantial privacy concerns. Even where all data involves matters of public record, the compilation and analysis of it

has been shown to implicate privacy concerns. In this sense, the privacy value of the whole is worth substantially more than the sum of the parts. The failure of government to properly account for and protect the privacy interest of reserve, which is potentially impaired by large collections of data, has derailed several multi-million dollar state and federal programs designed to use computer data bases to provide intelligence data on human activity.

6. Case Studies of the United Kingdom, France, and Germany

Studying the development of CCTV in the United Kingdom, France and Germany provides some interesting insights for developing governance strategies here in the United States. In the United Kingdom, the legal environment for CCTV was relatively unconstrained at the start. This allowed for a substantial proliferation of CCTV systems.

In the wake of a high profile case where CCTV data was disseminated to the media and broadcast and in the face of the adoption of a data protection law, structures were developed to begin regulating CCTV. The system in the United Kingdom is predicated on self-regulation in accordance with a CCTV code of conduct. This system provides flexibility to permit CCTV growth, but some critics contend that the regulation lacks aggressive enforcement.

In contrast to the United Kingdom, both France and Germany have much more stringent legal regulation of data protection and the use of CCTV for surveillance of public areas. In Germany, for example, there is a requirement for state legislation before CCTV cameras are permitted. In France, there are substantial administrative requirements that must be satisfied. In both countries, the use of CCTV is significantly less than the United Kingdom. However, news reports from both countries, particularly France suggest they may be adapting their laws to allow greater use of CCTV particularly for anti-terrorist purposes.

The key lessons from these case studies seem to be a convergence of thought regarding the use of surveillance technology. In the United Kingdom, there is a growing recognition of privacy implications of surveillance and the need to regulate it to protect

privacy interests. In France, there is recognition that the stringent administrative requirements retard application of CCTV and deprive government of a useful security tool. Understanding the effects of differing governance schemes and the need to balance between weak self-regulation and detailed centralized regulatory schemes provides helpful guidance to policymakers.

7. The Chicago Experience

The Chicago experience through its two federal court consent decrees also provides policymakers with important insight on how to develop governance of surveillance systems. Under the first consent decree Chicago operated with a procedurally detailed regulatory structure which did not afford sufficient flexibility to operate a public CCTV surveillance system. The modified consent decree which still imposes requirements for written policy development, training and audits, affords significant flexibility to allow for the operation of a large CCTV surveillance network. This experience demonstrates that systems can operate effectively within constitutional bounds with some regulation and oversight. It also demonstrates the importance of audits or other processes to maintain system accountability.

8. Next Steps

This research suggests that the next steps in harnessing the value of digitized surveillance technology like CCTV center on developing a governance strategy that addresses privacy concerns. There are a number of policy models that can be utilized to effect governance. Some are statutory with detailed mandates for conduct. Some, like the concept of self-regulation, are more flexible and likely more adaptable to manage a rapidly changing technology. Rigid statutory or regulatory structures will likely stifle deployment of emergent technologies. However, there will likely need to be some blend of legislative and regulatory approaches. For example, legislative enactments may be required to protect surveillance data from third party access, but subject access could be managed by a self-regulated process.

While there are differing structures offered by a variety of sources for addressing the privacy considerations of digitized surveillance data collection and use, they all seem to coalesce around a set of common principles. Those principles, articulated in the 1970s as the Fair Information Practice Principles (FIPP), provide a framework for development of governance strategies.[2] They include requirements of: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress.

Government policymakers in implementation of CCTV systems or any other digitized surveillance system should consider the FIPP in the application of the entities that are addressed in their system of governance. Additionally, policymakers should be mindful of the following concepts in their policy development and system operation:

- Privacy is not a monolithic concept
- Privacy is constitutionally protected
- Application of surveillance technology in public generally does implicate the fourth amendment
- Technology can and should be used to mitigate impacts on privacy
- Complex data bases in and of themselves have significant privacy implications
- Measures must be in place to ensure that practice conforms to written policies through supervision, training, discipline, and retraining of employees and internal and system audits.
- The pace of change in technology requires periodic review of policies and practices to ensure they are meeting governance goals

Developing an adequate governance system is a crucial component in the over all development and operation of CCTV and other digital surveillance systems. This consideration should be addressed early in the process so that system design can be adapted to support governance requirements.

[2] U. S. Federal Trade Commission, *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (accessed February 2, 2008).

E. PROBLEM STATEMENT

The threat of domestic terrorism combined with the increase in availability and sophistication of surveillance technology in publicly accessed areas and the advancing ability of the government to store and analyze massive amounts of public data has substantial implications for the privacy of citizens. Technological advancements in the areas of CCTV surveillance, biometrics, sensor technology, GPS and RFID monitoring, combined with enhancements in computer technology to store and analyze data collected from public sources, have implications on personal privacy. Existing legal protections do not address the complete spectrum of privacy concerns. Development of consistent and understandable ethical and legal standards and an accepted governance strategy for the application of surveillance technology in public areas will enhance the ability of local governments to employ developing surveillance technology consistent with legitimate privacy concerns. It can also help shape the design and development of surveillance technology so that it meets security requirements and protects privacy.

1. The Rise of CCTV Surveillance in the United States Post 9/11

The rise of CCTV surveillance in the United States post 9/11 offers perhaps the most vivid example of government employment of surveillance technology in public areas to address terrorist threats and the absence of comprehensive privacy protections. While the United Kingdom has long had an aggressive program of utilizing CCTV to address terrorist threats, other European countries have been more circumspect in application of CCTV technology. Large scale government use was not common in the United States prior to 9/11. Subsequently, the use of CCTV for surveillance of public areas has begun to be entertained in the United States.

The first large scale public area CCTV system was initiated in Washington D.C. shortly after the attacks in September, 2001.[3] While initially designed for

[3] Metropolitan Police Department, Washington D.C., "MPDC's Closed Circuit Television (CCTV) System," http://mpdc.dc.gov/mpdc/cwp/view,a,1238,q,541201,mpdcNav_GID,1545,mpdcNav,%7C31748%7C.asp (accessed September 17, 2007).

counterterrorism, the Washington D. C. system has been expanded to address ordinary crime problems in neighborhoods.[4] A similar phenomenon has occurred in Chicago. In 2004, Chicago announced development of a camera system characterized as the "most extensive in the United States."[5] The Chicago CCTV plan encompasses development of a surveillance system that includes both downtown areas and high crime neighborhoods.[6] Despite the lack of clear empirical evidence of CCTV impact on crime reduction, CCTV has been extremely well received by the residents of the high crime areas.[7]

The 2005 terror attacks in the United Kingdom served to bolster the position of many U.S. CCTV advocates. The Constitution Project notes in its "Guidelines for Public Video Surveillance"

> Within days of the July 2005 bombings on London's subway and bus system, authorities had identified the bombers, retraced their paths, and detained suspected accomplices thanks in part to footage from London's elaborate public video surveillance system. While the cameras did not prevent the attacks, their value in the subsequent investigation has reinvigorated movements, both in the United States and elsewhere, to develop similar systems. From Washington, D.C. to Paris, France to Cicero, Illinois, local officials are expressing renewed interest in video surveillance.[8]

---

[4] Metropolitan Police Department, Washington D.C., "MPDC's Closed Circuit Television (CCTV) System," http://mpdc.dc.gov/mpdc/cwp/view,a,1238,q,541201,mpdcNav_GID,1545,mpdcNav,%7C31748%7C.asp (accessed September 17, 2007).

[5] The Constitution Project, *Guidelines for Public Video Surveillance* (Washington D.C.: The Constitution Project, 2007), http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf (accessed September 17, 2007).

[6] Steven Kinzer, "Chicago Moving to 'Smart' Surveillance Camera," *The New York Times*, September 21, 2004, http://www.nytimes.com/2004/09/21/national/21cameras.html?ex=1190174400&en=8b9b4d48e88d756f&ei=5070 (accessed September 17, 2007).

[7] Mark J. Konkol, "Do Cop Cameras Give Crooks the Blues: Jury is Still Out," *Chicago Sun Times*, March 5, 2006, and Gary Washburn, "Another 100 Cameras Bound for Street," *Chicago Tribune*, October 4, 2006, http://pqasb.pqarchiver.com/chicagotribune/access/1139976581.html?dids=1139976581:1139976581&FMT=ABS&FMTS=ABS:FT&type=current&date=Oct+4%2C+2006&author=Gary+Washburn%2C+Tribune+staff+reporter&pub=Chicago+Tribune&edition=&startpage=2&desc=Another+100+cameras+bound+for+street+ (accessed September 17, 2007).

[8] The Constitution Project, *Guidelines for Public Video Surveillance*.

More recent terrorist activity in the United Kingdom has further reinforced support for CCTV in combating terror. In a recent *New York Times* article outlining the Lower Manhattan Security Initiative (LMSI), the value of London's similar CCTV system was highlighted. The LMSI is a $25 million program utilizing CCTV to monitor license plate information on vehicular traffic. The system is similar to the "Ring of Steel" a CCTV system in London to monitor access into the central London area. The article observes: "For all its comprehensiveness, London's Ring of Steel, which was built in the early 1990s to deter Irish Republican Army attacks, did not prevent the July 7, 2005 subway bombings or the attempted car bombings in London last month. But the British authorities said the cameras did prove useful in retracing the paths of the suspects' cars last month, leading to several arrests."[9]

While these systems may not prevent any given act of terror, as noted above, they clearly prove useful in bringing to justice the alleged perpetrators of such acts. Regarding the recent London attacks, within hours after the discovery of an explosives-laden vehicle left in central London, law enforcement officials were in pursuit of suspects. CCTV cameras had captured a good likeness of one of the terrorist suspects.[10] The quick apprehension of those suspects could be reasonably assumed to have prevented additional terror attacks, at least by that cell.

Washington D.C., Chicago and New York are not the only American cities in the process of implementing CCTV to address terrorism and street crime. Recently joining the ranks of those cities are Baltimore,[11] Newark,[12] and Charleston, SC.[13] In a 2007 report, the American Civil

---

[9] Cara Buckley, "New York Plans Surveillance Veil for Downtown," *The New York Times*, July 9, 2007, http://www.nytimes.com/2007/07/09/nyregion/09ring.html?ex=1341633600&en=2644be97bd9577f9&ei=5088&partner=rssnyt&emc=rssp (accessed September 17, 2007).

[10] Ian Stewart, "Glasgow Attacks Seen Tied to London Bombs," *The Washington Post*, June 30, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/06/30/AR2007063000562.html (accessed September 17, 2007).

[11] Martin O'Malley, "Mayor O'Malley Unveils New CitiWatch Control Center," City of Baltimore Press Release, May 12, 2005, http://www.ci.baltimore.md.us/news/press/050512.html (accessed September 17, 2007).

[12] William S. Sessions and Michael German, "Cameras Alone Won't Stop Crime," *The Star Ledger*, Newark, New Jersey, August 19, 2007, http://www.nj.com/starledger/stories/index.ssf?/base/news-0/118750266928240.xml&coll=1#continue (accessed September 17, 2007).

[13] Glenn Smith, "Cameras May Join City's Crime Fighting Arsenal," *The Post and Courier*, Charleston, South Carolina, August 29, 2007, http://www.charleston.net/news/2007/aug/29/cameras_may_join_citys_crimefighting_ars14298/ (accessed September 17, 2007).

Liberties Union (ACLU) of Northern California noted that some thirty-seven California municipalities had implemented CCTV programs, with most having been installed in the past few years.[14]

These recent developments regarding the use of CCTV are not the only areas where technology is applied to "public space." As noted above, the expansion of surveillance is seen in the use of biometric encoded identity cards used by a range of business and government agencies, the use of GPS coding on communication devices like cell phones and use of computer tracking and data mining techniques. Like the use of CCTV, government's use of these surveillance technologies is also growing. These technologies all raise some common questions concerning the issue of personal privacy.

2. Controlling the Government's Implementation of Surveillance Systems and Management of Data

In response to increased surveillance and the absence of legal protections for individual privacy rights, groups like the Constitution Project and the ACLU are urging imposition of legal restrictions. The Constitution Project has prepared extensive model legislation to address privacy concerns.[15] The ACLU of Northern California recommends that use of CCTV technology be stopped.[16]

Dissatisfaction with the extent of current federal legal protections for privacy has led some states to extend privacy protections under state law. This can be seen in state court decisions regarding government use of tracking devices to monitor movement in public areas. Two states, Oregon and Washington, have moved from the federal conclusion that application of these devices in public has no protected privacy implications.

As the government refines its ability to track individuals with common devices like public area CCTV and cell phones that emit GPS signals, this debate will likely

---

[14] Mark Schlosberg and Nicole A. Ozer, *Under the Watchful Eye: The Proliferation of Video Surveillance in California* (San Francisco: American Civil Liberties Union of Northern California, 2007), http://www.aclunc.org/issues/government_surveillance/aclu_issues_report_on_the_proliferation_of_video_surveillance_systems_in_california.shtml (accessed January 13, 2008).

[15] The Constitution Project, *Guidelines for Public Video Surveillance.*

[16] Schlosberg and Ozer, *Under the Watchful Eye.*

intensify in coming years. Privacy concerns have already resulted in the elimination or restriction in the use of programs that involve analysis of public activity. For example, concerns raised by civil right groups led to elimination of the Multi-State Anti-Terrorism Information Exchange (MATRIX)[17] program, which involved the collection and compilation of individual activity from public information.

The absence of accepted rules of governance protecting privacy presents an unsatisfactory state of affairs for state and local governments attempting to operate surveillance programs and develop the technology to support those programs. The existing legal theories that provide only limited privacy protection in public space were developed in the absence of technology that allowed government the ability to collect and analyze massive amounts of data to track the public conduct of individuals. The absence of clear guidelines on the use of public surveillance data constrains the ability of state and local governments to direct investment to technologies that will meet future legal and ethical scrutiny. This state of affairs is also unsatisfactory for citizens who may be operating under false expectation that their individual conduct is not the subject of government surveillance.

Governmental leaders committed to utilizing technology should recognize legitimate privacy concerns, especially with regard to compiled surveillance data, and implement protective measures. Failure to do so may undermine public support and result in litigation or onerous legislation burdening such programs. However, the development of safeguards needs to be accomplished in a way that does not deny government the use of surveillance technologies that can reduce terror threats, hinder the ability of government to respond to those threats or use technology for a range of legitimate governmental purposes.

---

[17] William J. Krouse, "The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project," *CRS Report for Congress* (Washington D.C.: Congressional Research Service, 2004) http://www.fas.org/irp/crs/RL32536.pdf (accessed January 26, 2008).

F. RESEARCH QUESTIONS

What is the impact of the emerging technologies on existing protections for privacy? What are the elements of privacy that should be generally accepted as critical to a democratic society, particularly in the wake of the development of these emerging technologies? Understanding those essential elements, what types of guidelines can be developed for governmental officials that can protect the legitimate privacy interests of citizens while at the same time allowing for the introduction of technological surveillance techniques that can enhance public safety and security?

G. PRACTICAL SIGNIFICANCE

Based on the information gleaned through the methodology outlined above, the essentials of a governance scheme for development and use of emergent surveillance technologies can be developed. Drawing on these essential elements, states and localities can be informed in the development of statutes, ordinance or appropriate regulatory processes to govern the implementation and operation of surveillance technologies. Such guidelines can be used not only in the operation of systems, but also to influence the industry developing technology so they can be directed in their efforts to produce technology that will be purchased and used. Implementation of uniform standards that acknowledge and provide protection for individual privacy should also serve to enhance public confidence in the government's operation of surveillance programs.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

The literature in the area of privacy and privacy protection is extensive.

The body of literature directly applicable to emergent technology is also growing. While applications of emergent technology vary widely, there are common themes that run through the literature. Those themes include an outline of the way in which technology can greatly enhance security, but oftentimes with hidden costs to privacy. There is also dissatisfaction with the existing protections for privacy in the U.S. This literature review included a survey of literature relevant to the area of privacy and the legal theories used to address public privacy concerns. Also reviewed is literature discussing the impact of privacy caused by several areas of emerging surveillance technology. The issues of governance are brought into focus through examination of case studies of CCTV deployment in other countries and the experiences of Chicago in the management of its surveillance programs. There is also ample literature examining a range of approaches to privacy governance.

B. UNDERSTANDING PRIVACY AND SURVEILLANCE

A wealth of literature on this issue, and a few important journal articles, relate the issue of privacy to American Jurisprudence. In his article, "The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—the Proper Balance,"[18] Emanuel Gross provides an excellent survey of the literature defining privacy. In his references at notes 6 through 26, Gross identifies numerous works addressing the essential elements of privacy. He also cites several important journal articles that reflect the thoughts of American legal scholars on privacy and the need for protections. Those works include the seminal work of Warren and

[18] Emanuel Gross, "The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance," *Cornell Int'l L. J.* 37 (2004): 27.

Brandeis, "The Right to Privacy,"[19] as well as more recent scholarship on the question of privacy's definition. While a range of approaches can be utilized with regard to defining privacy, this analysis will focus primarily on the analytic frame developed by Alan Westin.[20]

In addition to exploring the theoretical underpinnings of privacy, there is also a need to examine how those rights intersect with surveillance. The work of philosopher Michel Foucault provides an interesting perspective on surveillance its impacts on the relationship between the individual and the state. This work has spawned a substantial degree of international thought on the social and psychological impacts of surveillance.[21]

C. CURRENT LEGAL PROTECTIONS FOR PRIVACY

Analysis of the state of the law on privacy is bountiful. The issue of privacy is addressed in numerous written court opinions, legal treatises, and law journal articles. The sources of law addressing privacy include: federal constitutional and statutory requirements; state law requirements; and private rights of action statutory requirements; and common law requirements. One of the more important summary works in the area is Wayne Lafave's six volume treatise on the law of search and seizure.[22] This work is a compendium of the most important case laws and statutes regarding search and seizure in the United States.

1. Federal Constitutional Requirements

The federal constitutional protections for privacy are primarily found in the provisions of the fourth amendment. That amendment protects persons and their homes from unwarranted governmental intrusion. With regard to the protections of the fourth amendment, the primary case interpreting the reach of constitutional protections is the

---

[19] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard L. Rev.* 4 (1890): 193.

[20] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970).

[21] Michel Foucault, *Discipline and Punish, The Birth of the Prison* (New York: Vintage Books, 1995).

[22] Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, 4th ed., 6 vols. (St. Paul: Thomson/West, 2004).

U.S. Supreme Court decision in *Katz v. United States*.[23] Examining *Katz* and its progeny, along with the substantial body of legal commentary discussing those cases, provides a solid base for understanding legal theory regarding privacy in public areas. For example, some of the cases decided subsequent to *Katz*, provide greater refinement to the dimensions of fourth amendment protection.[24] It is also important, however, to delve into the range of additional protections for privacy under the first, ninth and fourteenth amendments to the Constitution so that the body of case law on public privacy is placed in a larger context.

With respect to the application of developing surveillance technology, the most significant recent case law development is found in *Kyllo v. United States*[25] and the literature discussing that decision. Understanding *Kyllo*, and its application in subsequent court decisions and the opinions of legal commentators will illuminate the likely shape of future decisions on the application of new technologies affecting privacy.

The literature tracking Supreme Court developments in the evolution of privacy protection, or as some critics would argue, absence of privacy protection is fairly dense. It gives a good understanding of the strengths and limitations of current federal constitutional jurisprudence on the subject.

2. Federal Statutory Provisions

In his article "Symposium: The Power and Pitfalls of Technology-Enhanced Surveillance by Law Enforcement Officials," Ric Simmons provides an excellent summary of the statutory requirements enacted for the government's use of technology to electronically intercept communications.[26] The literature analyzing the promulgation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)[27] provides

---

[23] *Katz v. United States*, 389 U.S. 347 (1967).

[24] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986); and *Florida v. Riley*, 488 U.S. 445 (1989).

[25] *Kyllo v. United States*, 533 U.S. 27 (2001).

[26] Ric Simmons, "The Powers and Pitfalls of Technology: Technology-Enhanced Surveillance by Law Enforcement Officials," *New York Univ. Annual Survey of American Law* 60 (2005): 711.

[27] The Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. §§ 2510-20 (2000).

insight on how governance strategies can be formulated. The case law and commentary analyzing the applicability of Title III and its expansion with the Electronic Communications Privacy Act of 1986 (ECPA)[28] provide a menu of issues that require consideration in governing technology to ensure privacy protection.

3. State Law Requirements

While the Constitution provides uniform protections for privacy across all fifty states, under our federal system states can provide enhanced protections. The federal Constitution provides only a common baseline for the protection of individual rights. While for many years most state constitutions were thought to provide no greater protections for individual rights than those provided by federal law, that paradigm is breaking down. Examination of the law in this area will show that states are diverging from the "lockstep" approach.[29] One such example is the decision of the Oregon State Supreme Court decision in *State v. Campbell*. [30] There that court provided additional protection against public surveillance activities.

As technology develops, it is likely more states may diverge from the federal baseline and provide enhanced privacy protection. These enhanced standards will have to be accommodated in the collection and use of any unified data collection and analysis system. Analysis of state law decisions diverging from the lockstep doctrine provides insight on should be beneficial in assessing the likely requirements for technology implementation. While the literature is scarcer on these subjects, review of primary source materials such as subsequent state court decisions should provide good insight into the developing body of state constitutional law regarding privacy protection.

---

[28] The Electronic Communications Privacy Act of 1986 (EPCA), 18 U.S.C. §§ 2701-2710 (2000).

[29] Robert F. Williams, "State Courts Adopting Federal Constitutional Doctrine: Case-by-Case Adoptionism or Prospective Lockstepping," *William and Mary L. Rev.* 46 (2005): 1499; Helen W. Gunnarsson, "The Limited Lockstep Doctrine," *Ill. Bar J.* 94, no. 7 (July 2006): 340.

[30] *Oregon v. Campbell*, 759 P.2d 1040 (Or. 1988).

4. Private Rights of Action

The issue of remedies for violations of privacy rights is important for governance. Common law provisions providing a private right of action for privacy infringements are outlined in the *Second Restatement of Torts*.[31] While the protections of tort law generally do not extend to governmental action because of immunities extended to government and governmental actors, the theories of legal protections for privacy may be instructive in developing remedies for persons whose privacy rights are violated. Also important to defining the picture of privacy protection is an understanding of the private right of action offered under federal law codified in 42 U.S.C. § 1983.

This private right of action approach is in many ways more similar to the European models that provide substantial protections to privacy. Review of these legal protections may provide theoretical underpinnings for guidelines to protect privacy interests. They may be particularly helpful for understanding how to protect against non-governmental use of surveillance data.

D. SURVEILLANCE TECHNOLOGIES

As digital technology matures and computer capacity continues to there is an increasingly sophisticated array of surveillance tools and techniques to gather and compile information on individuals.[32] There are a range of new technologies that implicate privacy concerns. Commentators analyzing the technologies have used a variety of formats to assess those technologies. Those approaches have centered on intrusiveness of the technique,[33] expectation of privacy in the area of examination[34] and even analysis of individual personal privacy expectations and measures taken to protect

---

[31] The Restatement (Second) of Torts (New York: West Publishing Company, 2006), http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (accessed March 4, 2008).

[32] Richard Posner, *Catastrophe* (New York: Oxford University Press, 2004) 88-9.

[33] Simmons, "The Powers and Pitfalls of Technology"; Patrick J. McMahon, "Counterterrorism Technology and Privacy," *Cantigny Conference Series* (Chicago: McCormick Tribune Foundation, 2005).

[34] Andrew Taslitz, "Enduring and Empowering: The Bill of Rights in the Third Millennium: The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions," *Law and Contemporary Problems* 65 (2002): 125.

privacy.[35] When analyzing the literature on surveillance, it may help to group the technology into five areas: contraband identification technology; area surveillance technology; tracking technology to monitor activity of suspect persons; cyberspace tracking; and developments in surveillance data management.

1. Contraband Identification Technology

The literature on the use of contraband detection technology continues to grow as technology solutions for the detection of contraband continue to refine. Much of the case law on the use of detection technology arises out of the use of canines and field testing equipment for detection of narcotics. This area of analysis of technologies that can only detect the presence or absence of a contraband substance is referred to by commentators as "binary search" technology.[36] Much of the literature centers on three cases.

Examining legal developments in light of U. S. Supreme Court decisions like *United States v. Place*,[37] *United States v. Jacobsen*,[38] and, most recently, *Illinois v. Caballes*[39] provides insight into how law enforcement can use binary search technology to address issues related to contraband. While the bulk of the analysis on this topic has focused primarily on the issue of narcotics, there are wide number of implications for development of binary search technology. The federal government is piloting various explosive detection technologies to secure public areas like airports and rail and bus stations and platforms.[40] A similar argument can be made for technology such as millimeter wave and backscatter x-ray technology that could be used to detect weapons

---

[35] Lee Tien, "Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law," *DePaul Univ. L. Rev.* 54 (2005): 873.

[36] Ric Simmons, "The Two Unanswered Questions of Illinois v. Caballes: How to Make the World Safe for Binary Searches," *Tulane L. Rev.* 80 (2005): 411.

[37] *United States v. Place*, 462 U.S. 696 (1983).

[38] *United States v. Jacobsen*, 466 U.S. 109 (1984).

[39] *Illinois v. Caballes*, 543 U.S. 405 (2005).

[40] Thomas Frank, "Security Devices Falter in Rail Tests," *USA Today*, February 13, 2007.

or bombs.[41] Review of the official websites of the Transportation Security Administration (TSA) demonstrates a range of uses envisioned for these technologies.

In light of the case law and commentary discussion of the binary search concept, the privacy features of CCTV surveillance could likely be enhanced by the addition of developing technologies such as ”intelligent video” and “facial recognition.” These technologies would focus the area surveillance on suspicious conduct, patterns, or persons. For example, intelligent video technology allows cameras to be programmed with algorithms allowing them to alert when suspicious conduct is recognized (e.g. leaving an unattended bag in a crowded terminal lobby or approaching and throwing and object over a perimeter fence or barrier).[42] This technology is relatively new and has generated relatively little peer reviewed literature. This is likely a result of the fast paced movement of technology in this area.

2. Area Surveillance Technology

The primary method of area surveillance involves the use of CCTV. The literature demonstrates that anti-terror and law enforcement are only some of the functions related to area surveillance. It also illustrates the applicability of digitized surveillance technology to area surveillance to such as traffic enforcement and monitoring, as well as, direction of response assets. Moreover, the literature demonstrates that the use of CCTV is not limited to the United States. On the contrary, there is extensive experience in the use of CCTV in the United Kingdom. The British use of CCTV is particularly interesting in light of the common legal experience of both

---

[41] Jon S. Vernick et al., “National Challenges in Population Health: Technologies to Detect Concealed Weapons: Fourth Amendment Limits on a New Public Health and Law Enforcement Tool,” *J. of Law, Medicine and Ethics* 31 (2003): 567; David A. Harris, “Superman’s X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology,” *Temple L. Rev.* 69 (1996): 1.

[42] Avi Nusimow, “Intelligent Video for Homeland Security Applications,” *2007 IEEE Conference on Technologies for Homeland Security*, Institute of Electrical and Electrons Engineers, Inc., New York, 2004, http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=4227766&arnumber=4227798&count=57&index=31 (accessed June 27, 2007).

countries and their commitment to civil rights. The extensive use of those systems has generated substantial literature on the subject of CCTV usage.[43]

While in the United States the use of CCTV covering public areas is solidly accepted as permissible under the fourth amendment, the discussion hardly ends there. There is a developing body of literature discussing the efficacy and privacy implications of such programs.[44] Examination of the literature on this subject suggests that a properly designed area oriented surveillance program can be squared with privacy concerns and protections.

3. Tracking of Suspect Persons

The tracking of individuals can be accomplished through a range of technologies. These technologies include CCTV, GPS systems,[45] and RFID systems,[46] and biometrics. These programs represent a shift of focus to activities of a specific individual. This seems to shift the nature of the privacy concerns implicated.

There is a growing body of material discussing the use of devices to track individuals even when that tracking is limited to public space. Beginning with the U.S.

---

[43] See, e.g., Michael McCahill and Clive Norris, *CCTV Systems in London, Their Structure and Practices*: *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*, Working Paper No. 10 (Hull, UK: Centre for Criminology and Criminal Justice, University of Hull, 2003), http://www.urbaneye.net/results/ue_wp10.pdf (accessed May 11, 2007); and Leon Hempel and Eric Topfer, *CCTV in Europe, Final Report*: *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*, Working Paper No. 15 (Berlin: Centre for Technology and Society, Technical University, 2004), http://www.urbaneye.net/results/ue_wp15.pdf (accessed May 11, 2007).

[44] Loren Siegel, Robert A. Perry and Margret Hunt Gram, *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight*, A Special Report by the New York Civil Liberties Union (New York: New York Civil Liberties Union, 2006), http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf (accessed May 11, 2007); Marcus Nieto, *Public Video Surveillance: Is It an Effective Crime Prevention Tool?* (Sacramento: California Research Bureau, 1997), http://www.library.ca.gov/CRB/97/05 (accessed January 22, 2007); U. S. General Accounting Office, *Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington D.C.*, Report to the Chairman, Committee on Government Reform, House of Representatives, 108th Cong., 2d sess., 2003, http://www.gao.gov/atext/d03748.txt (accessed January 22, 2007).

[45] April A. Otterberg, "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment," *Boston College L. Rev.* 46 (2005): 661.

[46] Reepal S. Dalal, "Chipping Away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights," *Boston Univ. L. Rev.* 86 (2006): 485.

Supreme Court decision in *United States v. Knotts*[47], there has been commentary and significant state case law developments concerning technology-aided, individualized surveillance occurring in the public space. Additionally, the relative maturity of GPS technology and satellite tracking capabilities has generated additional literature on this subject.[48] Add to these technologies the introduction of tracking through cellular communications technology[49] and RFID tracking,[50] and there is a mature body of literature exploring the implications of tracking capabilities on the privacy.

A related form of tracking revolves around the concept of identification technology, specifically biometrics. Biometrics is technology that uses certain biometric features like fingerprint, hand geometry, retinal scan or facial geometry to establish identity.[51] Newly developed federal programs utilizing this technology include: U.S. Visitor and Immigrant Status Indicator Technology (VISIT) program (which seeks to track the comings and goings of foreign nationals);[52] the Travel Worker Identification Credentials (TWIC) (which would allow the federal government to positively establish the identity of all persons working in the transportation field);[53] and the registered traveler (RT) program (which allows travelers expedited passage through airport security

---

47 *United States v. Knotts*, 460 U.S. 276 (1983).

48 William A. Herbert, "No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?" *I/S: A Journal of Law and Policy for the Information Society* 2 (2006): 409; John S. Ganz, "It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices," *J. of Criminal Law and Criminology* 95 (2005): 1325.

49 David J. Phillips, "Beyond Privacy: Confronting Locational Surveillance in Wireless Communication," *Communication Law and Policy* 8 (2003): 1.

50 Dalal, "Chipping Away at the Constitution," 485.

51 See generally, The National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics, *Biometrics Frequently Asked Questions*, http://www.biometrics.gov/docs/faq.pdf (accessed February 24, 2007); *Biometrics Overview*, http://www.biometrics.gov/docs/biooverview.pdf (accessed February 24, 2007); Margaret Betzel, "2004 Year in Review Special Topic: Biometrics: Privacy Year in Review: Recent Changes in the Law of Biometrics," *I/S: A Journal of Law and Policy for the Information Society* 1 (2005): 517; Rudy Ng, "Catching Up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology," *Hastings Communications and Entertainment L. J.* 28 (2006): 425.

52 See generally, U.S. Dept. of Homeland Security, *US-VISIT Program*, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed February 24, 2007).

53 See generally, U.S. Dept. of Homeland Security, Transportation Security Administration, *Transportation Worker Identification Credential (TWIC) Program*, http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed February 24, 2007).

lines).[54] Literature on these three particular federal programs demonstrates the range of capabilities for passive tracking of individuals through biometrics. This type of tracking to gain control of U.S. borders was strongly advocated by the 9/11 Commission.[55]

4. Cyberspace Tracking

Just as tools are developed to track individuals in physical public space, there is increasing ability of the government to track activities, preferences and movement in cyberspace. The tracking of a person's movements on the internet raises considerable privacy concerns. There is significant literature that examines the privacy implications of two government programs initiated by the FBI.

Through the "Carnivore" program, the FBI was able to trap internet[56] communications of suspect individuals without application for a warrant. Carnivore demonstrates the ability of the government to monitor individual conduct which can relate directly to the most intimate and private thoughts. Utilizing Carnivore the government can track all of an individual's electronic contacts. It collects and stores communications for later review if a warrant is issued. Commentators have noted this poses substantial implications for personal privacy in the digital age.[57] Similar concerns are posed by the FBI's keystroke logging systems like "Magic Lantern."[58] This program allows the government to access computers remotely and then monitor all the activity on the keyboards.

---

[54] See generally, U.S. Dept. of Homeland Security, Transportation Security Administration, *Registered Traveler*, http://www.tsa.gov/what_we_do/layers/rt/index.shtm (accessed February 24, 2007).

[55] 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, D.C.: U. S. Government Printing Office, 2004), p. 389, http://www.gpoaccess.gov/911/index.html (accessed May 11, 2007).

[56] See generally, IIT Research Institute, *Independent Technical Review of the Carnivore System* (U.S. Dept. of Justice, 2000), http://www.usdoj.gov/archive/jmd/carniv_final.pdf (accessed February 24, 2007).

[57] Maricela Segura, "Is Carnivore Devouring Your Privacy?" *S. Calif. L. Rev.* 75 (2001): 231; Raymond Shih Ray Ku, "Modern Studies in Privacy Law: Searching for the Meaning of Fourth Amendment Privacy after Kyllo v. United States: The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance," *Minnesota L. Rev.* 86 (2002): 1325, 1355.

[58] Christopher Woo and Miranda So, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance," *Harvard J. of Law and Technology* 15 (2002): 521.

5. Technology Developments in Surveillance Data Management

In addition to the use of cyber tools directed toward the computers of suspect individuals or organizations, another government use of computer technology raises significant privacy concerns. That tool is the use of powerful and complex government computer systems to coordinate and analyze massive amounts of data about individuals. An example of this type of computer use in the law enforcement context is the MATRIX program which was a computer program designed to mine data from a range of private and public databases. The development of similar programs is being researched by TSA and the Department of Homeland Security (DHS) to identify individuals that pose potential threats. These databases have generated significant commentary from a range of privacy advocacy groups concerning the potential impact they have on personal privacy.[59]. They are also the subject of several governmental reports and analyses with respect to privacy impacts.

E. NATIONAL AND INTERNATIONAL STANDARDS

The proliferation of emerging surveillance technology has led to the development of a range of governance schemes. Most all the legal commentary referenced in this literature review involves proposals for management of emerging surveillance technology. While some of the proposed guidance is contradictory, there is amazing consistency around those central principles articulated in the FIPP. This is true of systems adopted in the United Kingdom, the date protection principles adopted throughout Europe, or the principles offered by groups like the American Bar association or the Constitution Project. The range of possibilities for governing surveillance and the methods for implementing that governance is presented in great detail throughout the literature on this subject.

[59] American Civil Liberties Union, "Data Mining Moves into the States," http://www.aclu.org/FilesFDPs/matrix_20report.pdf (accessed May 9, 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

III. UNDERSTANDING PRIVACY AND SURVEILLANCE

While privacy has been characterized as one of the most important values of human culture, it is not a unitary concept. Understanding what exactly constitutes privacy and its function in democratic society is a first step in determining how and to what extent it should be protected. Both the positive and negative dimensions of privacy must be analyzed.

In juxtaposition to the individual right of privacy is the responsibility and the power of the State to maintain a level of common security and compliance with accepted social rules. Defining what is and is not surveillance is an important fist step. The Panopticon described by Foucault offers the example of complete surveillance where behavior is controlled through observation by an almost omniscient authority. This extreme form of government control demonstrates the negatives of surveillance, but also offers some positive possibilities. Understanding those positives and negatives, especially as they interplay with privacy, can help in the development of guidelines that preserve the positive elements of both.

A. UNDERSTANDING PRIVACY

Arriving at an accepted definition of privacy is, in and of itself, a difficult task. Emanuel Gross notes that "… the vast literature in the field teaches us that it [privacy] is one of those concepts that everyone understands but cannot be defined in an objective and descriptive way that clearly expresses the scope of its application."[60] His construct is that privacy definitions can be placed in three categories: privacy as moral claim or right; privacy as an exercise of control over personal information; and privacy as matter claim or right.[61] However, further exposition of each of these categories seems to lead to similar tenets that underpin the privacy definition. Where the focus is as a claim, control or accessibility, the central premise seems to be on the type of information about the

60 Emanuel Gross, "The Struggle of a Democracy against Terrorism," 31.

61 Ibid.

individual to be disseminated. In short, it is the process of information dissemination, or perhaps more appropriately the restriction of dissemination of information about an individual, that is the key to privacy.

Perhaps one of the better definitions of privacy is the one offered by Westin. While his assessment of privacy is based on a theory of a claim of right, the definition offered seems equally applicable to a control or accessibility based theory. Westin posits

> [p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups in a condition of anonymity or reserve.[62]

Westin acknowledges the individual's desire for privacy competes with a similar compelling desire for social interaction. The appropriate balance between the two competing desires is weighted with the final balance being struck based on personal preference and societal influences.[63]

1. States of Privacy (How It is Achieved)

Westin's definition offers four mechanisms by which individuals achieve privacy: solitude; intimacy; anonymity; and reserve. Examining each of these mechanisms, in turn, provides insight in how surveillance technology intersects with privacy rights. Each of these mechanisms presents differing degrees of challenge for protection against the intrusion of surveillance.

Solitude is perhaps the most perfected degree of privacy. It is the state of being separated from society physically and psychologically. The individual in solitude is unobserved by the group; this is the state where the individual can be "…especially

[62] Westin, *Privacy and Freedom*, 7.

[63] Ibid.

subject to that familiar dialogue with the mind or conscience."[64] It is in this solitude that original thought can occur and the mind can achieve peace. It presupposes an absence of any surveillance.

Intimacy is the action of disseminating information about one's self to a small unit or group. The purpose of intimacy is to reveal highly personal information. Westin describes it as a "corporate seclusion" for purposes of achieving "…a close, relaxed, frank relationship between two or more individuals."[65] Intimacy generally encompasses relations among family, friends, and close work associates. Unlike solitude which presupposes no surveillance, there may be some intersection with the exercise of intimacy.

In contrast to solitude and intimacy, which are exercised *away* from the general public, a state of anonymity is exercised *in* the general public. Anonymity is "…when the person is in public places or performing public acts but still seeks, and finds, the freedom from identification and surveillance."[66] It is the ability of the individual to "…merge into the 'situational landscape.'"[67] This state of privacy is profoundly affected by enhanced surveillance technology. This is so because it is not only can conduct that can be observed and catalogued — the perpetrator can be identified.

The final state of privacy, reserve, like anonymity, is an exercise of privacy in public. The concept of reserve is that of placing "…psychological barriers against unwarranted intrusion…."[68] This occurs by limiting the communication of information about one's self to others. Westin equates this "mental distancing" to "social distancing."[69] Citing the work of Simmel, Westin notes this reservation of information is that deemed necessary by the individual to "…protect the personality." It is the holding

---

64 Westin, *Privacy and Freedom*, 31.

65 Ibid.

66 Ibid.

67 Ibid.

68 Ibid., 32.

69 Ibid.

back of information to preserve a public perception of who the individual truly is.[70] While reserve may be undermined by surveillance, it is not directly affected the way anonymity is affected. Instead it is more directly affected by dissemination of information gained through surveillance.

Having identified the states of privacy and how they may be impacted by surveillance, there is a need to understand why privacy is important. Why it is valued. Perhaps the best way to do that is to examine the functions that privacy serves for both the individual and the society.

2. Functions of Privacy (Why It is Important)

The four functions of privacy identified by Westin provide a good starting point for understanding why privacy is important. Those functions include: personal autonomy; emotional release; self-evaluation; and limited and protected communications.[71] Examining the applications of the states of privacy to these functions, it becomes clear how surveillance can serve to undermine important features of both individual development and support for democratic processes.

Personal autonomy is the ability to control the information about one's self, to maintain one's independent identity. To protect that autonomy, individuals build defenses that provide increasing restriction on access to information. Westin, relying on the work of researchers like R. E. Park, Kurt Lewin, and Ervin Goffman, notes that these restrictions on access form "'zones'" which are like concentric circles emanating out from one's inner personality at the core.[72] As one proceeds from the core, where one's "ultimate secrets" are held and not shared, the next level are those secrets shared with intimates, then secrets shared with friends, and, finally, the circle of information shared with casual acquaintances.[73]

---

[70] Westin, *Privacy and Freedom*, 32.

[71] Ibid.

[72] Ibid., 33.

[73] Ibid.

Piercing those circles that surround the individual's core secrets undermines independence. It leaves the person susceptible to "ridicule and shame" placing them within the control of those who know their secrets.[74] While at first blush it would not seem that public surveillance technologies can impact the core privacy values of individual autonomy, the ability to compile and manipulate massive amounts of data about individuals can give insights into a range of personal information. Technology is able to compile information about websites being visited, places a person goes and even the most fundamental genetic information about an individual's make-up.

Emotional release is the second function of privacy outlined by Westin. This concept is recognition of the fact that there is a balancing between many social roles a person plays and the individual needs to retreat and receive mental relief. Privacy affords the individual the opportunity to let down his or her guard. Emotional release is also seen in the relief from the stimulation of daily life, the ability to vent and express anger over the life problems one confronts and restorative relief from public failures.[75] Even with new enhanced surveillance technologies, it is unlikely that these privacy functions will be affected.

Emotional release also involves management of the body and its functions. This includes privacy for procreation, bodily excretions, dressing and medical treatment. Privacy for these functions has long been engrained in society. However, despite the longstanding protections for this aspect of privacy, the advent of DNA collection and analysis threaten these privacy protections.

A final area of the function of emotional release outlined by Westin is that of protection for non-compliance from social norms. This aspect of emotional release relies substantially on anonymity. Release is predicated on the fact that minor transgressions can occur in public (i.e., speeding, jaywalking, and consensual sexual indiscretions)

---

[74] Westin, *Privacy and Freedom*, 33.

[75] Ibid., 35-6.

without resulting in social sanction.[76] The advent of sophisticated surveillance technology like CCTV can and, in cases like traffic enforcement, is rapidly shrinking the area of public deviance based on anonymity.

Self evaluation is another function served by privacy. Like personal autonomy this function relies on solitude and intimacy. Withdrawn from society, the individual has time to reflect on ideas and original thought. In the company of trusted confidants, the individual can discuss and examine new thoughts and concepts.[77] Like individual autonomy, the exercise of the self evaluation function might be affected by surveillance systems that are calculated to assess individual preferences and areas of interest and inquiry.

The final function of privacy is to support limited and protected conversation. The purpose of this conversation is twofold. First, it serves as a catalyst for evaluation of ideas and thoughts and for receiving advice and counsel. Second, it serves as a mechanism for distancing individuals from others. Depending on the level of intimacy to the individual, information communicated becomes more limited and circumspect. As with other privacy functions, the development of new surveillance technologies has even invaded the search for knowledge and information that occurs across the public space of the internet. Moreover, through tracking and other types of electronic surveillance, the identity of parties engaged in communications can be identified, and under certain circumstances, the content of their conversation invaded.

In addition to importance for the individual, privacy is also important to organizations and society. The individualism achieved through personal autonomy is a key to the development of "… the pursuit of pluralism necessary to create the democratic existence." [78] Westin notes that functions of individual privacy are repeated in organizational conduct. Organizational autonomy derives from individual autonomy. Release from public roles derives from emotional release. Evaluative decision making

---

[76] Westin, *Privacy and Freedom*, 35.

[77] Westin, *Privacy and Freedom*, 37.

[78] Emanuel Gross, "The Struggle of a Democracy against Terrorism," 33.

derives from self evaluation. Protected public communications derive from individual limited and protected communications. The functions of individual privacy buttress the organizational structures that support western democratic systems.[79]

3. Negative Aspects of Privacy (How It Threatens Us)

While most of the scholarship on privacy focuses on its positives, particularly in its contribution to democratic societies, some aspects of privacy can lead to adverse results. Gross notes in his work that "…in the absence of privacy many wrongful, fraudulent and hypocritical acts world wide might not have been committed…."[80] Of particular concern is public anonymity. While perhaps essential to the public non-conformance and civil disobedience and providing some healthy emotional release, anonymity can have a darker side. Those aspects are well explored in the work of Philip Zimbardo.[81]

The non-conformity that is fostered by anonymity has been shown to enhance aggression in individuals and increase their ability to inflict pain on others. Zimbardo catalogues the results of three studies that examine the effects of anonymity on human behavior. The experiments include examination of women administering electric shock, children in Halloween costumes, and masked warriors. In each of these studies, the existence of anonymity affected behavior in a negative fashion. Zimbardo delineates this feature of anonymity as "deindividuation."

In a study of women delivering electric shock, Zimbardo found that when the women were made anonymous, by virtue of wearing a hood and concealing lab coat, they

79 Westin, *Privacy and Freedom*, 42-51.

80 Gross, The Struggle of Democracy against Terrorism," 33.

81 Philip Zimbardo, *The Lucifer Effect: Understanding How Good People Turn Evil* (New York: Random House 2007), 298-306.

would deliver electro shock for a period twice as long as when they were identifiable.[82] He concluded that "[t]he sense of a lack of personal identifiably can also lead to antisocial behavior."[83]

The Halloween costume experiments conducted by Scott Fraser and cited by Zimbardo, further document a relationship between anonymity and anti-social conduct. Those experiments involved studying the effects of costumes and masks on aggressive play among children. Zimbardo notes that "[t]the data [from the Fraser study] are striking testimony to the power of anonymity. Aggression among these young children increased significantly as soon as they put the costume on."[84]

Citing the work of cultural anthropologist R.J. Watson, Zimbardo notes that anonymity as social phenomena can exacerbate destructive tendencies. Watson studied the actions of warriors in societies based on whether or not the warrior' appearance was altered for battle, Zimbardo observes that "…90 percent of the time when victims of battle were killed, tortured or mutilated, it was by warriors who had first changed their appearance and deindividuated themselves."[85]

Zimbardo's conclusions about anonymity's dangers run squarely in opposition to some of Westin's positive conclusions. With respect to anonymity, Zimbardo observes:

> People can become evil when they are enmeshed in situations where the cognitive controls that usually guide their behavior in socially desirable and personally acceptable ways are blocked, suspended or distorted. The suspension of cognitive control has multiple consequences, among them the suspension of: conscience, self-awareness, sense of personal responsibility, obligation, commitment, liability, morality, guilt, shame, fear, and analysis of one's actions in cost-benefit calculations.

---

82 Zimbardo, *The Lucifer Effect,"* 299-300.

83 Ibid., 301.

84 Ibid., 302.

85 Ibid., 304.

> The two general strategies for accomplishing this transformation are: (a) reducing the cues of social accountability of the actor (no one knows who I am or cares to) and (b) reducing concern for self-evaluation by the actor.[86]

In light of the work of social psychologists like Zimbardo, the full application of the states of privacy may not be fully appropriate to the public sphere. That work, at least, should caution us that some aspects of privacy in the public sphere should be appropriately restricted; this brings to the fore the concept of surveillance.

B. UNDERSTANDING SURVEILLANCE

Just as the concept of privacy requires some examination, so too does the concept of surveillance. David Lyon offers a relatively simple definition. "*Surveillance* refers to the monitoring and supervision of populations for specific purposes. "[87] He goes on to note that "[s]urveillance—literally, some people "watching over' others—is as old as social relationships themselves, but the phenomenon has acquired new and distinctive meanings in the modern era."[88]

A more comprehensive definition of surveillance is offered in *A Report on the Surveillance Society*, the work of the Surveillance Studies Network, for the United Kingdom's Information Commissioner.[89] That work provides this definition of surveillance:

> Rather than starting with what intelligence services or police may define as surveillance it is best to begin with a set of activities that have a similar characteristic and work out from there. Where we find purposeful, routine,

---

86 Zimbardo, *The Lucifer Effect,"* 305.

87 David Lyon and Elia Zureik, eds., *Computers, Surveillance and Privacy* (Minneapolis, MN: University of Minnesota Press, 1996) 3.

88 Ibid.

89 David Murakami Wood, ed., *A Report on the Surveillance Society: Full Report,* Report for the Information Commissioner by the Surveillance Studies Network (London, United Kingdom 2006), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed September 25, 2007).

> systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance.[90]

This definition adds important components to understanding surveillance. Perhaps most importantly, it links the concept to identifying individuals. It is not just a generalized overlook of the crowd, although the technology may be used to gather the big picture view. Ultimately, observations must be linked to the individual to be surveillance. Moreover, this definition recognizes that the results of surveillance activity can be (and usually are) manipulated in a variety of ways all linked to the individual.

The Report's definition also requires the observation to be systematic in nature. Unlike the historic concept of surveillance described by Lyons, with people watching over each other, this definition presupposes a more organized and comprehensive examination. The only real controversial component of this definition is the requirement that the surveillance be routine. While such a definition may characterize surveillance in the United Kingdom, it is unclear why occasional surveillance could not occur. Despite this quibble, the Report's definition provides a good starting point for understanding surveillance. It links together the concepts of observation and the compiling and processing of the data generated by observation.

1. Enter the Panopticon

If privacy is the individual's attempt to limit and control the ability of others to discover information about himself or herself, the perfect form of surveillance is the Panopticon. This concept discussed extensively in the work of philosopher Michel Foucault, was originally devised in the eighteenth century by Jeremy Bentham, as a schema for the operation of a prison. Examination of this extreme form of surveillance, that destroys almost all vestiges of privacy, provides insights into the advantages and disadvantages of surveillance.

---

90 Wood, ed., *A Report on the Surveillance Society."*

The Panopticon has two dimensions. The first, and perhaps most well known, is the architectural dimension of the Panopticon. It was a design for a prison cell house that maximized the ability of guards or warders to keep watch over the prison inmates. The design involved the placement of a watchtower, with large windows, in the center of the cell house, encircled by galleries of cells. The interior of the cells were backlit and visible to the guards who would occupy the tower. This would allow the guard to view completely the activity in any cell. While the tower is windowed, allowing the guard to view out into the cells, venetian blinds are placed over the windows, to obscure the view from the cells into the tower. Thus, the inmate cannot tell when, or if, he or she is being observed at any time.[91]

As Foucault describes the effect of Bentham's Panopticon,

> …the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its actions; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relationship …. In view of this Bentham laid down the principle that power should be visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know if he is being looked at any one moment; but he must be sure that he may always be so…. The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen without ever seeing; in the central tower, one sees everything without ever being seen.[92]

The primary feature of the architectural schema of the Panopticon is faceless and constant surveillance or perception of surveillance. It is a shift of power from individual to control by unseen authority. While the design was to control prisoners, Foucault notes that the concept is easily transferred to functions such as education, medical treatment, or

---

91 Foucault, *Discipline and Punish,* 200-01.

92 Ibid., 201-2.

production.[93] The Panopticon is a device for efficient exercise of power from a central source over the individual. It is a mechanism designed to enforce a code of discipline relating to individual conduct.

2. Positive Attributes of the Panopticon

While most of the privacy rights advocates who discuss the Panopticon focus on the negative impacts on privacy, the system is not without positive attributes. The ability to create the perception of observation (even when it may not actually be occurring) makes for an efficient use of power in controlling behavior. Moreover, as Foucault notes, the observational aspects of the Panopticon can also be used to monitor the power of the state. With respect to the open nature of the Panopticon that protects it from being a tool of tyranny, Foucault observes:

> …the arrangement of this machine is such that its enclosed nature does not preclude a permanent presence from the outside: we have seen that anyone may come and exercise in the central tower [of the Panopticon] the functions of surveillance, and that, this being the case, he can gain a clear idea in which the surveillance is being practiced. In fact, any panoptic institution, even if it were as rigorously closed as a penitentiary, may without difficulty be subjected to such irregular and constant inspections, and not only by appointed inspectors but by the public…. There is no risk, therefore, that the increase in power created by the panoptic machine may degenerate into tyranny;…. The Panopticon, subtly arranged so that an observer may observe at a glance, so many different individuals, also enables everyone to come and observe any of the observers.[94]

The transparent nature of the properly operated Panopticon allows for protection against improper exercise of government power. The notion of random inspection is much easier to effectuate in modern surveillance systems where the results of surveillance are digitized and stored.

In light of the assessments by Zimbardo and others about the potential antisocial effects of anonymity, the imposition of panoptic surveillance in public places may serve to reduce antisocial conduct. At the same time, in light of the observations by Foucault,

---

[93] Foucault, *Discipline and Punish,* 206.

[94] Ibid., 207.

the panoptic mechanism itself can help to guard against government overreaching or abuse through monitoring of the government surveillance activities.

3. Specter of the Total Panopticon

While the Panopticon was a matter of architectural design to effect observation, that was not the only feature. The system of observation envisioned by Bentham was only part of the equation. In addition to observation, there was also to be a comprehensive system of documentation. It is this later feature of the Panopticon that may be the most troubling for civil libertarians.

In the context of a penitentiary, the Panopticon "… was also a system of individualizing and permanent documentation."[95] The observations made were documented in reports on each inmate "… making it possible to assess each case, each circumstance, and, consequently, to know what treatment to apply to each prisoner individually."[96] With the advent of digitization technology, that allows for the cataloguing and compiling of massive amounts of data, it is this documentation feature of the Panopticon that can dramatically shift power between the individual and his or her government. The ultimate effect of this compilation of data that allows the subsequent manipulation of the individual is not known. However, the dramatic shift in power between the individual and government needs to be recognized.

C. SUMMARY

Assessing the states of privacy and their functions will be helpful in crafting public policy regarding surveillance. There are certainly areas of privacy that need extensive protection, not only for the sake of the individual, but for society as well. However, there are some areas where privacy, especially in the form of anonymity, may lead to undesirable behaviors that need to be restrained.

---

95 Foucault, *Discipline and Punish,* 250.

96 Ibid.

Just as understanding the nature of privacy is important so too is understanding the nature of surveillance. The extreme example of the Panopticon demonstrates the positives and negatives of extensive surveillance systems. It also points out features like observation of the surveillance mechanisms themselves that can serve to address concerns over civil liberties abuses.

Both the features of privacy and surveillance must be considered in the formulation of policy to manage emerging surveillance technologies. Both have the potential for profound impact on human behaviors. Both have the potential for profound impacts on democratic institutions and individual rights.

IV. CURRENT LEGAL PROTECTIONS FOR PRIVACY

The states of privacy offer a good framework for analysis of the general state of privacy protection in the United States. While some commentators have suggested scant protections, that criticism seems inaccurate. Some of the states of privacy seem to be afforded significant protection. Those protections are perhaps better characterized as uneven and not well suited to guard against intrusion by some aspects of advancing technology.

A. CONSTITUTIONAL PROTECTIONS FOR PRIVACY.

While some commentators contend that privacy rights are relatively unprotected under the U.S. Constitution, an examination of the law suggests otherwise. Initially using Westin's model of four states of privacy, the following conclusions can be drawn about legal protections.

1. Solitude

With regard to the state of solitude, legal protections seem fairly significant. Under the fourth amendment, a person and his or her home and papers are secure from government intrusion except upon probable cause of some criminal act. Protections for the personal privacy state of solitude begin in the home and emanate outward. Those protections, at least with respect to the physical dimensions of the home, have consistently been also held to be relatively inviolate. The privacy of the person outside the home has been afforded protection, but in a more limited sense.

As early as the late 1920s, the U.S. Supreme Court addressed protections for privacy against the use of surveillance technology directed at activity in the home. In *Olmstead v. United States*,[97] the Court addressed the issue of the privacy of telephone communications emanating from a residence. The Court took a trespass-based analysis of the fourth amendment and concluded that it only protected against surveillance that would constitute something in the nature of a trespass to a person's property. Because

97 *Olmstead v. United States*, 277 U.S. 438 (1928).

the action of the government in the *Olmstead* case involved wiretaps to phone lines which were off the subject's property, the Court held there was no search of either an individual's house or person.

In reaching its conclusions, the Court in *Olmstead* rejected the proposition offered in Justice Brandeis' dissent. He argued that the protections of the amendments were much more expansive:

> The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by men.[98]

By the mid-1960s with widespread government use of surveillance technology, particularly to conduct wiretaps, the Court moved away from its trespass-based analysis for extending fourth amendment protections In *Katz* the Court articulated a test for evaluating fourth amendment protections that was not based on trespass analysis. Rather, the determination of whether government's public surveillance violates fourth amendment provisions was focused on whether the individual in question had an expectation of privacy in the area being subject to search and whether society accepted that expectation as reasonable. In *Katz,* the Court found that the FBI's actions in placing a bug on the roof of a public phone booth violated the defendant's fourth amendment rights. The Court noted a reasonable expectation of privacy in the closed phone booth, even when that phone booth was located in a public area. While the *Katz* decision did not involve the issue of solitude in the home, it clearly extends the protections for privacy in the home and beyond, by shifting the analytic focus on protecting privacy expectations not just in the geographic limits of the home.

---

98 *Olmstead,* 277 U.S at 478.

a. Solitude in the Home

The most recent examination of privacy protection against home surveillance in *Kyllo* harmonizes the trespass and expectation of privacy analysis to provide extensive protection for privacy in the home. The *Kyllo* case involved examination of government use of a thermo-imaging surveillance technology to determine whether or not a home was being used to grow marijuana. Government agents, operating from a public street, directed the thermo-imaging device against the exterior walls of Mr. Kyllo's home. Based on the high volume of heat detected, the officers inferred that heat lamps were in use in the home. Based on this information, a warrant was issued, and upon entering the Kyllo home, a marijuana-growing operation was discovered.

In holding that the application of this surveillance technology violated the fourth amendment, the Court in *Kyllo* noted the special protection that the interior of a home enjoys in fourth amendment jurisprudence. The Court observes:

> … in the case of the search of the interior of homes— the prototypical and hence most commonly litigated area of protected privacy— there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology anyinformation regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," [citation omitted], constitutes a search— at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[99]

In reaching its conclusions, the majority relied on a lengthy line of cases supporting the special status of the home. Quoting *Silverman* v. *United States*,[100] the Court observed "'At the very core' of the Fourth Amendment 'stands the right of a man

---

[99] *Kyllo*, 533 U.S. at 34.

[100] *Silverman* v. *United States*, 365 U. S. 505 (1961).

to retreat into his own home and there be free from unreasonable governmental intrusion.'"[101] Careful examination of the case of *United States* v. *Karo*[102] demonstrates the special nature of intrusion in to the home.

In *Karo,* the Court found that the use of a beeper that had been secreted in a container of ether did not violate fourth amendment protections. Government agents had planted the beeper in an attempt to track unauthorized possession of the substance. The Court in *Karo* concluded that the use of a beeper to track the location of the ether within a residence was unlawful. The decision in *Karo* stands in stark contrast to an earlier decision in the case of *Knotts*. In *Knotts*, the Court concluded that the use of surreptitiously planted beepers to track an ether container, as it traveled over public roadways, was completely permissible. The distinguishing feature between the use of the beeper in *Karo,* as opposed to *Knotts,* was the location of the beeper in the home.

The protection of the interior of the home as a sanctuary was conceded by the dissent in *Kyllo* as a well-established principle. The Court, citing the prior decision in *Payton v. New York,*[103] noted that "…searches and seizures *inside a home* [emphasis provided] without a warrant are presumptively unreasonable."[104] However, the dissent argued that the observation of the heat emanating from the exterior walls of the residence constituted nothing more than observation of something that was in plain view of the public.

Just as the case law consistently protects the interior of the home, the exposure of items to public view has long been found to destroy the privacy interest. Both the majority and dissenting opinions note the effect of plain view on the type of protections afforded to things inside the home. Citing cases involving rulings on discoveries made through aerial surveillance and inspection of garbage left for collection

---

101 *Kyllo*, 553 U.S. at 31.

102 *United States* v. *Karo*, 468 U. S. 705 (1984).

103 *Payton v. New York*, 445 U.S. 573 (1980).

104 *Kyllo*, 553 U.S. at 42.

outside the curtilage of the home, the dissent observed "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[105]

Despite the commitment of both the majority and minority opinions in *Kyllo* to the dedicated space on the home's interior as a place of privacy, the majority clearly noted that this space has already decreased with the advent of modern technology. As the majority noted:

> as the cases discussed above [on aerial surveillance] make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. [citation omitted]. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.[106]

Though the majority and dissenting opinions in *Kyllo* both concluded that exposure to public scrutiny outside a home divested the owner of protected privacy interests, the majority sought to place limits on application of technology that would allow observation. Its opinion attempts to create a bright line rule prohibiting government use of surveillance technology directed against homes where that technology is not generally available to the public. The dissenting Justices reasoned that emanations from the house should be addressed under the plain view doctrine. They proposed making a distinction between a technology that penetrated into the home ("through-the-wall" technology) and one that simply measured emanations ("off-the-wall" technology).[107] The majority opinion rejected such a distinction, concluding that either would constitute an unacceptable invasion of protected privacy.

While the *Kyllo* decision advances privacy protections for solitude in the home, the decision is not an absolute one. It contains a caveat that privacy is only protected against surveillance techniques that are not generally available to the public. This leaves the bright line protections uncertain in the face of advancing technology.

---

105 *Kyllo*, 553 U.S. at 42.

106 Id. at 34.

107 Id. at 36.

b. Integrity of the Person

While, initially, the notion of privacy protection was based on laws of real property like trespass and, therefore, limited to places like the residence, the advent of technology compelled an adjustment of those property-based doctrines. Following the logic of the *Katz* decision, the Court confirmed the protections of the person in the case of *Terry v. Ohio.*[108] The decision in *Terry* ensured a degree of personal integrity and solitude for persons in public places.

In *Terry*, the Court addressed the privacy rights of persons in the public sphere. Citing its recent decision in *Katz*, the Court noted:

> This inestimable right of personal security belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. For, as this Court has always recognized, "No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law." *Union Pac. R. Co. v. Botsford*, 141 U.S.250, 251 (1891). We have recently held that "the Fourth Amendment protects people, not places," *Katz v. United States*, 389 U.S. 347, 351 (1967), and wherever an individual may harbor a reasonable "expectation of privacy," id., at 361 (MR. JUSTICE HARLAN, concurring), he is entitled to be free from unreasonable governmental intrusion.[109]

Terry provides protection for solitude of the individual on the street. It allows the individual can come and go unmolested. The protections were given despite growing national concerns over crime.

The protections against physical intrusion of the person or his or her conversations provided by *Terry* and *Katz* under the fourth amendment were supplemented by protections under the fifth amendment concerning compelled self incrimination. In *Miranda v. Arizona*,[110] the Court expanded the fifth amendment right outside the context of court testimony noting that the "…Fifth Amendment privilege is

---

108 *Terry v. Ohio*, 392 U.S. 1 (1968).

109 Id. at 8-9.

110 *Miranda v. Arizona*, 384 U.S. 436 (1966).

available outside of criminal court proceedings…."[111] The Court later observed in *Davis* v. *Mississippi*,[112] "the police have the right to request citizens to answer voluntarily questions concerning unsolved crimes," but "they have no right to compel them to answer."[113]

c. Limits of Solitude in Public Places

The legal protections of the individual to ensure physical integrity and solitude in public places are not without limit as the Court decisions in *Katz* and *Terry* both observed. Legal protection under the fourth amendment limits only unreasonable searches. While the Court in *Kyllo* established a bright line that limited intrusion into the home in almost any case where probable cause was absent, the Court has been less receptive to limiting the use of technology or sensors that do not interfere with accepted expectations of privacy or where a heightened law enforcement interest can be demonstrated.

(1) Sensor Technologies and Limited Expectations of Privacy. Two Supreme Court cases showcase the willingness of the Court to allow application of technology in the public realm. Those cases demonstrate that expectations of privacy can be affected by the nature of the activity in which a person is engaged and the nature of the activity or substances being subjected to sensor analysis. As to the former category, in the *Knotts* case the Court analyzed the expectation of privacy in activity on a public street. Government agents had placed a transmitter in a barrel of chloroform. The barrel was subsequently tracked as it traveled over public roadways. Because the surveillance conducted was limited to conduct which could be publicly observed, the Court concluded there was no expectation of privacy that warranted protection. The insertion of the beeper into the ether occurred before it was transferred to the subject being followed and no use was made of the device to track the barrel once it reached the suspect's property. The barrel was visible in plain view outside the cabin on the property.

---

[111] *Miranda v. Arizona*, 384 U.S. 437 (1966).

[112] *Davis* v. *Mississippi*, 394 U.S. 721, 727 (1969).

[113] Id. at 727, n. 6.

The Court spent much time focusing on the absence of an accepted privacy interest in travel on the public way noting "[A] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[114] The Court also noted the generally more limited expectation of privacy in automobiles. The clear implication of *Knotts* is that the nature of the public conduct (i.e., driving on a public road versus a telephone conversation) influences the extension of protection the law is willing to afford.

A second area of public conduct where privacy expectations are clearly diminished is in the area of possessing or transporting contraband. In *Caballes*, the Court addressed the use of drug sniffing dogs to detect the presence of narcotics. While a driver was stopped for a routine traffic violation by one Illinois State trooper, another trooper with a trained narcotics sniffing dog who happened to be in the area, arrived on the scene. The dog conducted a walk-around the vehicle and alerted to the presence of narcotics.

In addressing this issue the Court in *Caballes* noted:

> Official conduct that does not "compromise any legitimate interest in privacy" is not a search subject to the Fourth Amendment. *Jacobsen*, 466 U.S., at 123. We have held that any interest in possessing contraband cannot be deemed "legitimate," and thus, governmental conduct that only reveals the possession of contraband "compromises no legitimate privacy interest." *Ibid.* This is because the expectation "that certain facts will not come to the attention of the authorities" is not the same as an interest in "privacy that society is prepared to consider reasonable." [citation omitted].[115]

In upholding the use of the evidence secured as a result of the canine sniff, the Court, citing its decision in Place, reiterated the fact that a canine search was *sui generis* "because it 'discloses only the presence or absence of narcotics, a contraband item.'"[116] The Court reaffirmed its previous conclusion in *Place* that

---

114 *Knotts*, 460 U.S. at 281.

115 *Caballes*, 543 U.S. at 408-9.

116 *Caballes*, 543 U.S. at 409.

government conduct of a sensor analysis that disclosed the presence of contraband in a closed container located in the public space did not implicate protected privacy interests.

The approval of the canine "technology" to conduct olfactory sensing of an object to determine the presence of contraband was distinguished from the thermo technology utilized in *Kyllo*. The Court noted that the canine sniff which detected only contraband was significantly less intrusive than the thermo imaging that could be utilized to determine intimate details, like the lady of the house repairing from her bath, a fact that was afforded privacy protection.[117] Thus, what is sometimes characterized as the "binary" nature of the technology itself may well affect conclusions about the ability of whether or not the technology designed only to detect illegal activity could ever unreasonably intrude on privacy interests. The Court's final conclusion in *Caballes* is quite telling in this regard:

> The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car. A dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment.[118]

The dissenting opinions in *Caballes*, particularly the dissent of Justice Ginsburg, express concern over the possibility of expansion of the binary search approach to other contexts. Both speculate as to the ability to use this technology on parked cars, cars sitting at long traffic lights, or even persons walking down the street.[119] Justice Souter raises concerns in his dissent over the efficacy of the *sui generis* canine technology. While the majority opinion assumes the accuracy of highly trained canines, Justice Souter expresses concern over what level of falsely positive identification of contraband would still be acceptable under the majority's analysis for use of the

---

117 *Caballes*, 543 U.S. at 409-10.

118 Id. at 410.

119 Id. at 417, 422.

technology.[120] The questions of expansion and reliability of the search technology and the resultant interference with protected areas of solitude remain unanswered by Supreme Court decision.

(2) Government Interest and the "Special Needs Doctrine." While much of the privacy jurisprudence has centered upon the expectation of privacy on the part of the individual, there is apparent Supreme Court support for the application of surveillance technology that may invade protected privacy interests when there is a showing of special need on the part of the government. In two recent Supreme Court cases, the justices have differentiated between methods for "ordinary crime control" and search or surveillance techniques designed to protect against special threats. The application of this doctrine to protect against terrorist threats like bombings is clear from these decisions.

This "special needs" doctrine was originally articulated to address special circumstances where surveillance was being conducted in public areas to address governmental concerns that were administrative or regulatory in nature. The doctrine articulates circumstances where searches of individuals or spaces occupied by them would be permissible irrespective of individual privacy interests. In *Griffin v. Wisconsin*,[121] the Court extended application of the special needs doctrine to searches of the home of a probationer, pursuant to a Wisconsin statutory penal scheme:

> we have permitted exceptions when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T. L. O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in judgment). Thus, we have held that government employers and supervisors may conduct warrantless, work-related searches of employees' desks and offices without probable cause, [citation omitted], and that school officials may conduct warrantless searches of some student property, also without probable cause, [citation omitted]. We have also held, for similar reasons, that in certain circumstances government investigators conducting searches pursuant to a regulatory scheme need not adhere to the usual warrant or probable-cause

120 *Caballes*, 543 U.S. at 411-31.

121 *Griffin v. Wisconsin*, 483 U.S. 868 (1987).

> requirements as long as their searches meet "reasonable legislative or administrative standards." [citations omitted][122]

In *City of Indianapolis v. Edmonds,*[123]the Court specifically addressed the subject of terror prevention while addressing the application of the "special needs" doctrine to the use of drug inspection checkpoints. The City of Indianapolis had created a series of traffic checkpoints to utilize canines to check vehicles for the presence of narcotics. The City reasoned the checkpoints were sufficiently similar to and no more intrusive than the sobriety checkpoints that had already been approved by the Supreme Court in *Sitz v. Michigan.*[124] In rejecting the application of the "special needs' doctrine to these checkpoints, the Court noted that the City's purpose was the pursuit of ordinary crime control, relating to narcotics, and differentiated the drug checkpoint from the sobriety checkpoints in *Sitz* that were designed to effectuate a regulatory scheme of roadway safety. Significantly however, the Court in *Edmonds* went on to note:

> Of course, there are circumstances that may justify a law enforcement checkpoint where the primary purpose would otherwise, but for some emergency, relate to ordinary crime control. For example, as the Court of Appeals noted, the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route. [citation omitted]. The exigencies created by these scenarios are far removed from the circumstances under which authorities might simply stop cars as a matter of course to see if there just happens to be a felon leaving the jurisdiction. While we do not limit the purposes that may justify a checkpoint program to any rigid set of categories, we decline to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control.[125]

---

122 *Griffin*, 483 U.S. at 873.

123 *City of Indianapolis v. Edmonds*, 531 U.S. 32 (1990).

124 *Michigan v. Sitz*, 496 U.S. 444 (1990).

125 *Edmonds*, 531 U.S. at 44.

This position articulated in *Edmonds* was vigorously affirmed by the dissent in *Caballes*. There Justice Ginsburg drew a significant distinction between narcotics sniffing dogs and those used to search for explosives.[126]

The *dicta* in the Supreme Court cases addressing application of the "special needs" doctrine suggest that where a surveillance program can be closely linked to anti-terror strategies, there may be some room for application of surveillance techniques that affect otherwise protected privacy interests. Rather than looking at the individual's expectation of privacy, in cases of surveillance pursuant to an anti-terror program, the existence of an appropriate regulatory or statutory scheme may result in permissible surveillance programs that impair some privacy interests in public spaces.

2. Intimacy

Just as there is protection for solitude through the sanctity of the home, protection is also extended to intimacy. Those protections find root both inside and outside the protections of the fourth amendment. For example, in *Kyllo*, the majority opinion discusses the fact that protections for the home are designed to protect intimacy. The Court notes "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes [emphasis provided]."[127] The dissenting justices were similarly concerned with invasive technology that exposed intimate details, but they concluded the "off-the-wall" technology of thermo-imaging revealed no such intimate details.[128]

The protections of intimate conduct exceed the fourth amendment concept of privacy protection. Beginning in the late 1960s, the U.S. Supreme Court began to craft a body of law to protect the rights of citizens in their most intimate relationships. These cases touched on the most intimate of human relationships: procreation; marriage and childbirth. The first of the cases, *Griswold v. Connecticut*,[129] involved state regulation of

---

126 *Caballes*, 543 U.S. at 423-24.

127 *Kyllo*, 553 U.S. at 37.

128 Id. at 50-51.

129 *Griswold v. Connecticut*, 381 U.S. 479 (1965).

information regarding birth control to marital couples. In *Griswold*, there is an articulation by Justice Douglas of the "zones of privacy" that are protected by the provisions of the Bill of Rights.

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. [citation omitted] Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." [130]

Applying this concept of a penumbra, subsequent Court decisions have suggested that the protections of the fourteenth amendment seem to apply to the aspects of intimate association. As the Supreme Court noted in the decision in *Roe v. Wade*,[131]

> The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as *Union Pacific R. Co. v. Botsford*, 141 U.S. 250, 251 (1891), the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment, *Stanley v. Georgia*, 394 U.S. 557, 564 (1969); in the Fourth and Fifth Amendments, *Terry v. Ohio*, 392 U.S. 1, 8-9 (1968), *Katz v. United States*, 389 U.S. 347, 350 (1967), *Boyd v. United States*, 116 U.S. 616 (1886), see Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); in the penumbras of the Bill of Rights, *Griswold v. Connecticut*, 381 U.S. at 484-485; in the Ninth Amendment, id. at 486 (Goldberg, J., concurring); or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment, see *Meyer v. Nebraska*, 262 U.S. 390, 399 (1923). These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty," *Palko v. Connecticut*, 302 U.S. 319, 325 (1937), are

---

130 *Griswold v. Connecticut*, 381 U.S. 479 (1965) at 514-15.

131 *Roe v. Wade*, 410 U.S. 113 (1973).

> included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage, *Loving v. Virginia*, 388 U.S. 1, 12 (1967); procreation, *Skinner v. Oklahoma*, 316 U.S. 535, 541-542 (1942); contraception, *Eisenstadt v. Baird*, 405 U.S. at 453-454; id. at 460, 463-465 [p153] (WHITE, J., concurring in result); family relationships, *Prince v. Massachusetts*, 321 U.S. 158, 166 (1944); and childrearing and education, *Pierce v. Society of Sisters*, 268 U.S. 510, 535 (1925), *Meyer v. Nebraska*, supra.[132]

Protections for intimate relationships are clearly provided by the Constitution, whether under the fourteenth or ninth amendment. Moreover, those protections extend to the exercise of the underlying relationships that form the right, not just the location, where they are exercised (e.g., the home). While the Supreme Court in its 1984 decision in *City of Dallas v. Stanglin*[133] rejected a challenge to dance hall restrictions that was based in part on claims of protected intimate social association, it noted the vitality of those protections. Citing a prior decision in *Roberts v. United States Jaycees*,[134], it observed '"…the Court has concluded that choices to enter into and maintain certain intimate human relationships must be secured against undue intrusion by the State because of the role such relationships have played in safeguarding the individual freedom that is central to our constitutional scheme.'"[135]

The protections for intimacy seem to be quite strong and comprehensive. Interestingly, in the concurring opinion of Justice Stevens in *Stanglin*, we find them even extended to development of friendship and social relationships at a dance hall (although he felt that Dallas' restrictions did not sufficiently impair those rights).[136] Moreover, those associational protections extend beyond familial types of relationships.

Associational protections are also extended to political, religious and cultural matters. While not always intimate in a family sense, these protections allow for the establishment of associational relationships for a range of activities covered under the

---

132 *Roe*, 410 U.S. at 152-53.

133 *City of Dallas v. Stanglin*, 490 U.S. 19 (1989).

134 *Roberts v. United States Jaycees*, 468 U.S. 609 (1984).

135 *Stanglin*, 490 U.S. at 24.

136 *Stanglin*, 490 U.S. at 28-29.

first amendment. In *Roberts*, the Court discussed the importance of protecting close relationships that foster individual growth and development.

> The Court has long recognized that, because the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State. [citation omitted]. Without precisely identifying every consideration that may underlie this type of constitutional protection, we have noted that certain kinds of personal bonds have played a critical role in the culture and traditions of the Nation by cultivating and transmitting shared ideals and beliefs; they thereby foster diversity and act as critical buffers between the individual and the power of the State. [citations omitted].[137]

The Court in *Roberts* went on to recognize a continuum in relationships that run from the most intimate family relationships to affiliations in large organizations that are much more attenuated. These relationships are important to individual thought and development. While the Court noted that the more attenuated relationships do not require associational protection under the rubric of the first amendment, there are close associational relationships outside intimate family relationships that are afforded such protections.

While intimate relationships and associations related to the exercise of first amendment rights are not afforded absolute protections, they must be considered and effectively addressed in the execution of surveillance. With respect to any surveillance technology that might adversely impair or interfere with those protected relationships, there is a strong likelihood that a court challenge to that technique or practice would be successful.

---

[137] *Roberts*, 468 U.S. at 619-20.

3. Anonymity

Perhaps the state of privacy that is offered the least protection under the law is that of public anonymity. While the state of solitude enjoys extensive protection under the fourth amendment, and intimacy is protected under a range of provisions in the Bill of Rights, anonymity finds little protection under the Constitution. Protections are largely limited to the first amendment. Moreover, a range of statutory provisions that limit or constrain anonymity in public have been found to pass constitutional muster. Overall, a fair characterization of the law with respect to anonymity is that it generally ranges from non-supportive to hostile.

The only area in which anonymity has been afforded constitutional protection has been in those cases where the Court has found it a necessary prerequisite to effective political activity. In *NAACP v. Alabama*,[138] the Court addressed the ability of members of political organizations to maintain their anonymity. In *NAACP v. Alabama*, the Court addressed the compelled disclosure of membership information for the National Association of Colored People (NAACP).

In overruling a decision of the Alabama Supreme Court and denying access to the NAACP membership records, the Court observed:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. …Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs. [citation omitted].[139]

---

138 *NAACP v. Alabama*, 357 U.S. 449 (1957).

139 Ibid. at 462.

So long as the surveillance techniques employed were not designed or applied in a way that served to chill the exercise of associational rights by techniques like the identification and cataloguing of group members, it is likely those surveillance techniques would be permitted.

Outside the concept of protecting anonymity for the purpose of effectuating associational rights protected by the first amendment, anonymity in the public sphere receives little protection. In fact, in a recent Supreme Court decision in *Hiibel v. Sixth Judicial Circuit Court, Humboldt County*,[140] the ability of law enforcement to compel identifying information was addressed. The *Hiibel* case involved a challenge to a Nevada "stop and identify" statute. When police stop an individual based on the reasonable suspicion he or she is involved in criminal activity, the statute provided that the individual can be compelled to provide identifying information.

The Court rejected Mr. Hiibel's argument that compelling him to provide his name constituted a violation of rights secured by the fourth and fifth amendments. The Court observed that there was a long history of cases that indicated police inquiries into identity were permissible under the fourth amendment. The question that remained unanswered prior to the *Hiibel* case was whether or not penalties could be imposed for maintaining anonymity in the face of police inquiry. In upholding the Nevada statute, the Court concluded:

The principles of Terry permit a State to require a suspect to disclose his name in the course of a Terry stop. The reasonableness of a seizure under the Fourth Amendment is determined "by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests." *Delaware v. Prouse*, 440 U.S. 648,654 (1979). The Nevada statute satisfies that standard. The request for identity has an immediate relation to the purpose, rationale, and practical demands of a Terry stop. The threat of criminal sanction helps ensure that the request for identity does not become a legal nullity. On the other hand, the Nevada statute does not alter the nature of the stop itself: it does not change its duration, [citation omitted], or its location, [citation omitted].

[140] *Hiibel v. Sixth Judicial Circuit Court, Humboldt County*, 542 U.S. 177 (2004).

A state law requiring a suspect to disclose his name in the course of a valid Terry stop is consistent with Fourth Amendment prohibitions against unreasonable searches and seizures.

The Supreme Court found similarly unpersuasive Hiibel's argument that compelled disclosure of identity constituted a Fifth Amendment violation.

> In this case petitioner's refusal to disclose his name was not based on any articulated real and appreciable fear that his name would be used to incriminate him, or that it "would furnish a link in the chain of evidence needed to prosecute" him. *Hoffman v. United States*, 341 U.S. 479, 486 (1951). As best we can tell, petitioner refused to identify himself only because he thought his name was none of the officer's business. … While we recognize petitioner's strong belief that he should not have to disclose his identity, the Fifth Amendment does not override the Nevada Legislature's judgment to the contrary absent a reasonable belief that the disclosure would tend to incriminate him.

The Court in *Hiibel* noted that some seventeen states have similar statutes requiring persons to identify themselves in response to police inquires. The Court also recounted extensive legal history supporting the authority of government to seek identifying information from persons in public. While compelling a person's identity under *Hiibel* requires the law enforcement officer to have reasonable suspicion for stopping someone in the first place, it clearly eliminates any argument that anonymity in public is constitutionally protected.

4. Reserve

The final state of privacy, reserve, finds sparse protection under federal law. Two U.S. Supreme Court decisions have addressed the issue of privacy in government data compilations. Both have provided insight into concerns over the importance of protections for this aspect of privacy, especially in the light of government controlled computerized data compilations. Both decisions were decided on more narrow grounds that avoided directly addressing the issue of constitutional protection of privacy.

In *Whelan v. Roe*,[141] the Supreme Court reviewed a challenge to a New York statute that created a database of all prescriptions issued for certain controlled substances. The challenge was based on claims that the creation of such a database raised a specter of potentially embarrassing private information being made public and that the existence of this possibility might inhibit persons from seeking needed medication. In a unanimous opinion, the Court found that state interest in controlling access to dangerous drugs and stringent statutory and regulatory safeguards over collected data, outweighed any possible constitutional privacy protection that might be implicated in the data collection.

In concluding its opinion, the Court observed:

> A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.[footnote omitted] The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure.[142]

While the Court notes the potential threat to privacy inherent in the data collection to essential governmental operations it avoided directly addressing the issue. Instead it found adequate the protections imposed under state law. The clear language of the Court's opinion leaves unresolved the question of privacy under the Constitution.

The absence of clear guidance in the opinion is compounded by a debate over interpreting the opinion. In the concurring opinions, Justices Brennan and Stewart highlight opposing opinions on the question of whether the data compilations implicate

---

141 *Whelan v. Roe*, 429 U.S. 589 (1977).

142 Ibid. at 605-06.

protected privacy interests. In Justice Brennan's concurrence, he observes that "[t]he Court recognizes that an individual's 'interest in avoiding disclosure of personal matters' is an aspect of the right of privacy, [citation omitted], but holds that in this case, any such interest has not been seriously enough invaded by the State to require a showing that its program was indispensable to the State's effort to control drug abuse."[143]

Justice Stewart offers an opinion that no constitutional protection for privacy is available in this case. Justice Stewart observed:

> In *Katz v. United States*, 389 U.S. 347, the Court made clear that although the Constitution affords protection against certain kinds of government intrusions into personal and private matters,[footnote *omitted*] there is no "general constitutional `right to privacy.' . . . [T]he protection of a person's general right to privacy - his right to be let alone by other people - is, like the protection of his property and of his very life, left largely to the law of the individual States." Id., at 350-351 (footnote omitted).[144]

A second Supreme Court decision in *Department of Justice v. Reporters Committee for Freedom of the Press*,[145] also addressed extensively the subject of privacy without providing a precedential ruling. In *Reporters Committee*, the Court reviewed decisions concerning a request under the Federal Freedom of Information Act (FOIA) for criminal history data. A network news station was seeking the rap sheet of a government contractor. The rap sheet contained information generated from disparate government records of arrests of an individual over time.

The Court in *Reporters Committee*, characterized the matter in dispute as follows:

> …the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county

143 *Whelan*, 429 U.S. at 606.

144 Ibid. at 607.

145 *Dept. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749 (1989).

> archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.[146]

With regard to the question posed at the beginning of its opinion regarding extension of privacy to information that once had been public, the Court reached the following conclusions:

> In sum, the fact that "an event is not wholly `private' does not mean that an individual has no interests in limiting disclosure or dissemination of the information." Rehnquist, Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Nelson Timothy Stephens Lectures, University of Kansas Law School, pt. 1, p. 13 (Sept. 26-27, 1974). The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded.[147]

The Court noted that a range of legal sources supported such a position.

> In addition to the common-law and dictionary understandings, the basic difference between scattered bits of criminal history and a federal compilation, federal statutory provisions, and state policies, our cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.[148]

While there is little precedential value outside the state and federal statutes directly considered in both the decisions in *Whelan v. Roe* and *Reporters Committee*, these decisions demonstrate concern over reserve as a protected state of privacy. The absence of a precedential decision that links reserve to a constitutionally protected liberty interest, however, exposes this state of privacy to varied and possibly limited enforcement.

---

[146] *Reporters Committee*, 489 U.S. at 764.

[147] Ibid. at 770-71.

[148] Ibid. at 767.

While the opinion in *Reporters Committee* notes the interpretation of the provisions of the federal FOIA statute is not controlled by state law, the converse is also true. Federal FOIA only governs the production of documents or compilations in the control of the federal government. The protection extended to data compilations under state FOIA statutes are governed under state law. Thus, the net result of failure to develop a body of federal constitutional law directly addressing reserve means that protection of surveillance data drawn from public conduct will vary from state to state.

5. Summary

The legal protections for the states of privacy vary substantially. The states of solitude and intimacy are afforded significant protections under the Constitution. However, there remains considerable room for the conduct of surveillance in public space consistent with protection of these states of privacy. The state of anonymity has limited protection for associational rights, but generally seems disfavored with regard to the extension of legal protections. The state of reserve seems to be a matter of great interest and concern to the Supreme Court, but as of yet, it has not been extended constitutional protection. In the absence of such protections for reserve, there is likely to be varied protection of this privacy interest from jurisdiction to jurisdiction.

B. PROTECTIONS OF PRIVACY FROM OTHER LEGAL SOURCES

In addition to protections under the U.S. Constitution, protections for privacy are found in other legal sources. The federal Constitution provides only a common baseline for the protection of individual rights. Federal legislative enactments, state law protections, and federal and state remedial statutes can provide a private right of action for an individual whose protected rights are violated.

1. Federal Legislative Protections

Legislative enactments at the federal level have been introduced to provide a common standard for privacy protections particularly in field of electronic communications. In the wake of the 1967 U.S. Supreme decision in *Berger v. New*

York,[149] the U.S. Congress promulgated a statute to govern access to telephone communications. In *Berger*, the Court found that the provisions of a New York law permitting wiretaps violated fourth amendment protections. The Court concluded that the sweep of the law was too broad and procedural protections inadequate to protect privacy rights. Informed and controlled by the Supreme Court decision in *Berger*, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) was created to regulate wiretap activity by law enforcement.[150]

Wayne Lafave, in his treatise on arrest search and seizure, discusses the history of Title III noting how its provisions were generally crafted to address the fourth amendment concerns articulated in *Berger*.[151] Title III controls the warrant process for electronic surveillance of communications. This process allows law enforcement officials to make an application based on probable cause of certain criminal activity for a authorization to conduct wiretaps. These applications must be presented to a judicial officer and must outline with particularity matters like: the facts supporting probable cause for belief the suspect is involved in criminal activity; reason why other investigative procedures are unsuitable; and the basis for conclusion that the places being subject to intercept will likely be involved in the criminal conduct. The order authorizing the intercept must specify the person or persons whose communications can be intercepted, the type of communications to be intercepted and the criminal activity to which it relates. The orders for interception cannot be unlimited in duration. They are limited to 30 days with the possibility of extensions being granted upon subsequent application. Within a reasonable time after the surveillance has concluded, notice must be provided to the subject. This notice must include an inventory of the activity. Where information is gathered in violation of the provisions of Title III, the statute requires it be excluded from use as evidence in a criminal proceeding.[152]

---

149 *Berger v. New York*, 388 U.S. 41 (1967).

150 Title III, 18 U.S.C. §§ 2510-20.

151 Wayne R. LaFave, *Search and Seizure,* Volume 2, Chapter 4, Section 4.2.

152 Ibid.

One of the critical features of Title III is the concept of "minimization." Minimization is the concept of limiting intercepts only to specific conversations relevant to the criminal investigation. "'Minimization' was deemed essential to satisfy the fourth amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime."[153]

Title III protections were subsequently expanded through the Electronic Communications Privacy Act of 1986 (ECPA)[154] to address forms of electronic communications other than voice. Despite the enhancements in protections for electronic communications, some commentators like Dempsey have indicated that enhanced digitization of communication and the growth in dependence on those communications should engender an increased review of Title III.[155] For example, Dempsey argues that refinement in search capabilities of internet tools may allow for greater protections in the area of minimization.

> Technology, however, may offer a solution, producing more effective minimization than is available in the context of voice communications. Whether law enforcement accesses e-mail from the telephone company (or access provider) while in transmission, or from an e-mail service provider while it is in storage incident to transmission, it may be relatively easy for the service provider to perform the minimization. The service provider can use screens or filters to select from the e-mail messages to or from parties identified in the order only those containing certain key words or phrases that would be identical to those used by monitors in the voice context. [citation omitted].[156]

The standards of regulation for use of wiretap information have been already been applied by some courts to the use of covert video surveillance in private places. In *United States v. Torres*,[157] the U.S. Court of Appeals for the Seventh Circuit applied the

---

153 James X. Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany L. J. of Science and Technology* 8 (1997): 72.

154 EPCA, 18 U.S.C. §§ 2701-2710.

155 James X. Dempsey, "Communications Privacy in the Digital Age," 65.

156 Ibid., 87.

157 *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984).

model of regulation from Title III to the use of video surveillance. There the court noted that where the terms of video surveillance complied with the same requirements for interception of oral communications under Title III the requirements of the fourth amendment were satisfied.[158] The commentator Ric Simmons notes that subsequent to the Seventh Circuit's adoption of this position it has been adopted by U. S. Courts of Appeal in six other circuits.[159] While application of Title III protections has only been applied to covert video surveillance in private areas where fourth amendment rights are clearly present, this structure can also be instructive for regulation of public surveillance. Where techniques are applied that may be considered to be extremely intrusive, like prolonged tracking of individuals through extended areas of private space, the prophylactic use of Title III standards may be advisable.

2. State Law Protections

In addition to the protections afforded by federal law, states are free to expand those rights and provide additional protections for privacy. In fact, there has been a growing trend in recent years for states to provide additional protections for civil liberties under the provisions of their own state constitutions. While for many years most state constitutions were thought to provide no greater protections for individual rights than those provided by federal law, that paradigm is breaking down. States are diverging from what commentators refer to as the "lockstep" approach.[160] The lockstep approach is the concept that provisions in state constitutions that mirror provisions in the federal Constitution are interpreted by state courts in an identical fashion to the federal provisions.

An examination of the case law demonstrating departure with the lockstep approach is found in the Oregon Supreme Court's review of the use of tracking devices. That opinion demonstrates the possibility of enhanced state protections for privacy rights.

---

158 *Torres*, 751 F.2d. at 884.

159 Ric Simmons, "The Powers and Pitfalls of Technology…," 711, 726 n.50.

160 Robert F. Williams, "State Courts Adopting Federal Constitutional Doctrine," 1499; Helen W. Gunnarsson, "The Limited Lockstep Doctrine," 340.

In the *Knotts* case the Court affirmed the use of electronic tracking devices in tracking vehicles in public areas. In contrast to the U.S. Supreme Court's conclusion that vehicle tracking beepers do not implicate any legally protected privacy interest was the Oregon State Supreme Court decision in *State v. Campbell*. [161] In that case the court concluded that the provisions of the Oregon Constitution, though similar to the provisions of the fourth amendment to the federal Constitution, were more expansive in protecting privacy rights of individuals. Under Oregon law, a warrant is required for law enforcement investigation involving the placement of tracking devices.

The trend of state court divergence from federal precedent with respect to public surveillance is also seen in a 2003 decision of the Washington Supreme Court in *State v. Jackson*.[162] In that case, the Washington Court addressed the use of GPS devices to track vehicles. The court concluded that Washington State Constitutional protections for privacy would require a warrant before law enforcement could use GPS locators to track suspect vehicles on public streets.

As technology develops it is likely more states may diverge from the federal baseline and provide enhanced privacy protection. These enhanced standards will have to be accommodated in the collection and use of any unified data collection and analysis systems. In addressing governance issues, policymakers need to be mindful of the fact that federal law is not necessarily dispositive of the issue. States like Oregon and Washington diverging from the lockstep doctrine may assert additional protections. A developing body of state law on the subject will certainly influence not only how surveillance systems will function in any given jurisdiction, but also how the information gathered can be transmitted or exchanged between governmental users.

In addition to the existence of state constitutional provisions that can affect privacy considerations, states are free to promulgate a range of penal and civil statutes to address violations of individual privacy rights. For example, Illinois recently enacted criminal penalties for persons using CCTV surveillance technology to monitor

---

161 *Oregon v. Campbell*, 759 P.2d 1040 (Or. 1988).

162 *State v. Jackson*, 76 P.2d 217 (Wash. 2003) (*en banc*).

individuals in areas of public accommodation like tanning salons, hotel bedrooms, restrooms and similar areas.[163] As of December 2007, 19 other states had similar legislation, with four other states in the process of promulgating such legislation.[164] While this legislation applies to the use of surveillance technology in areas of public accommodation that are generally considered as private, nothing precludes more expansive state legislation to limit surveillance in other public areas. In fact, expanded state legislation to enhance protection for privacy is the very approach advocated by privacy advocacy groups like the Constitution Project with its model legislation.

In addition to constitutional or legislative enactments directly addressing privacy, states have laws to address transparency in government that will have a range of consequences on privacy protection, some unintended, for operators of CCTV and other surveillance systems. Most all states have statutes addressing retention and access to information collected and maintained by governmental agencies. In Illinois, for example, those statutes are the Local Records Retention Act[165] and the Freedom of information Act.[166] These types of statutes are typical for most states and directly impact on the data gathered by surveillance systems.

Under the provisions of state document retention statutes like the one in Illinois copies of digital recordings made by a CCTV network must be maintained in accordance with retention schedules approved by the local records commission. The length of storage time imposed directly impacts on privacy issues and affects the capacity of the recording system. Most privacy advocates argue for short retention periods. While law enforcement may want longer periods of retention, there is a significant financial cost associated with such a practice. The longer the retention requirement, the larger the

---

163 Public Act 093-0851, codified at 720 ILCS 5-26/4 (2008), http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=093-0851 (accessed March 2, 2008).

164 Stacy St. Clair, "Keeping up with Toms Who Peep Via High Tech," *Chicago Tribune*, December 26, 2007, http://pqasb.pqarchiver.com/chicagotribune/access/1403629641.html?FMT=FT&dids=1403629641:1403629641&FMTS=ABS:FT&type=current&date=Dec+26%2C+2007&author=Stacy+St+Clair&pub=Chicago+Tribune&desc=Keeping+up+with+Toms+who+peep+via+high+tech&pf=1 (accessed March 4, 2008).

165 50 ILCS 205/1 *et seq.*

166 5 ILCS 140 *et seq.*

digital/video storage capacity is required in the system. That capacity impacts directly on price (i.e., the number of servers required to store the information). Ultimately, these legal requirements will place a capacity limit on the operating system.

While retention statutes place a constraint on the intake side of the ledger, Freedom of Information Act (FOIA) statutes, like the one in Illinois, place requirements on information outflow. Operation of digital surveillance systems, like CCTV, will generate substantial amounts of information on public activity in which there is no significant government interest. However, this surveillance information will doubtless be sought by a variety of individuals or organizations for a range of reasons. Without provisions explicitly exempting data collected from digitized public surveillance systems this data may be required to be disseminated in response to public requests. Such third party dissemination raises significant privacy concerns. In fact, privacy advocacy groups generally recommend the statutory protection against dissemination under FOIA and other statutes.

Response to public information requests raises issues that not only implicate privacy concerns, but also practical operational concerns for policymakers regarding responding to FOIA requests. Personnel resources required for response to requests, as well as liability issues raised for improper dissemination, are major areas for concern. Any system design must address the administrative costs and privacy implications of public dissemination of information.

3. Private Rights of Actions

The protection of privacy is a private right of action recognized by the common law adopted in the tort laws of most states. The common law has provided individuals with a private right of action for damages and injunctive relief in response to actions that impinged upon protected privacy interests. The common law provisions protecting privacy are outlined in the *Second Restatement of Torts*.[167] They include activities such as: intrusion on seclusion; appropriation of another name or likeness; publicity given to

[167] The Restatement (Second) of Torts (New York: West Publishing Company, 2006), § 652, http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (accessed March 4, 2008).

the private life of another; and publicity placing someone in a false light.[168] These protections for privacy are applicable in over half the states.[169]

This common law approach to privacy protection has substantial limitations. It has almost universally been interpreted by courts as being largely inapplicable to conduct observed or recorded in public.[170] Moreover, immunity statutes often make it difficult to bring actions against governmental entities which would be the operators of large surveillance systems. The remedies provided under existing tort law are largely limited to private parties engaged in conduct on private property.

A more robust private right of action is provided under the provisions of federal law. As noted above, there are extensive privacy protections provided under the provisions of the U. S. Constitution. Governmental action in violation of those constitutional provisions is actionable under provisions of 42 U.S.C. § 1983. That statute provides individuals whose constitutional rights have been violated with a remedy for money damages and injunctive relief. Individuals who prevail in asserting rights under 42 U.S.C. § 1983 are entitled to attorney's fees under the provisions of 42 U.S.C. § 1988. These statutes provide individuals with powerful tools to redress the failure of government to respect constitutionally protected privacy rights.[171]

---

168 The Restatement (Second) of Torts.

169 Note, "In the Face of Danger: Facial Recognition and the Limits of Privacy Law," 120 *Harvard L. Rev.* (2007): 1871, 1876.

170 Ibid., 1877.

171 The U.S. Supreme Court has concluded similar remedies are also available where the violation of constitutionally protected rights occurs at the hands of federal agents. *Bivens v. Six Unknown Federal Narcotics Agents*, 403 U.S. 388 (1971).

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPACTS OF MODERN SURVEILLANCE TECHNOLOGIES ON PRIVACY

The development of surveillance technology has occurred in two significant areas. First, the ability to collect data through surveillance has been significantly enhanced through developments in technology. Second, the ability to store, categorize and analyze that data has also been revolutionized. Together technological advances in both these areas pose significant implications for privacy protection. While current legal authority provides some constraints on surveillance, data collection and manipulation, the technological advances have in some cases outpaced controls or exploited gaps in those protections. In assessing those technologies, focus will first be placed on developments in the area of data collection; then it will turn to surveillance data manipulation and analysis.

A. DEVELOPMENTS IN SURVEILLANCE DATA COLLECTION

As digital technology matures and computer capacity continues to increase, society is confronted with an increasingly sophisticated array of surveillance tools and techniques to gather and compile information on individuals.[172] A range of new technologies implicate privacy concerns. Commentators analyzing the technologies have used a variety of formats to assess those technologies. Those approaches have centered on intrusiveness of the technique,[173] expectation of privacy in the area of examination[174] and even analysis of individual personal privacy expectations and measures taken to protect privacy.[175]

This analysis will focus on developing technologies from the perspective of public safety professionals operating in public space. The focus is not on the impact of

---

[172] Posner, *Catastrophe*, 88-9

[173] Simmons, "The Powers and Pitfalls of Technology"; Patrick J. McMahon, "Counterterrorism Technology and Privacy."

[174] Taslitz, "Technology, Privacy and Human Emotions."

[175] Tien, "Doors, Envelopes, and Encryption."

the technology, but rather, the purpose for which it can be utilized in supporting a range of homeland security strategies. Using this approach there are essentially three areas of surveillance for purposes of analysis: detection of dangerous items, substances, or persons, based on physical characteristics; observation or monitoring of public areas; and surveillance that tracks or monitors the activity of suspect persons.

Certain items of technology, CCTV for example, can be utilized across the full range of surveillance purposes. Examining these technologies and the way in which legal and ethical guidelines have progressed to address privacy concerns can be helpful to developing a comprehensive set of guidelines that balance public safety concerns with privacy considerations.

1. Detection of Dangerous Items or Persons

Detecting the presence of suspect items is a function that occurs everyday in a range of public venues across the country. Use of magnetometers and x-ray technology has long been accepted at public airports. The use of this technology has been expanded to areas such as public places of amusement and public and private schools as public officials look to secure those areas from dangerous items like guns. These systems are often augmented by CCTV technology that allows control room personnel to visually identify suspect items and the location of the item.

Detecting the presence of suspect persons, until recently, has involved much more primitive forms of technology. Use of visual technology has largely been confined to circulating to law enforcement or posting in public places the photographs or artists' renditions of wanted persons. Recent development in CCTV technology may someday allow for identification based on physical characteristics.

Detection technology can be divided into two categories. The first category includes those technologies that can be programmed to only alert the surveillance operator of the existence of contraband items. This sort technology is sometimes referred to as binary. An example of it is the canine sniff. A second kind of detection technology is the technology that exposes a range of concealed items. This technology allows for

identification of contraband items only through additional processes like physical search or application of more refined visual analysis tools. These technologies include the magnetometer, x-ray technology, chemical analysis and explosive detection technology and the newly developed millimeter wave technologies.

a. Binary Technology

Much of the "binary search" technology[176] revolves around a form of olfactory sensing. The predominant system used for that sensing has been canines used to sniff for narcotics and explosives. However, while canines are still used extensively for this function,[177] there is now a shift to mechanical sensors. Post 9-11 saw a proliferation of explosive trace detection technologies at airports. Those technologies initially included explosive trace detection (ETD) for checked and carry-on luggage of all passengers.[178] ETD systems have been augmented with scanners for liquid explosives,[179] document scanners,[180] and trace detection portals[181] to be used to check passengers for trace evidence of contact with explosives.

While special rules have been applied with regard to application of search technologies at places like airports,[182] the growth of these binary surveillance technologies may well have applications outside of the airport context. In fact, the

---

176 Simmons, "The Two Unanswered Questions."

177 U. S. Department of Homeland Security, Transportation Security Administration, "Mitigating High Consequence Risk," *Mass Transit, Transportation Security Administration Official Website,* http://www.tsa.gov/what_we_do/tsnm/mass_transit/risks.shtm (accessed December 3, 2007).

178 U. S. Department of Homeland Security, Transportation Security Administration, "Explosives Trace Detection," *Innovation & Technology, Transportation Security Administration Official Website,* http://www.tsa.gov/approach/tech/trace_portals.shtm (accessed December 3, 2007).

179 U. S. Department of Homeland Security, Transportation Security Administration, "Bottled Liquid Scanners," *Innovation & Technology, Transportation Security Administration Official Website,* http://www.tsa.gov/approach/tech/bls.shtm (accessed December 3, 2007).

180 U. S. Department of Homeland Security, Transportation Security Administration, "Mitigating High Consequence Risk," http://www.tsa.gov/what_we_do/tsnm/mass_transit/risks.shtm (accessed December 3, 2007).

181 U. S. Department of Homeland Security, Transportation Security Administration, "Trace Portals," *Innovation & Technology, Transportation Security Administration Official Website,* http://www.tsa.gov/approach/tech/trace_portals.shtm (accessed December 3, 2007).

182 See, e.g., *United States v. Aukai,* 497 F.3d 955 (9th Cir. 2007) (en banc) (finding that airport searches are an appropriate regulatory search scheme not relying on implied consent).

Transportation Security Administration (TSA) Website notes that these technologies are being piloted with respect to securing rail transit.[183] News reports have also related TSA attempts to pilot sensor technology for use in rail facilities.[184]

In the area of narcotics detection there has recently been development of commercially available portable mechanical sensors to address this issue.[185] These sensors, while targeted to emanations from the manufacture of methamphetamine, are not in principle unlike biological and chemical sensor equipment long available for military use. An extensive commercial market is now growing for the civilian use of these sensor technologies. While the bulk of the legal analysis on this topic has focused primarily on the issue of narcotics, there are significant homeland security implications. Development and utilization of these technologies in a binary format to detect the presence of explosives is viewed as key to the ability to safeguard the national transportation.

Binary contraband detection protocols may even be extended into searches conducted across cyberspace. In a legal note for the Yale Law Journal, Michal Adler discusses legal issues that surround the possibility of net-wide searches for digital contraband.[186] Using the example of child pornography that could be tagged or specifically identified by law enforcement, the possibility exists to track that pornography to the computer hard drive of the person who possesses it. The hard drive search would only detect contraband and not search other items. While the item is contraband and this is generally afforded no protection, the search would necessarily invade a hard drive that might well be in a person's residence. It is unclear with the current state of the law

183 U. S. Department of Homeland Security, Transportation Security Administration, "Mitigating High Consequence Risk," http://www.tsa.gov/what_we_do/tsnm/mass_transit/risks.shtm (accessed December 3, 2007).

184 Thomas Frank, "Security Devices Falter in Rail Tests," *USA Today*, 13 February 2007.

185 Pete Smith, "Meth Detector Tested by Police May Fall into a Legal Grey Zone," *USA Today*, November 6, 2007, http://www.usatoday.com/news/nation/2007-11-05-methgun_n.htm?loc=interstitialskip (accessed December 2, 2007).

186 Michael Adler, "Note: Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and Net-Wide Search," 105 *Yale L. J.* (1996): 1093.

whether such a net-wide search would be permitted or precluded by the Fourth Amendment. Adler posits that the result may largely depend on the danger posed by the contraband being sought.[187]

Professor Ric Simmons, based largely on critiques from the dissenting opinions of *Caballes*, outlines some of the key factors that need to be considered in the application of the binary technology.[188] Those considerations include questions of accuracy and invasiveness.

(1) Accuracy. Assessment of system accuracy involves three inquiries. The rate of false negatives; the rate of false positives; and the positive predictive value. A false negative is an occurrence where the technology fails to detect the presence of the contraband item that it is designed to identify. The false negative does not implicate legal or privacy concerns but it has serious implication for operational security concerns. The false negative results in contraband escaping detection.

On the other hand is the false positive. This is the circumstance where the sensor or testing mechanism wrongfully identifies the existence of contraband where none exists. In mechanical sensor devices, there is frequently a relationship between the rate of false negative and false positive. The more sensitive the analytic tool, the more prone it is to attribute a false positive. Dulling the analysis may reduce the false positive rate, but raise the incidence of false negatives. [189]

Positive predictive value concerns the false positive rate as it relates to the number of persons subjected to the detection technique. Simmons explains this phenomenon as follows:

> The positive predictive value is calculated by dividing the total number of true positives by the total number of positive responses returned by the device. For example, let us assume that in the course of one year, a drug dog conducts 1000 sniffs for narcotics, and alerts 100 times out of the thousand. Of those 100 positive alerts, 90 are accurate and 10 are false positives. This translates into a 1% false positive rate (10 false positives

187 Adler, "Note: Cyberspace, General Searches," 1119.

188 Simmons, "The Two Unanswered Questions," 448.

189 Ibid., 451-53.

> out of 1000 attempts, meaning that only 1% of subjects are falsely accused by the dog), but a 90% positive predictive value (90 true positives out of 100 positive responses, meaning that once the dog returns a positive response, the law enforcement agent can only be 90% sure that contraband is actually present).[190]

Significantly when the number of the population subjected to the detection technique is high and the likelihood of the existence of any contraband item in that population is low, the positive predictive value shifts dramatically. Simmons illustrates:

> … the positive predictive value will vary widely depending on the actual frequency of the illegal activity that is being investigated. In our example above, 9 out of every 100 subjects carried narcotics, but if the dog were randomly sampling the general population, the number might be closer to 9 out of 100,000. Assuming the dog still falsely alerts 1% of the time (a consistent 1% false positive rate), he will now falsely accuse 1000 individuals (and correctly alert to the 9 carrying narcotics), but because there are so many fewer true positives, the positive predictive rate would be dramatically lower than in the previous example: 9 out of 1009, or 0.9%. In other words, if the search is for a type of illegal activity that is very rare (or at least very rare among the pool of subjects being searched), the vast number of innocent subjects will inflate the absolute number of false positives, and make the binary search much less accurate.[191]

While the Court in *Caballes* recognizes that no detection technology is perfect, it leaves unclear the acceptable rate of failure that will result in unwarranted searches or other intrusion into personal privacy. Certainly a critical driver in determining what is an acceptable rate of false positives or predictive value is the danger posed by the contraband. Where the contraband sought is nuclear material or a potentially deadly chemical or biological substances, the courts will likely accept a higher rate of false positives or a lower predictive value. Moreover, as Simmons' work points out, the positive predictive value of the tool can also be shaped by its utilization. Using technology that has a low false positive rate may be unacceptable if it is applied in high volume populations where the likelihood of occurrence of contraband is low.

---

190 Simmons, "The Two Unanswered Questions," 452.

191 Ibid., 452-53.

(2) Invasiveness. The second unanswered question goes to the issue of invasiveness of the search process. This seems to be a relatively easier question to resolve than the question of accuracy for searches that are truly binary in nature. Inasmuch as the surveillance technique reveals the presence or absence of an item in which there is no privacy interest, i.e., contraband, the only invasion into personal liberty is restraint on movement that may have to occur for the surveillance to be conducted. Certainly prolonged restraint would not be permissible, but whether or not requiring individuals to pause for a few seconds, wait in line or perform limited physical movements like raising their arms, are matters open to question. Actually, this is not an issue of "search" under the fourth amendment so much as it is in "seizure."[192] While this may implicate significant liberty interests, the effect on privacy seems *de minimus.*

While *Caballes* offers considerable support for the application of binary surveillance technology where accuracy and lack of invasiveness can be demonstrated, a further consideration that should factor into decisions on the use of binary search technology, or any technology for that matter, is the danger posed by the contraband itself. This factor is discussed at length by Judge Posner in *Catastrophe.*[193]

Certainly searches for potentially catastrophic items like explosives, particularly as they may be introduced on an aircraft, will likely allow implementation of binary search technology with both higher false positive and lower positive predictive values that would be afforded for a search for narcotics or drugs on the street. Such exigent circumstance might also allow for greater license with regard to the invasiveness of such surveillance. Application of the special needs doctrine referenced in *Caballes* and *Edmonds* would certainly support such a contention. The notions of special needs to combat unusual and extraordinarily dangerous threats may extend as well to non-binary object surveillance.

---

[192] Simmons, "The Two Unanswered Questions," 459-61.

[193] Posner, *Catastrophe.*

b. Non-Binary Detection Technology

Non-binary technologies are ones that identify not only contraband, but also a range of other items that an individual may possess. While there may be no privacy interest in contraband, there is a privacy protection in those non-contraband items possessed by an individual. Examination of the contents of man's pocket or woman's purse undoubtedly raises issues of privacy related to isolation and the ability to withdraw information about ones self from others.

Some of the newly developed non-binary technologies go beyond indicating the presence of items an individual possess to showing detailed images of the individual's body. This challenge to physical integrity goes to the heart of privacy protected by the state of isolation and intimacy. The implication of developments in this non-binary object identification technology can be advanced by examining developments in concealed weapons identification technologies like millimeter wave and backscatter x-ray especially in contrast to enhancements in object identification through CCTV.

(1) Concealed Weapon Search Technologies. Just as there have been evolutions in binary object surveillance technology looking for explosives, there have also been revolutionary developments in non-binary technology searching for concealed weapons. Technology like magnetometers, used for the detection of dangerous objects, have long been used in airports and other public buildings like courthouses and even the Capitol. This technology measures disturbances in an electromagnetic field to determine the presence of concentrations of metal associated with weapons like knives and firearms.[194] It has been consistently found to constitute a search.[195] The use of these search devices has been permitted under two theories: regulatory search essential to facility operation; or consent search under a notion that the individual consented to the procedure by entering the area where the magnetometers were established.[196]

---

194 David A. Harris, "Superman's X-Ray Vision," 1, 47.

195 Ibid., 47-8.

196 Wayne R. LaFave, *Search and Seizure,* Volume 2, Chapter 3, Section 3.9(h).

Use of magnetometers has expanded to other public venues like schools, and public places of amusement like stadiums and large sporting events. Courts have found these non-intrusive search techniques to be consistent with fourth amendment protections. Recently several lower courts have even upheld a policy of the National Football League to implement a policy of more highly intrusive physical pat-down searches to accomplish the same goal of searching for dangerous contraband. However, as demonstrated in the recent Eleventh Circuit decision upholding pat-downs at Tampa Stadium, these searches are permissible because the subjects consented to them.[197] A completely opposite conclusion was reached where the City of Columbus, Georgia sought to use magnetometers to screen a crowd of non-consenting demonstrators.[198]

Seeking to increase the effectiveness of the magnetometer, the law enforcement community has been looking to develop technology to enhance the ability to screen for concealed weapons at a distance. Beginning in the mid 1990's, the National Institute of Justice (NIJ) began analyzing the feasibility of certain technologies to provide law enforcement officers with stand-off capability to detect the presence of concealed weapons. Those technologies examined included millimeter wave technology and backscatter x-ray technology. The goal of the NIJ research was to develop technology capable of alerting law enforcement personnel of the existence of weapons from a distance of up to 30 feet.[199] As Jon Vernick notes in his work assessing developments in concealed weapon detection development, this technology may be used to replace pat down searches in those places where it is permissible such as incident to a *Terry*[200] stop, during administrative searches at entrances to airports and some public buildings and in processing persons incident to arrest.[201] In these circumstances, where physical search is

197 *Johnston v. Tampa Sports Auth.*, 490 F.3d 820 (11th Cir. 2007).

198 *Bourgeois v. Peters*, 387 F.3d 1303 (11th Cir. 2004).

199 National Law Enforcement and Corrections Technology Centers (NLECTC), "Innovations in Concealed Weapons Detection Technology," *TechBeat*, (Rockville, MD: National Institute of Justice, October 1997), http://www.nlectc.org/pdffiles/techbt.pdf (accessed December 4, 2007).

200 *Terry v. Ohio*, 392 U.S. 1 (1968).

201 Vernick et al., "National Challenges in Population Health."

permitted, the use of this technology might well be considered less intrusive. However, this technology to conduct suspicionless searches of the general population raises different questions.[202]

Millimeter wave and backscatter x-ray promised higher resolution and better ability to determine the presence of weapons than did the magnetometer. Such technology would likely make searches both more efficient and effective. Consequently, both technologies have been selected for piloting by the TSA for use in transportation in enhancing transit security.[203]

Millimeter wave technology involves the use of radio frequency waves bounced over the subject.[204] Differences in irradiation from the subject allow for the creation of pictures of suspect items. Tests of the technology allow for identification of weapons from portable detectors up to twelve feet away.[205] One of the beneficial features of this technology is that suspect items like knives or guns appear as darkened objects on a lighter grey field. The technology does not delineate body features.[206] The TSA reports this technology is currently used in safeguarding several federal, state, and local public buildings as well as a number of international airports. It is reported to expose the subject to significantly less energy than exists in a cell phone transmission.[207]

Another concealed detection device utilizing different technology is the backscatter x-ray. Backscatter x-ray technology involves high speed scanning with low level x-ray beams. The radiation that is reflected back is translated by the computer into high resolution images. These images depict not only metallic and non-metallic

---

[202] Vernick et al., "National Challenges in Population Health."

[203] U. S. Department of Homeland Security, Transportation Security Administration, "Whole Body Imaging," *Innovation & Technology, Transportation Security Administration Official Website,* http://www.tsa.gov/approach/tech/body_imaging.shtm (accessed December 3, 2007).

[204] U. S. Department of Homeland Security, Transportation Security Administration, "Millimeter Wave," *Innovation & Technology, Transportation Security Administration Official Website,* http://www.tsa.gov/approach/tech/mwave.shtm (accessed December 3, 2007).

[205] NLECTC, "Innovations."

[206] Ibid.

[207] U. S. Department of Homeland Security, Transportation Security Administration, "Millimeter."

items that may secreted on a body,[208] they also include high resolution depiction of the body itself. In fact, the TSA has installed privacy filters on the backscatter x-ray technology it is piloting to eliminate depiction of sensitive private areas of the body.[209] The backscatter x-ray technology is reported as "…equivalent to the ambient radiation received in two minutes of airplane flight at altitude."[210]

As demonstrated above by the TSA's attempt to mask private areas of the body, proponents of both the millimeter wave and backscatter technologies are attempting to move these surveillance techniques close to binary search technology. The TSA descriptions of use of both backscatter[211] and millimeter wave[212] technologies emphasize the fact that operators are not provided with intimate details of the body. In addition, in response to the highly revealing features of backscatter x-ray technology, the TSA has taken additional measures to ameliorate privacy concerns.[213]

Those measures include making the use of the technique voluntary for those passengers who would otherwise be subject to physical pat-down searches. TSA has introduced operational procedures that have the individuals' monitoring the images offsite, away from the checkpoint, with no visual of the person being screened, only the computer image. Information about the images is then phoned to the personnel at the checkpoint. The checkpoint personnel never see the backscatter image. Moreover, those images are not stored, printed or transmitted.[214]

Moving to a completely binary technology in the area of concealed weapons may be extremely difficult to achieve. In addition to technology challenges of blinding the scans only to the presence of "contraband" concealed weapons, in many

---

208 U. S. Department of Homeland Security, Transportation Security Administration, "Backscatter," *Innovation & Technology, Transportation Security Administration Official Website*, http://www.tsa.gov/approach/tech/bscatter.shtm (accessed December 3, 2007).

209 Ibid.

210 Ibid.

211 Ibid.

212 U. S. Department of Homeland Security, Transportation Security Administration, "Millimeter."

213 U. S. Department of Homeland Security, Transportation Security Administration, "Backscatter."

214 Ibid.

states carry of concealed weapons is permitted.[215] In fact, federal legislation permits retired law enforcement officers to carry concealed weapons nation-wide. While there are some areas like airports and public buildings that are accepted under this legislation, it does extend to most other public areas. Thus, unlike, drugs or explosives, items identified by concealed carry searches may not in fact be "contraband" at all depending on the location of the search. This undercuts the entire theory of binary search which is predicated on the absence of privacy interest in contraband.

Even if the technology could be made binary by enhancing imagery and use in areas where weapons would be contraband, e.g. airports, the application of this technology is subject to the same scrutiny with regards to the issues of accuracy and invasiveness discussed above with respect to approved binary search technology like canine sniffs. If the invasive technology can be programmed to alert only the operator with a positive or negative indicator for the presence of weapons or other contraband, this type of technology might then be available for use in public areas to look for dangerous contraband.

One last issue with regard to concealed weapons technology is the issue of public concern over interference with reasonable expectations of privacy. Some polling evidence suggests that such technology would receive general acceptance. Vernick notes in work concerning studies he conducted about privacy expectations and gun scanners:

> Study findings might be used to conclude that society does not recognize a reasonable expectation of privacy regarding gun scanners. The strongest evidence for this conclusion derives from the overwhelming general support for police use of gun scanners. When asked, "Overall, do you favor or oppose police using new weapon detection devices in high crime areas?", eighty-six percent favored or strongly favored such uses. Overall support varied surprisingly little by age, race, or gender. [footnote omitted]
>
> Despite the high levels of general support for the technology, study findings suggest less societal consensus for certain uses of the technology. Specifically, when asked about support for random, suspicionless scans of

[215] Vernick, National Challenges in Population Health, 573.

> persons on the street, fifty-five percent expressed support. [footnote omitted] Although this is still a majority of respondents, it may not provide sufficient evidence that society does not recognize a reasonable expectation of privacy for this use of gun scanners, especially by comparison with the ninety-three percent of respondents who supported using the devices at the "entrance to a school where students have previously brought weapons." [footnote omitted][216]

The use of non-binary concealed weapons detection technology poses questions for applications of a range of non-binary technologies. Public acceptance of these technologies, at least for some limited uses is also significant. The current approach of the TSA to try and mold this non-binary technology into the model of a binary system in object identification offers some interesting prospects for general rules about governance for surveillance systems.

(2) CCTV as a Detection Technology. While the non-binary magnetometer technology has been found to constitute a search, some traditional non-binary techniques for object detection have generally been viewed as not implicating any protected privacy concern. Chief among those technologies is CCTV. Like magnetometers, CCTV systems have long been used in connection with object identification. For example, CCTV has also been used to identify suspicious objects warranting follow up search. They have also been used in a variety of commercial and employment contexts as anti-theft devices.

The application of this non-binary technology seems to be covered by the "plain view" doctrine. As the U.S. Supreme Court noted in *Coolidge v. New Hampshire*, "it is well established that, under certain circumstances, the police may seize evidence in plain view without a warrant."[217] Where a person is observed through CCTV to be in possession of what appears to be a piece of contraband, the plain view doctrine supports police action.

While there would seem to be little controversy over using cameras at fixed points or perhaps in conjunction with x-ray machines or magnetometers to assist in the detection of contraband items like weapons, the technology does not significantly

---

[216] Vernick, National Challenges in Population Health, 570.

[217] *Coolidge v. New Hampshire*, 403 U.S. 465 (1971).

enhance the existing technology. This is particularly true where the contraband is concealed from view, which is usually the case. The growing field of video analytics may help to enhance the value of object detection by automating the process of object search.[218]

The value of this technology dramatically shifts, however, when the object of detection becomes the physical traits of an individual who may be wanted for some crime. That is the value proposition of facial recognition technology. If this technology could be used in a binary fashion, like concealed weapons technology to identify persons who are wanted on a warrant or other judicial court order, it is difficult to see what constitutional argument could be mounted. Those individuals wanted on a warrant have no constitutionally protected interest to remain at large.[219]

The use of face recognition technology has already been piloted in both the United Kingdom and in the U.S. However, the promise of facial recognition technology has not yet been realized by the existing technology. For example, in 2001 the Tampa, Florida police department began utilizing facial recognition software in connection with camera systems in its entertainment district, Ybor City.[220] Where the photographic image was designated by the computer system as matching a wanted person in the database, officers could be dispatched to investigate.

The success rate of facial recognition systems piloted thus far has been less than impressive. The ACLU has reported that Tampa abandoned use of the system within months of its rollout with no arrests having been made. The Tampa police deny abandoning facial recognition; instead, indicating they are configuring the system to work with more cameras.[221] Testing at the Palm Beach Airport resulted in a positive

---

[218] Arun Hampapur, et. al, "Smart Video Surveillance: Exploring the Concept of Multiscale Spatiotemporal Tracking," *IEEE Signal Processing Magazine* (March 2005), http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1406476 (accessed January 13, 2008).

[219] See, e.g., *Barry v. Fowler*, 902 F.2d 770 (9th Cir. 1990); and *Foster v. Metropolitan Airports Commission*, 914 F.2d 1076 (8th Cir. 1990) (single indivisible liberty interest of persons wanted on a warrant).

[220] Taslitz, "Technology, Privacy and Human Emotions," 125.

[221] David Kopel and Michael Krause, "Face the Facts Facial Recognitions Trouble Past and Troubling Future," *Reason Magazine*, (Los Angeles, CA 2002), http://www.reason.com/news/show/28539.html (accessed January 12, 2008).

identification rate of only 47% over the four-week test period. There were also some 1,081 false alarms generated (a rate of two to three per hour of operation) from a facial database of only 250 photos.[222]

Despite the absence of positive results in the early years of this decade, facial recognition technology has made improvements. In 2003, the *New York Times* reported that tests conducted by the National Institute of Standards and Technology (NIST) found substantial improvement over systems tested in 2000.[223] Results of similar assessments conducted by NIST in 2006 show further progress. [224] Moreover, government funded research for facial recognition technology was estimated to be in excess of $48 million dollars as of January 2001, and has likely grown since.

In light of the government demonstrated interest and growing efficacy of facial recognition technology, an understanding of how the technology functions is important. Use of facial recognition in conjunction with CCTV is actually a merger of two surveillance technologies, digital CCTV with embedded software and biometric facial recognition technology. The biometric portion of the technology is described as follows:

> F[acial] R[ecognition] T[echnology] works by combining photographic images with computer databases. After an image is captured by a camera, a computer program measures some of the 80 or so nodal points on your face, such as the distance between your eyes, the width of your nose, the depth of your eye sockets, and the length of your jaw line. The technology then turns the nodal measurements into a numerical code called a "faceprint." A properly working face recognition system supposedly can match a person standing in front of a camera with a record from a database including tens of millions of faceprints.[225]

---

[222] David Kopel and Michael Krause, "Face the Facts Facial Recognitions Trouble Past and Troubling Future," *Reason Magazine*, (Los Angeles, CA 2002), http://www.reason.com/news/show/28539.html (accessed January 12, 2008).

[223] Barnaby J. Feder, "Face Recognition Technology Improves," *The New York Times*, March 14, 2003, http://query.nytimes.com/gst/fullpage.html?res=9805E0D9103EF937A25750C0A9659C8B63 (accessed January 12, 2008).

[224] P. Jonathan Phillips et. al, "FRVT 2006 and ICE 2006 Large-Scale Results," *NISTIR 7408* (Gaithersburg, MD: National Institute of Standards and Technology, 2007), www.frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf (accessed January 12, 2008).

[225] Phillips et. al, "FRVT 2006 and ICE."

In addition to the biometric database of faceprints there is also a requirement for the development of software for the operation of the CCTV system. This involves programming software that operates the CCTV system so that the faceprint database can be matched against the live CCTV images. This matching process is done based on a system of mathematical formulas called algorithms. These algorithms themselves may contain biases. As Lucas Introna and David Wood note in their work on algorithmic surveillance, the algorithms used to power facial recognition software contain biases. These biases occur in the process of reducing the results of photographic images into the algorithms that power analysis. For example, software that is based on "template based algorithms" which are predicated on the gallery of templates (facial shapes) that vary among the population tend to have greater predictive accuracy rates for minority populations because their faces differ most from the templates.[226]

The existence and extent of biases caused by algorithms used in any given system need to be addressed and understood before the imposition of any facial recognition system. The introduction of, for example, racial biases in the software employed implicate fourteenth amendment due process and equal protection concerns. In addition to biases based on race, Introna and Wood point out that the algorithms may also impact the efficacy of the system based on a variety of other factors including: sex; lighting condition; position of the subject's head when being scanned by CCTV; and the presence or absence of glasses or facial hair.[227] Until the issues of accuracy can be more successfully addressed, facial recognition technology will have little practical use. Moreover, because the algorithms are included in code written for software systems that are often proprietary in nature and involve extremely complex mathematical formulas, it is difficult for an assessment to be conducted by most purchasers before implementation.

When the accuracy and bias issues are finally resolved, the application of facial recognition technology holds great promise for identifying individuals particularly in areas that require great security. However, even if those

---

[226] Lucas D. Introna and David Wood, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems," *Surveillance and Society* 2, No. 2/3 (2004): 177, 185-90, http://www.surveillance-and-society.org/cctv.htm (accessed January 12, 2008).

[227] Ibid., 190.

questions were answered a significant question remains regarding what faces should be placed in the database for matching and identification. Placing the faces of those individuals wanted pursuant to warrant or some court order would likely raise little concern. However, the placement into that database of individuals determined to be of general law enforcement interest raises significant legal questions both in terms of maintaining such a database (what criteria warrants identifying someone as suspect) and use of the database (what do law enforcement officers do if a suspect person is found—how and why should they be treated differently). These two questions will be treated more in depth with regard to the tracking of suspect persons. However, the current use of computer based networks to identify sex offenders so they can be precluded from accessing areas like schools, and the government maintained "no-fly" lists, provide concrete examples where facial recognition software might be helpful in maintaining security.

One additional feature of automated CCTV surveillance is what is known as an "anonymization" or "video masking" features.[228] Just as algorithms can be introduced through software to identify facial features, different algorithms can be introduced to block or blur facial features. This anonymization feature could be used to make binary a CCTV system facial recognition program designed to look only for specific persons. If, for example, the system could be successfully programmed only to look for individuals wanted on a warrant and to block the facial features of all other persons, it would seem that such a system would meet the type of binary system requirements outlined above. Of course, this anonymization technology is in its infancy and like the facial recognition technology requires future development.

Building on the analysis outlined in the Simmons article, there needs to be an examination of standards of reliability for use of search technologies to identify suspect items and persons based on physical characteristics. This analysis combined with an understanding of what types of threats (e.g. explosives, chemical

---

228 Samuel K. Docknevich, "Technology Perspectives: CCTV Technology," *U. S .Department of Homeland Security, Privacy Office, Public Workshop CCTV: Developing Privacy Best Practices* (PowerPoint Presentation), December 17, 2007.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Technology_Perspectives_Panel.pdf (accessed March 15, 2008)

weapons, biological weapons or conventional firearms) should be subject to search utilizing this technology is a matter for further research and analysis.

2. Area Observation and Monitoring Technology

Area observation and monitoring for public safety purposes is a broader function than simply law enforcement. While deterring and preventing crime are certainly functions of many programs involving surveillance, they are not the only public functions served by those technologies. The availability of area observation and monitoring equipment may prove critical to a range of other public safety activities. Situational awareness provided by those technologies can serve to facilitate public safety response, whether that be through dispatch of police assets or fire and emergency medical service, (EMS) in response to an event. Area observation and monitoring technology can help to ensure compliance with safety regulations through programs like red light or speed enforcement or be utilized to adjust traffic patterns to meet requirements of emergency situations or even the daily rush hour. While observation and monitoring technologies play a role in terrorist and crime prevention and control, they can also play important roles in response and management of public safety service to public areas. Oftentimes, this latter function of area observation and monitoring technology is overlooked.

The preferred method of area observation and monitoring involves the use of CCTV. While a range of other surveillance technologies are available for this purpose, they all have significant limitations. Sensor devices like ground surveillance radars, motion detectors, thermal sensors and pressure sensors, can be used to secure perimeters and areas, but the information gleaned from them is limited. They can be triggered and distorted by a range of environmental factors. For example, a fence line equipped with pressure sensors will alert when the fence is disturbed. The operator seeing the disturbance will have no way of knowing what caused it. It might be a downed tree limb, someone passing by and touching the fence, an animal attempting to pass through or an intruder entering the premises. Moreover, even where an intrusion can be ascertained, data for marshalling a response is much more limited. For example, unless the grounds

of the property are equipped with additional detection devices there will be no way to track any perpetrator, see if he or she is armed, what they look like or gather other pertinent data to manage response.

Contrasted with other sensors, cameras provide much greater depth of information for both law enforcement and emergency response. Cameras can be used in the perimeter security context described above can not only provide information as to the nature of activities resulting in compromise of the perimeter, they can also be utilized in directing the response. Utilizing cameras, the persons directing response can provide precise information about the nature of the intrusion. Descriptions of the intruders, armament, direction of flight; all those pieces of information can be provided by CCTV. This information can be critical for shaping real-time response and also for the legal process of prosecuting offenders.

Area observation and monitoring, whether with cameras or other sensors, is already widespread in communities for a wide variety of purposes. Some of those purposes bear little relationship to law enforcement. One example of a family of technologies that monitor activities in the public space is the host of sensor technologies related to traffic movement. This family includes sensors on the roadways that are used to report traffic times and conditions. Recently several states have introduced data scanning devices to facilitate traffic movement at toll plazas through specially created sensor lanes. The I-Pass program in Illinois is one example.[229] These technologies are often augmented with CCTV technology to record noncompliance. Another traffic related use is red light monitoring cameras. This program involves placement of license plate reading cameras at intersections to monitor compliance with traffic signals. These cameras are credited with 40 percent reductions in red light violations at the intersections in cities that employ them.[230] Recent scholarship on the use of these cameras confirms

---

229 Illinois Toll Highway Authority, I-Pass, General Information, About I-Pass, http://www.illinoistollway.com/portal/page?_dad=portal&_schema=PORTAL&_pageid=133,1471150 (accessed January 13, 2007).

230 Thomas Barlas, "Lawmakers Allow Municipalities to Implement Red Light Program," http://www.pressofatlanticcity.com/news/local/atlantic/v-page2/story/7526811p-7428234c.html (accessed January 13, 2008).

they affect driver behavior, but a question is raised as to whether or not those effects cause more accidents and injuries.[231] This study points to the need for additional research.

The use of sensors including CCTV to secure public buildings and some pieces of critical infrastructure has long been recognized and accepted by the public. For example, perhaps among the most secure public spaces in the U.S. are courthouse buildings, which are routinely equipped with contraband detection devices like magnetometers, and frequently have extensive CCTV systems.

As noted at the beginning of this thesis, the advent of CCTV cameras to support public programs for observation and monitoring is a rapidly developing phenomena across the country. The conduct of government observation of open areas has long been supported by the Supreme Court. This even includes private areas that are privately owned. Beginning with the "open fields" doctrine articulated in *United States v. Hester*.[232] There the court noted "…the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields. The distinction between the latter and the house is as old as the common law."[233] The decision has been reaffirmed by a string of more recent Supreme Court cases from the mid-1980s. Those cases include: *Oliver v. United States*,[234] *California v. Ciraolo*,[235] and *Dow Chemical Company v. United States*.[236] Significantly, the *Dow Chemical* case directly involved the use of cameras to record the observations made.

---

231 Barbara Langland-Orban, Etienne E. Pratch, and John T. Large, "Red Light Running Cameras: Would Crashes, Injuries and Automobile Insurance Rates Increase If They are Used in Florida," *Florida Public Health Review*, 2008: 5: 1., http://health.usf.edu/NR/rdonlyres/C1702850-8716-4C2D-8EEB-15A2A741061A/0/2008pp001008OrbanetalRedLightPaperMarch72008formatted.pdf (accessed March 18, 2008)

232 *United States v. Hester*, 265 U.S. 57 (1924).

233 Ibid. at 59.

234 *Oliver v. United States*, 466 U.S. 170 (1984).

235 *California v. Ciraolo*, 476 U.S. 207 (1986).

236 *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

Given the fact that government can monitor and observe activities on private lands under the "open fields doctrine." It is difficult to see how such observations of public properties cannot be permissible.

Some of the critics of CCTV programs contend that CCTV programs are of questionable efficacy.[237] However, there seems to be little evidence on either side of the efficacy debate. In a report prepared by the California Research Bureau analyzing CCTV programs in the mid to late 1990s, Marcus Nieto concludes "[g]enerally, the data suggests that CCTV video surveillance is successful in reducing and preventing crimes and is helpful in prosecuting individuals caught in the act of committing a crime."[238]

The General Accounting Office (GAO) in a 2003 Report concerning CCTV surveillance programs of the United States Park Police and Washington D.C. Metro Police concluded the following with respect to efficacy: "[m]easuring CCTV effectiveness is difficult because of the lack of comparisons of similar areas with and without CCTV to show a direct cause and effect relationship, and because it is often used in tandem with other law enforcement tools."[239] The GAO reported that during its investigation city officials had the following observations about efficacy:

> Most CCTV users in the selected U.S. cities whose systems were fully operational at the time of our visit did not statistically measure the effectiveness of their CCTV systems. They perceived it to be difficult to measure, although officials in the selected cities said that CCTV had been very effective in, among other things, detecting and investigating crime, monitoring areas for public safety, and enhancing security. Officials provided anecdotes to demonstrate their system's effectiveness. For example, an official in one city said that the CCTV cameras filmed a drug transaction that resulted in an arrest.[240]

---

[237] Mark Schlosberg and Nicole A. Ozer, *Under the Watchful Eye*; and Loren Seigel, Robert Perry, and Margret Hunt Gram, *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight* (New York: New YORK Civil Liberties Union, Fall 2006), www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf (accessed January 13, 2008).

[238] Nieto, *Public Video Surveillance: Is It an Effective Crime Prevention Tool?*

[239] U. S. General Accounting Office, *Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington D.C.*

[240] Ibid., 30.

Information about efficacy of public CCTV surveillance is not limited to the United States. In fact, the GAO report notes the experience of the United Kingdom. The GAO observed the following with respect to the United Kingdom's studies of efficacy.

> A study undertaken on behalf of the Home Office, found mixed results for the crime prevention effectiveness of CCTV. However, in October 2002, a Home Office official said that the Home Office had provided funding for an evaluation of effectiveness for 17 CCTV systems as part of a CCTV initiative begun in 1999 for the implementation of 684 local government operated CCTV systems in the UK. The evaluations are to be completed in November 2004. Home Office officials cautioned that using crime statistics as a measure of effectiveness may not be a good measure. They said that arrest rates might increase because the CCTV cameras view more criminal activity and police are reacting to more reports originating from CCTV control centers. They also said that increased crime rates are notnecessarily bad because it may mean more crimes are being reported that had previously gone undetected. Furthermore, one CCTV user in the UK said that the effectiveness of various CCTV systems could vary due to differences in CCTV supervisory personnel, training, and procedures.[241]

A 2002 British Home Office Study concluded that CCTV programs only reduced crime to a "small degree" and called for the need for further study on the matter.[242]

In light of the state of research on the issue of efficacy of CCTV systems, it seems that there is little on which policymakers can rely on beyond anecdotal evidence. The types of empirical evidence that groups like the ACLU now apparently are requesting would likely require years to generate. While the need to place cameras in some areas and then use other areas as controls, not utilizing them would be politically unfeasible and prohibitively expensive.

Just as questions of efficacy remain with respect to crime reduction, similar questions remain with respect to preventing terrorism. Opponents of CCTV point to the fact that London, which arguably has more cameras than any major city in the world, has been the subject of terrorist attack. Such an argument hardly constitutes evidence of lack

---

[241] U. S. General Accounting Office, *Video Surveillanc*. 28-9.

[242] Brandon C. Welsh and David P. Farrington, "Crime Prevention Effects of Closed Circuit Television: A Systematic Review," *Home Office Research Study 252* (London: Home Office Research Development and Statistics Directorate, August 2002), 45, www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf (accessed January 13, 2008).

of efficacy. The conclusions of these opponents ignore, however, the role of CCTV in assisting authorities in identifying terror suspects and their confederates and facilitating arrests of suspects. Also ignored is the increased cost surveillance systems imposed on the operations of terror organizations.

Beyond the debate over efficacy with respect to crime control, there seems to be little argument that CCTV provides substantial benefit in a number of other public safety contexts. CCTV can clearly provide command and control assistance to those directing first response assets. Having situational awareness of crime scenes or disaster scenes can facilitate the dispatch of appropriate resources. As noted above, these systems also have substantial benefits for traffic management and safety.

The U.S. Supreme Court has recognized the important evidentiary value of CCTV images in its recent decision in *Scott v. Harris*.[243] There the court took the unusual step of appending footage of a police chase to its opinion. The Court concluded the CCTV images clearly evidenced the danger of the conduct of a fleeing motorist

In light of the case law and commentary discussion of the binary search concept, the privacy features of camera surveillance could likely be enhanced by the addition of developing technologies such as anonymization.[244] CCTV systems can also be adapted with "intelligent video" software programmed with algorithms to identify and alert operators to patterns of behavior that warrant scrutiny by system operators.[245] These behaviors include things like approaching secure perimeters, accessing areas where entry is unauthorized, leaving behind backpacks or packages. Like facial recognition technology, intelligent video technology is relatively new and will be required to mature before large scale implementation.

Use of CCTV equipped with these features may serve to reduce the need for continual surveillance and provide greater protections for privacy. For example,

---

[243] *Scott v. Harris*, Slip Op. No. 05-1631, 550 U.S. ___ (April 30, 2007).

[244] Docknevich, "Technology Perspectives: CCTV Technology."

[245] Nusimow, "Intelligent Video for Homeland Security Applications."

anonymizing images may serve to address concerns raised by critics like Marc Blitz[246] and Christopher Slobogin[247] who contend in their comprehensive examinations that increased CCTV surveillance will adversely affect important privacy concerns with regard to anonymity. Use of automated intelligent video to screen for behaviors of concern may help to mitigate some of the concerns raised by Jeffery Rosen who found voyeurism and inappropriate conduct in his examination of British CCTV operators.[248] While these technology solutions will not eliminate concerns, they may serve to mitigate them.

3. Tracking of Suspect Persons

In addition to technologies that detect and provide for observation across a wide area, there is a fast growing field of technologies that can be used to track the movements and actions of individuals. CCTV systems equipped with face recognition software is just one example of such technology. A wide range of other technologies can be used for that purpose. It is the tracking of individuals that seems to be the surveillance function that raises the most concerns with commentators like Blitz.[249]

The tracking of individuals can be accomplished through a range of technologies. Developing technologies for tracking include GPS,[250] cellular and RFID systems.[251] Tracking can also be accomplished through biometric measures that utilize some type of reading mechanism like a CCTV system enabled with facial recognition software, or identity cards or credentials that are read or scanned. Unlike the observation of areas where attention is focused on behaviors only while an individual is in a certain specified

---

246 See Marc Jonathan Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity," *Texas L. Rev.* 82 (2004): 1349.

247 Christopher Slobogin, "Symposium: Public Privacy: Camera Surveillance and the Right to Anonymity," *Mississippi L. Rev.* 72 (Fall 2002): 213.

248 Jeffery Rosen, "A Watchful State," *The New York Times Magazine*, October 7, 2001, http://query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63&sec=&spon=&pagewanted=1 (accessed January 13, 2008).

249 Blitz, "Video Surveillance and the Constitution of Public Space," 1383-1398.

250 Otterberg, "GPS Tracking Technology."

251 Dalal, "Chipping Away at the Constitution," 485.

geographic space, or detection that occurs over a brief time period, tracking is a function that occurs over a more extended period of time.

William Herbert, in his work on human tracking technology, notes the multiple uses already in existence. Use of this technology is by no means limited to the government. Tracking systems are used for a range of purposes, some desirable, some benign and some a little disconcerting. He observes:

> GPS, RFID, cellular technology, and biometrics are utilized by the government to conduct surveillance, employers to monitor employees, school districts to track their students, rental car companies to monitor the use of rented vehicles, and parents to keep track of their elusive teenagers.[252]

Herbert further notes that many of these technologies are largely unregulated.[253] Examining each of these technologies in turn it is clear they can potentially impact privacy both separately and in combination with other technologies like CCTV.

a. RFID Technology

RFID technology involves the communication of digital information through radio waves from a RFID chip or tag to a reading device. [254] This technology is already being used in a wide number of commercial venues for supply chain management. Tags are placed on items or products to ascertain their whereabouts in the delivery process or in managing inventory.[255]

In the public realm, RFID is being widely used in many states as part of an attempt to reduce traffic congestion.[256] The Illinois I-Pass system with over 3 million transponders in use is but one example of these systems.[257] Utilizing a radio transponder

---

[252] Herbert, "No Direction Home," 413.

[253] Ibid.

[254] Dalal, "Chipping Away at the Constitution," 485.

[255] Ibid., 488.

[256] Ibid., 490.

[257] Illinois Toll Highway Authority, http://www.illinoistollway.com/portal/page?_dad=portal&_schema=PORTAL&_pageid=133,1471150 (accessed January 13, 2007).

that is placed in the vehicle it can be tracked as it passes a reader's location, namely, toll plazas. The I-Pass is linked to an account and funds are withdrawn to pay the toll. While the I-Pass has the advantage of allowing a motorist to pass through toll plazas without stopping, it does leave behind a digital record of the motorists' presence. The RFID system is also integrated with a camera system to record the license plate numbers of vehicles that pass through the I-Pass toll lanes without the I-Pass transponders. These individuals are issued bills or citations for failure to pay the toll.

The integration of the two technologies RFID and license plate reading CCTV cameras provide a powerful example of how technology can be used to track movement. While the intent of these systems was just to expedite traffic flow and ensure compliance with toll collection, they have been used to monitor whereabouts of individuals. These records have been subpoenaed in criminal and civil cases to establish the whereabouts of individuals.[258]

RFID technology is also a component of an effort to expedite international travel. In response to the Western Hemisphere Security Initiative[259] that requires the presentation of passports and or other identifying information to pass into Canada or Mexico, several border states are currently investigating or piloting the use of RFID technology in driver's licenses. The "enhanced driver's licenses" are being contemplated or issued in several states including Vermont, Arizona, Washington, Michigan New York and Texas.[260] Washington is planning to issue enhanced driver's licenses beginning in 2008.[261] These driver's licenses contain RFID chips with identifying information. These enhanced drivers licenses would be used at border crossings in lieu of passports. The RFID chip in the license would be read by sensors as persons pull up to border

---

258 Dalal, "Chipping Away at the Constitution," 494.

259 U. S. Dept. of Homeland Security, "Western Hemisphere Travel Initiative," *DHS Website-Prevention and Protection*, http://www.dhs.gov/xprevprot/programs/gc_1200693579776.shtm (accessed January 27, 2008).

260 U. S. Dept. of Homeland Security, "Fact Sheet: Enhanced Drivers Licenses," *DHS Website-Press Room*, (December 5, 2007), http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm (accessed January 27, 2008).

261 Ibid.

crossings.[262] Privacy advocacy groups like the Electronic Privacy Information Center are raising concerns about the use of data from these systems.[263]

b GPS Technology

Similar concerns are raised with regard to GPS and cellular tracking technology. The ability to track wireless communications though GPS and cellular technology already exists and is programmed into most all wireless communications devices that individuals use. David Phillips examines the public safety and private concerns that drive the placement of location tracking features into wireless devices. He notes that the "primary motivating force behind wireless surveillance is the implementation of emergency response."[264] Using cellular or GPS technology, cell phones and other wireless communications devices provide information to public safety personnel answering points to allow police, fire or EMS responders to locate a caller. The installed surveillance technology is also required so that law enforcement with proper court authorizations can conduct wiretaps. A third factor driving surveillance is commercial. It allows the carriers to determine location and use for purpose of marketing their services.[265]

While this GPS or cellular surveillance function in wireless communication devices performs an important public safety function, it can be used for tracking in other contexts. William Herbert in his work on the legal implications of tracking technologies discusses the growth of use in the area of employment. Using GPS and RFID technologies, employers can monitor employee "… work performance and employee location."[266] Hebert notes that other researchers have coined the phrase

---

[262] U. S. Dept. of Homeland Security, "Fact Sheet: Enhanced Drivers Licenses."

[263] Electronic Privacy Information Center, "Proposed 'Enhanced' Licenses are Costly to Security and Privacy," *EPIC Website-Spotlight on Surveillance*, September 2007, http://epic.org/privacy/surveillance/spotlight/0907/default.html (accessed January 26, 2008).

[264] Phillips, "Beyond Privacy: Confronting Locational Surveillance in Wireless Communication," 3.

[265] Ibid., 3-5.

[266] Herbert, "No Direction Home," 455.

"geoslavery" to characterize this phenomenon of human tracking technology.[267] Herbert also notes the ability of RFID technology not only to facilitate tracking, but to catalogue data encoded in the RFID chips. For example, doctors in both the U.S, and United Kingdom have experimented with RFID implants that would allow doctors to access data about the patients.

Arrayed against technology that allows for active tracking of individuals using GPS and RFID technologies, there is little in the way of law or regulation. Commentators universally agree that the issue of government use of GPS and RFID technology to track individuals is a matter that has not been addressed by the Supreme Court.

The two cases that have come closest to addressing the matter are *Knotts* and *Karo*. Both cases involve use of battery powered beepers that had been employed law enforcement into containers carrying chemicals used in drug manufacture. Both involved law enforcement tracking of the beepers over the public way. In *Karo* the tracking also occurred within a residence. The Court upheld the use of the beeper in *Knotts* and rejected its use in *Karo*, While the significant distinguishing feature between the two cases seemed to be the fact that the technology was applied within the home in *Karo* and only in public areas in *Knotts* some of the Court's observation in *Knotts* raise questions about applicability of the case to technologies like GPS and RFID.

For example in *Knotts*, the Court noted that the beeper was a tool used in addition to visual surveillance to track the individuals. With regard to GPS technology, however, no visual surveillance would ever be required. The whereabouts of the item could be easily monitored from one central location. Moreover, there is an important dimension of scale. The capacity of beeper surveillance is very limited. GPS and RFID technology would allow for the monitoring of vast numbers of individuals simultaneously. In light of the power of RFID and GPS monitoring, it is unclear how the Court would treat, large scale use of such information technology. Concern would doubtless be enhanced if these systems could be linked to CCTV surveillance systems.

---

[267] Herbert, "No Direction Home," 425.

Herbert reviews some developments that have occurred in state courts and legislative enactments that have limited public and private uses of GPS and RFID technology. He advocates legislative solutions to the problem. Commentators like Blitz and Ottenberg suggest that the Supreme Court can and should expand privacy protections against governmental use of technology as the Court did in *Kyllo*. As noted above two states, Oregon and Washington, have ruled that privacy protections in their constitutions prohibit this activity in the absence of a warrant.

c. Biometric Technologies

In addition to the tracking of individuals through devices like GPS and RFID there is also a universe of tracking technologies based on monitoring movements of individuals through use of biometrics. In the realm of physical tracking, biometrics involves "… the automated methods of identifying a person based on unique physical features."[268]

The application of biometrics to tracking is essentially performed in one of two ways, identity verification and identification. Rudy Ng in his work artfully describes the distinction:

> In a typical application, an individual's physical traits are scanned by a machine and then a comparison is made to a database containing previously stored information about that individual. [footnote omitted]. This process is used to positively identify the individual and is referred to as verification, or one-to-one matching. [footnote omitted]. For example, one-to-one matching could be used at a security checkpoint before allowing individuals access to restricted areas of a building. [footnote omitted]. Biometric scanning can also be used to identify a person by comparing their biometric data to all of the records that have been stored in the database. [footnote omitted]. This process is referred to as identification, or one-to-many matching. [footnote omitted]. For example, one-to-many matching could be used to identify an unknown person by trying to match their biometric data to the data of known individuals saved in a database. [footnote omitted].[269]

---

[268] Ng, "Catching Up to Our Biometric Future," 428.

[269] Ibid.

Biometric measurement can be taken from a wide variety of areas of the body. The most commonly used biometric has been that of the fingerprint. Fingerprint matching has been employed in law enforcement as a source of positive identification since the early twentieth century. Once done through a process of comparison by trained technicians, digitized fingerprints can now be read through automated processes. The use of fingerprint based biometrics has expanded to a wide range of verification and identification systems. For example, Herbert talks about biometric used for employee timekeeping functions. "Increasingly, employers are replacing traditional time sheets with biometric technology to monitor time and attendance. [citation omitted]."[270]

Fingerprints are hardly the only biometrics measure that can be used for identification. In fact, several other biometric technologies come from the hand alone. Those biometrics include: hand geometry and vein pattern identification. The latter technology, introduced in Japan in 2004 has gathered large acceptance in the international banking community for its accuracy and the ability to defeat efforts at imitation.[271] Margret Betzel summarizes several other technologies that can be used for identification purposes. Those technologies include physical features like DNA, facial scan and iris scans. She also discusses activity or behavior based identifiers like signature and keystroke identification.[272] The federal government is investigating uses for a wide range of technologies to establish identity.[273]

This verification and identification function of biometrics is extending well beyond the employment context. The transportation industry, largely under the direction of the DHS through Customs and Border Protection (CBP) and the

---

[270] Herbert, "No Direction Home," 455.

[271] Chris Roberts, *Biometric Technologies: Palm and Hand*, (2006), www.ccip.govt.nz/newsroom/information-notes/2006/biometrics-technologies-palmhand.pdf (accessed January 21, 2008).

[272] Betzel, "Recent Changes in the Law of Biometrics."

[273] See generally, The National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics, *Biometrics Frequently Asked Questions*, http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf (accessed January 26, 2008); The National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics, *Biometrics Overview*, http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Biometrics%20Overview.pdf (accessed January 26, 2008).

Transportation Security Administration (TSA) is exploring a wide range of biometric technologies to safeguard the transit system. The technologies being piloted by these organizations include implementation of fingerprint based biometrics and iris scan technology.

An example of a fingerprint based biometric program is the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, seeks to track the comings and goings of foreign nationals.[274] Initiated in 2004, the US-VISIT[275] includes the use of two biometric measures, photographs and fingerprints. The program works as follows:

> US-VISIT is designed to use biographic information (e.g., name, nationality, and date of birth) and biometric information (e.g., digital fingerprint scans and photographs) to verify the identity of those covered by the program. The program applies to certain visitors whether they hold a nonimmigrant visa or are traveling from a country that has a visa waiver agreement with the United States under the Visa Waiver Program. [footnote omitted]. U.S. citizens, lawful permanent residents, and most Canadian and Mexican [footnote omitted] citizens are currently exempt from being processed under US-VISIT upon entering and exiting the country. [footnote omitted].[276]

The purpose of the program was to register all foreign nationals as they entered and departed the country.[277] Biometric samples in the form of fingerprints as well as photographs are taken and registered when a person enters the U.S. They are then checked when the individual leaves the U.S. Recognizing that the collection of this data involves sensitive personal information, DHS has enacted privacy guidelines.[278]

---

274 See generally, U.S. Dept. of Homeland Security, *US-VISIT Program*, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed February 24, 2007).

275 U. S. Government Accountability Office, "Border Security: US VISIT Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry," *Report to Congressional Requestors*, (Washington, D.C.: Government Printing Office, December 2006), http://www.gao.gov/new.items/d07248.pdf (accessed January 21, 2008).

276 Ibid., 2.

277 U. S. Department of Homeland Security, *US-VISIT Program*, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed February 24, 2007).

278 U. S. Dept. of Homeland Security, *US-VISIT: Privacy Information*, http://www.dhs.gov/xtrvlsec/programs/editorial_0678.shtm (accessed January 21, 2008).

This type of tracking to gain control of U.S. borders was strongly advocated by the 9/11 Commission.[279] The program is looking to expand from a 2 finger scanning program to 10 fingers beginning in November, 2007.[280] However, because of cost and operational problems in processing biometric information upon exit, the U.S.-VISIT program concluded that portion of its technology pilot was unsuccessful.[281] The US-VISIT program management office has been examining the use of RFID identification technology for exit processing. However, this identification only RFID technology, which is not encoded with biometric data, does not appear to meet congressional mandates. [282]

In addition to utilizing biometrics to secure borders, there are programs being piloted by the TSA to enhance system security and expedite travel through positive identification of passengers. These programs use a process of biometric verification of persons subjected to background screening so that screening at airports can be expedited. The concept is that trusted or registered travelers who have received background checks can be subjected to reduced on-site screening requirements. The program actually involves a series of private operated programs under the generic heading of Registered Traveler (RT) program.[283]

These RT programs involve the collection of biometric data in the form of fingerprints or iris scans. When the traveler is registered the biometric measurement is taken. A background check of the individual is conducted and if the person is found to be a low threat through a security threat assessment conducted in accordance with standards set by the TSA an encoded travel card is issued. The traveler presents the card when traveling and is processed through a separate screening lane once a biometric reader

---

279 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States.*

280 U. S. Dept. of Homeland Security, *US-VISIT: How It Works*, http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm (accessed January 21, 2008).

281 U. S. Government Accountability Office, "Border Security: US VISIT," www.gao.gov/new.items/d07248.pdf (accessed January 21, 2008).

282 Ibid.

283 See generally, U.S. Dept. of Homeland Security, Transportation Security Administration, *Registered Traveler*, http://www.tsa.gov/what_we_do/layers/rt/index.shtm (accessed February 24, 2007).

verifies identity.[284] Realizing the sensitivity of information collected and used in this process, the TSA has recently promulgated a set of guidelines on safeguarding information gathered.[285]

While the US-VISIT and RT programs are designed to address identification and verification issues amongst the general public, the federal government is also currently piloting biometric based "smart cards,"[286] identification cards coded with biometric and identifying data, for persons working in the transportation industry. Smart cards contain micro chips or memory chips and microprocessors. Unlike magnetic swipe cards that require access to data bases to function (like a credit card), smart cards equipped with memory chips can perform defined operations. Smart cards with micro processors can "…add delete and manipulate information."[287]

One example of smart card technology, the Travel Worker Identification Credentials (TWIC), would allow the federal government to positively establish the identity of all persons working in the transportation field.[288] Similar ideas have also been propounded for law enforcement personnel and emergency responders. The concept of TWIC is to place biometric identification data like digital photographs and fingerprints into a uniform identity card that can then be used to authenticate the identity of vetted personnel at access points in transportation facilities. The TWIC card would presumably become the basis for access control within critical areas of transportation facilities. Only individuals with TWIC cards would be allowed access to sensitive areas.[289]

As with the RT and US-VISIT the managers of the TWIC program recognize the sensitive privacy concerns with regard to collected data. General

---

284 U.S. Dept. of Homeland Security, Transportation Security Administration, *Registered Traveler*.

285 U. S. Department of Homeland Security, Transportation Security Administration, *TSA Register Traveler: Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers, Version 3.1* (January 2008), www.tsa.gov/assets/pdf/rt_standards_v3.1.pdf (accessed January 21, 2008).

286 Betzel, "Recent Changes in the Law of Biometrics," 533.

287 Ibid.

288 See generally, U.S. Department of Homeland Security, Transportation Security Administration, *Transportation Worker Identification Credential (TWIC) Program*, http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed February 24, 2007).

289 Ibid.

information about the program outlines some measures taken to safeguard the information. These mostly govern the collection of the data into a centralized protected database.[290] However, these measures appear to be much less extensive than the guidelines established for RT and US-VISIT data.

One final example of a proposed federal program with implications for human tracking is the REAL ID program. The REAL ID Act of 2005[291] is a program to ensure state issuance of verified identity documents that can be used by the federal government. On January 10, 2008, the Department of Homeland Security issued a final rule that provides guidance to states for issuance of compliant drivers licenses and identity cards.[292]

The REAL ID program requires states to issue complying drivers licenses and identity cards so that their citizens can access federally controlled facilities. Pursuant to the final rule:

> beginning on May 11, 2008, citizens of States that are not REAL ID compliant may not use their driver's licenses or identification cards for official federal purposes such as boarding federally regulated commercial aircraft or accessing federal or nuclear facilities. If these citizens do not have other acceptable forms of identification (e.g., a U.S. passport), they may suffer delays due to the requirement for enhanced security screening. REAL ID-compliant States are those that have both requested and obtained an extension of the compliance date from DHS, or have been determined by DHS to be in compliance with the Act and the final rule.[293]

---

290 U. S. Department of Homeland Security, Transportation Security Administration, *Transportation Worker Identification Credential (TWIC) Program: Frequently Asked Questions*, http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm#general (accessed January 21, 2008).

291 Public Law 109-13, 119 Stat. 231,302 (May 11, 2005), codified at 49 U.S.C. § 30301.

292 U.S. Dept. of Homeland Security, "Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes" *Final Rule*, Docket Number DHS-2006-0030 (6 CFR Part 37) (January 10, 2008), http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part1_2008-01-11.pdf (Part 1); and http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part2_2008-01-11.pdf (Part 2) (accessed January 28, 2008).

293U. S. Dept. of Homeland Security, "REAL-ID Final Rule: Questions and Answers," *DHS Website-Prevention and Protection*, http://www.dhs.gov/xprevprot/programs/gc_1172767635686.shtm (accessed January 27, 2008).

Compliance is required by 2009 with the ability of extension until 2011.[294] While the REAL ID program does not currently contain any requirement for biometric analysis or information in conjunction with issuance of licenses or identification cards, both signatures and digital photographs are required.[295] Both these pieces of data can form the basis for future biometric analysis. It should also be noted that the requirements of REAL ID are being aligned to be compatible with the enhanced driver's license program that uses RFID chips to encode data on driver's licenses.[296] Encoded REAL ID licenses with the RFID features of enhanced driver's licenses offer powerful mechanisms for human tracking.

4. Cyber Tracking

Tracking of human activity is not limited to the physical dimensions of public space. Developing technology allows for the tracking of individual activity in cyberspace as well. Two recent forays by government agencies into the tracking of activity in cyberspace have been well documented. They raise further concerns about the ability of government to track individuals in public space.

One program operated by the federal Bureau of Investigation is a computer program formerly known as "Carnivore".[297] Through the "Carnivore" program the FBI was able to trap internet communications of suspect individuals without application for a warrant. The Carnivore program involved the installation of a collection computer at an internet service provider (ISP) to collect all incoming and outgoing email from an internet address. While the content of the email was not reviewed (although it was stored), the addresses of incoming and outgoing email were recorded.

The FBI concluded that trapping the registration of the email addresses was likened to a pen register recording of the numbers dialed or received by a telephone. The

294 U. S. Dept. of Homeland Security, "REAL-ID Final Rule: Questions and Answers."

295 Ibid.

296 Ibid.

297 See generally, IIT Research Institute, *Independent Technical Review of the Carnivore System*.

Supreme Court had concluded in *Smith v. Maryland*[298] that pen registers did not implicate fourth amendment protections because the information was already registered with the phone company that used it for billing. Thus, there was no expectation of privacy in the numbers of calls made or received. While some privacy protections are afforded to this type of internet search through the provisions of the ECPA,[299] those protections are less than requirements for eavesdropping on electronic voice communications, especially in the areas of judicial oversight and minimization of unrelated information.

Carnivore demonstrates the ability of the government to monitor individual conduct which can relate directly to the most intimate and private thoughts. Utilizing Carnivore the government can track all of an individual's electronic contacts. It can also collect and store the subject of those communications for later review if a warrant is issued. Commentators have noted this poses substantial implications for personal privacy in the digital age.[300]

Similar challenges are posed by the FBI's keystroke logging systems like "Magic Lantern."[301] Utilizing programs like Magic Lantern, the government is able to access computers remotely and then monitor all the activity on the keyboards. This information is particularly useful in decrypting encoded messages. It also allows the key loggers the ability to reconstruct any activity that occurred on the computer. While the actual analysis of this data may not occur until after a warrant is secured, the entry into the system and collection of the keystroke data has been determined by at least one court not to constitute a fourth amendment violation.[302]

---

298 *Smith v. Maryland*, 442 U.S. 735, 743 (1979).

299 18 U.S.C. §§ 2701-2710.

300 Maricela Segura, "Is Carnivore Devouring Your Privacy?"; Raymond Shih Ray Ku, "Modern Studies in Privacy Law…," 1355.

301 Christopher Woo and Miranda So, "The Case for Magic Lantern…."

302 Nathan E. Carrell, "Spying on the Mob: United States v. Scarfo—A Constitutional Analysis…."

5. Summary

As demonstrated above, biometrics, particularly when combined with technologies like CCTV or smart cards, provides significant capacity for government and others to monitor individual movements and activities. The ability to track extends not just to physical space, but to cyberspace as well. The range of protection to address data collected through these programs is relatively small. While case law exists in some states to address some aspects of tracking and some federal statutory restrictions exist in the area of tracking in cyberspace, many aspects of tracking technology are largely unregulated.

The existence of this tracking technology, while not commonly used, at present, by local law enforcement, remains a possibility in the not too distant future. While these programs are designed for allowing access to enter the country, travel on aircraft or work in sensitive areas of transportation facilities, they raise the distinct possibility of tracking individual movement over a period of time. In addition to allowing for tracking activity at any given point in time, the digitization of this new surveillance technology allows for the creation of massive databases collecting activity over time. Sets of data that are collections of public record raise additional concerns.

Tracking technology, be it GPS, RFID, or biometrics, linked to databases and other technologies like CCTV provides powerful tools for monitoring large aspects of human conduct. Combined with technological enhancements in database management they provide a significant capacity for monitoring movement over time. The use of this technology in an individuated manner raises substantial concerns for the states of privacy of both anonymity and reserve. It is the existence of these databases and the enhanced ability of government and others to mine them that pose significant concerns for two of the four states of privacy with the state of reserve particularly at risk.

B. TECHNOLOGY DEVELOPMENTS IN SURVEILLANCE DATA MANAGEMENT

Just as the ability to collect surveillance data has grown with developments in technology, so to have there been improvements in data base management. The

development of digital technology has vastly increased the capacity for storing a wide range of information. It has also increased the ability of manipulating large amounts of data across different data bases. The result of these developments is to allow massive compilations of data by government and large corporate entities that can operate and maintain sophisticated computer systems.

As noted earlier, development of these systems has not gone unnoticed by the Supreme Court in both *Whelan*, and *Reporters Committee*, the Court observed that the government's growing ability to compile and analyze data pose significant concerns. These data compilations ultimately undermine an individual's right of reserve, as Westin characterizes it, the right to keep to one's self and to control dissemination of information about one's self.

Three recent government efforts in compiling massive databases point out: the capabilities of government to establish and manipulate large compilations of public information for security purposes; the attendant privacy issue implications of the creation and use of those compilations; and the cost to government when privacy concerns are not addressed. Looking at these integrated surveillance databases provides insight as to the issues surrounding compilation and use of databases populated with data from surveillance technology, whether that technology includes CCTV, GPS, RFID computer tracking or information from any combination of those technologies.

The Computer Assisted Passenger Prescreening System (CAPPS) is a security measure that has been used in the screening of commercial airline passengers for over ten years. Initiated by air carriers in 1998, pursuant to grant funding by the Federal Aviation Administration (FAA), the purpose of CAPPS was to enhance aviation security. CAPPS functioned as follows:

> Since the late 1990s, prescreening has been conducted using a computer-assisted system that, based on certain criteria and behaviors, identifies passengers that may pose a higher risk to aviation security. These higher-risk passengers and their baggage are subject to additional and more thorough screening.[303]

Post-9/11 as the nation sought to tighten security in the commercial aviation industry, the function of passenger screening was transferred from air carriers to the federal government. In addition to transferring responsibility for screening programs, the federal government, through the TSA, sought to expand the scope of the CAPPS database. Thus, the CAPPS II project was initiated to expand the data reviewed in connection with the issuance of boarding passes.

The CAPPS II project sought to conduct more detailed analysis of the background of passengers than was conducted under the original CAPPS program that just looked at passenger behavior (i.e., purchase of tickets in cash, purchase of only one-way tickets). CAPPS II was designed to operate in the following manner. Air carriers were to be required to obtain the name, address, phone number, and date of birth of potential passengers. That information was to be forwarded for a check against commercial databases to establish a score as to the confidence in the individual's identity. That scored information would then be processed by CAPPS II through a compendium of classified and unclassified government databases to specify a risk category for each passenger. The exact number and identity of databases to be queried has not been made public by TSA. Once a risk category is identified (either acceptable risk; unknown risk; or unacceptable risk) the information would be transmitted to the air carrier for encoding on the boarding pass. At the passenger-screening checkpoint, the encoded information would dictate the level of screening applied. [304]

While the CAPPS II planners paid some attention to issues like privacy concerns and data security, the Government Accountability Office (USGAO) in its 2004 review of

---

[303] U. S. Government Accountability Office, "Computer-Assisted Passenger Prescreening Faces Significant Implementation Challenges," *Report to Congressional Committees*, (Washington, D.C.: Government Printing Office, February 2004), www.gao.gov/new.items/d04385.pdf (accessed January 24, 2008).

[304] Ibid., 7-8.

the program found the TSA's efforts inadequate. The report noted that the TSA had not placed use limitations with regard to data collected. It also failed to provide for individual participation in the process so an individual could know what data was collected about him or her. Additionally the USGAO found inadequate procedures for redress and safeguards for data security.

The USGAO was not the only organization to raise concerns about CAPPS II. Privacy advocacy groups like the ACLU also voiced concerns.[305] When Delta Airline agreed to provide information for a pilot of the CAPPS II program, in March 2003, there were calls for a boycott of the airline.[306] Criticism was not limited to domestic sources. Concerns about the CAPPS II were expressed by foreign governmental organizations like the European Union whose citizens as air travelers were subject to the CAPPS II database.[307] In the face of this criticism, the TSA announced it was abandoning the CAPPS II program and, in August 2004, noted the creation of a new computer screen program "Secure Flight."[308]

While the August 2004, media announcement of Secure Flight indicated testing would begin before the end of 2004, the program has yet to be implemented. Secure Flight continues to suffer from a number of the same criticisms raised about its predecessor CAPPS II. A 2005 report by the USGAO assessing Secure Flight indicates that many of the same privacy issues confronted by CAPPS II remain unresolved:

> … TSA has recognized that Secure Flight has the inherent potential to adversely affect the privacy rights of the traveling public because of the use of passenger data, and has begun to take steps to minimize potential impacts on passengers and to protect passenger rights during the testing

---

305 American Civil Liberties Union, The Seven Problems With CAPPS II, http://www.aclu.org/privacy/spying/15258res20040406.html (accessed January 26, 2008).

306 Michelle Delio, "Privacy Activist Takes on Delta," *Wired* (March 5, 2003), www.wired.com/news/privacy/0,1848,57909,00.html (accessed January 26, 2008).

307 European Parliament, Draft European Parliament Resolution on the First Report on the Implementation of the Data Protection Directive (95/46/EC), February 24, 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ep_report_cappato_04_en.pdf (accessed January 26, 2008).

308 U. S. Department of Homeland Security, Transportation Security Administration, "TSA to Test New Passenger Pre-Screening," *TSA Website-Media Room*, August 26, 2004, http://www.tsa.gov/press/releases/2004/press_release_0496.shtm (accessed January 26, 2008).

> phase of Secure Flight. However, TSA has not yet clearly defined the privacy impacts of Secure Flight in an operational environment, or all of the actions TSA plans to take to mitigate potential impacts. TSA also drafted a redress process to provide passengers who believe they were inappropriately delayed from boarding their scheduled flights because of Secure Flight a means by which to appeal these decisions and possibly correct erroneous data found in the terrorist screening database or in commercial databases, should TSA decide to use commercially available data. However, TSA has not yet clearly defined how it plans to implement its redress process for Secure Flight, such as how errors, if identified, will be corrected, particularly if commercial databases are used. In addition, although DHS and TSA have taken steps to address international privacy concerns in developing Secure Flight, such as limiting Secure Flight to prescreening only domestic passengers, issues remain, particularly with regard to the European Union.[309]

The TSA continues to work toward implementation of the Secure Flight program. A notice of proposed rulemaking on the program was issued for public comment in August 2007.[310] The TSA has most recently projected implementation of the Secure Flight program for 2009.[311]

The federal government alone is not the only governmental entity that has sought to use complex data compilations to conduct surveillance of individuals though inter-related database searches to identify "suspect" persons and conduct. Another example of the use of computer analysis of complex databases is the Multi-State Anti-Terrorism

---

309 U. S. Government Accountability Office, "Aviation Security: Secure Flight Development and Testing Under Way, but Risk Should Be Managed as System Is Further Developed," *Report to Congressional Committees*, (Washington D.C.: U.S. Government Printing Office, 2005), http://www.gao.gov/new.items/d05356.pdf (accessed January 26, 2008).

310 U. S. Department of Homeland Security, Transportation Security Administration, *Notice of Proposed Rulemaking* [Docket No. TSA-2007-28572], August 8, 2007, http://www.tsa.gov/assets/pdf/secureflight_nprm.pdf (accessed January 26, 2008).

311 U.S. Transportation Security Administration, "Secure Flight Program," *TSA Website-What We Do*, http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm (accessed January 26, 2008).

Information Exchange (MATRIX) Pilot Project.[312] This project was a DHS funded program managed by the State of Florida.[313] The project concluded in December, 2005[314]

The MATRIX project involved computer aided analysis of a range of public records. The program boasted the ability to search up to 20 billion records. Those records include telephone and cell phone records, financial records and location records. The Congressional Research service report on MATRIX noted that the records utilized in MATRIX included:

> … a broad array of public data, ranging from motor vehicle driving records to bankruptcy filings. While much of these data have been available to law enforcement, they have not been previously queried, cross-referenced, and analyzed with computers. According to the MATRIX website, such records include the following:
>
> - pilot licenses issued by the Federal Aviation Administration;
> - aircraft ownership;
> - property ownership;
> - U.S. Coast Guard-registered vessels;
> - state sexual offender lists;
> - corporate filings;
> - Uniform Commercial Code filings or business liens;
> - bankruptcy filings; and
> - state-issued professional licenses.[citation omitted]

According to the MATRIX website, available records also include records that have historically been available to law enforcement agencies. Such records include

312 Krouse, The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project.

313 Ibid.

314 U. S. Dept. of Homeland Security, Privacy Office, *Report to the Public Concerning the Multi-Sate Anti-Terrorism Exchange (MATRIX) Pilot Program*, (Washington, D.C.: Government Printing Office, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy-matrix-122006.pdf (accessed January 26, 2008).

- criminal history records;
- department of corrections information and photo images;
- sexual offender criminal history files;
- driver's license information and photo images; and
- motor vehicle registration information.[citation omitted][315]

By aggregating all these data sources, none of which would independently be afforded Fourth Amendment protection, detailed profiles of individuals could be created.[316]

These systems are a source of great concern among civil rights groups concerning the potential impact they have on personal privacy.[317] Despite the fact that the MATRIX program used records that were commonly available to law enforcement, the program drew substantial criticism from privacy advocates.[318] The MATRIX program failed in part due to criticism over the program's handling of privacy concerns.

In its report reviewing the MATRIX program the DHS Privacy Office noted:

> …the MATRIX pilot project was undermined, and ultimately halted, in large part because it did not have a comprehensive privacy policy from the outset to provide transparency about the project's purpose and practices and protect against mission creep or abuse. The recommendations of the Privacy Office rest on the basic premise that information programs such as the MATRIX pilot project can protect privacy, while increasing homeland security. Building privacy into the architecture of an information program can help ensure that the program achieves its objectives while safeguarding individual privacy.[319]

---

315 Krouse, The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project.

316 McMahon, "Counterterrorism Technology and Privacy," 50; and American Civil Liberties Union, "MATRIX: Myths and Reality," http://www.aclu.org/privacy/spying/14999res20040210.html (accessed February 24, 2007).

317 American Civil Liberties Union, *Data Mining Moves into the States*, http://www.aclu.org/privacy/spying/15694res20031030.html (accessed January 26, 2008).

318 American Civil Liberties Union, *MATRIX Myths and Realities*, http://www.aclu.org/privacy/spying/14999res20040210.html (accessed January 26, 2008).

319 U. S. Dept. of Homeland Security, Privacy Office, *Report to the Public Concerning the Multi-State Anti-Terrorism Exchange (MATRIX) Pilot Program*, 5.

The failure of the MATRIX pilot to properly address perceived privacy concerns was a costly one. The project involved an expenditure of $12 million in federal funds. That funding included $4 million from the Department of Justice and $8 million from DHS. Before the project concluded, it was being piloted in 16 states covering half the U.S. population.[320]

Unlike Secure Flight and MATRIX, which have not left the pilot stage, the FBI is operating a complex computer based analysis system through its Carnivore program. As noted above Carnivore enables the FBI to track activity of a person on the internet. However the program has many other features.

> Carnivore is a device capable of collecting and monitoring all online activities from e-mail to web surfing at a particular Internet service provider (ISP). [citation omitted] According to the FBI, Carnivore would be configured so that it could return certain sought-after information. [citation omitted] It would accomplish this by capturing all of the information that passes through an ISP, and then extracting only the sought-after information. [citation omitted] For example, if the FBI sought to determine with whom a particular individual was corresponding via e-mail, Carnivore could be configured to "filter out" all other information, including the content of that individual's e-mail. [citation omitted] While it would chew all the information that came through the Internet, it would only digest the sought-after information. Carnivore, therefore, can be programmed to limit the information viewed by human eyes. [citation omitted] In many respects, Carnivore is the mirror image of the net-wide search. Instead of "going out" onto the net to search for information, however, the device collects information as it passes through one of the Internet's many gateways. Like an information roadblock, it screens all traffic, but pulls over only the data packets it has been programmed to capture.[321]

While Carnivore is reportedly used only pursuant to court order, it affords potential access to massive amounts of data.[322] In full collection mode the system not only looks at the addresses of email and net searches, but the contents of those transmissions. Unlike wiretaps where the operators are required to turn off the tapping

---

320 Krouse, The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project.

321 Ku, “Modern Studies in Privacy Law,” 1355.

322 IIT Research Institute, *Independent Technical Review of the Carnivore System.*

equipment when a conversation is determined to be outside scope of the court ordered overhear, Carnivore electronically records all the information.[323] The Carnivore system demonstrates a powerful capacity to store and manipulate massive amounts of data.

Privacy concerns over the Carnivore program came to the fore in the wake of a July 2000 article in the Wall Street Journal and resulted in a congressionally conducted hearing and an independent review of the system by the Illinois Institute of Technology Research Institute (IITRI).[324] While the IITRI report concluded that the Carnivore program could be operated within constitutional guidelines, it did note the power of the program with respect to data collection.[325] The IITRI report observes that "[w]hile the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors."[326] Among the IITRI report's recommendations were: separating Carnivore into two versions, one for full collection and the other simply to monitor address information, like a pen register; and improvements to enhance the audit and compliance features of the program to ensure against misuse.[327] Commentators note that despite the fact the IITRI report recommended some changes to Carnivore, the highly redacted report has left many critics skeptical of the program.[328] Subsequent to the IIRTI report's publication, the "Carnivore" program's name was changed to "DCS 1000." [329]

One of the more recent government forays into the area of using computer technology to analyze massive streams of data is the DHS' ADVISE project. ADVISE which stands for Analysis Dissemination, Visualization, Insight, and Semantic Enhancement is a massive computer program to monitor computer data about

---

[323] Segura, "Is Carnivore Devouring Your Privacy?" 236.

[324] Ibid., 233.

[325] IIT Research Institute, *Independent Technical Review of the Carnivore System.*

[326] Ibid.

[327] Ibid.

[328] Maricela Segura, "Is Carnivore Devouring Your Privacy?" 239.

[329] Jim Wolfe, "Carnivore Gets a New Name," *Reuters*, February 14, 2001, http://www.metrostate.com/library/stories/01/feb/msnbc.htm (accessed January 26, 2008).

individuals.[330] ADVISE is a data mining technology that accesses a wide range of data bases to identify threat behavior.[331] As DHS describes the ADVISE program:

> The ADVISE pilot initiatives use a data mining approach to glean insights from large amounts of data across various sources. Data mining is the process of knowledge discovery and predictive modeling and analytics, traditionally involving the identification of patterns and relationships from databases.[citation omitted] Data mining has been used successfully for a number of years in the private and public sectors for a broad range of applications.[332]

In that respect ADVISE seems to combine the aspects of systems like Carnivore, MATRIX and Secure Flight into one super computer program to identify suspect conduct.

At the time of the 2006 Christian Science Monitor story about this program it was noted that DHS had provided little information about the program.[333] Subsequent audits of the ADVISE program may provide some insight into the absence of information. It appears that the ADVISE program which was created in the Science and Technology Directorate of DHS failed to coordinate development with the DHS Privacy Office. The results were fatal to continuation of the ADVISE pilot program. The DHS Inspector General's Report notes:

> S&T planning and management activities for ADVISE have been insufficient to support effective implementation of the program. … Program managers also did not address privacy impacts before implementing three pilot initiatives to support ADVISE. DHS has discontinued its three ADVISE pilot programs, pending completion of such privacy assessments.[334]

---

330 Mark Clayton, "US Plans Massive Data Sweep," *Christian Science Monitor*, February 9, 2006, http://www.csmonitor.com/2006/0209/p01s02-uspo.html (accessed January 27, 2008).

331 Ibid.

332 U. S. Dept. of Homeland Security, Office of the Inspector General, *ADVISE Could Support Intelligence Analysis More Effectively*, July 2, 2007, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-56_Jun07.pdf (accessed January 27, 2008).

333 Clayton, "US Plans Massive Data Sweep."

334 U. S. Dept. of Homeland Security, Office of the Inspector General, *ADVISE Could Support Intelligence Analysis More Effectively,* 8.

Suspension of a massive computer surveillance project in the face of privacy concerns should have come as no surprise to DAH administrators. As the DHS Inspector General's Report observes:

> Due to the ease with which automated systems can be used to gather and analyze large amounts of previously isolated data, a number of concerns about potential misuse of personally identifiable information have been raised. Prior federal data mining efforts faced challenges in balancing the benefits and risks of this activity. For example, the Total Information Awareness program, a Department of Defense research and development data mining program to defend against the threat of terrorism, faced considerable negative publicity and was ultimately shut down by the Congress due to privacy concerns.[335]

C. SUMMARY

The four computer-based surveillance data analysis systems outlined above provide some obvious lessons for administrators regarding developing digital technology. Primarily, these systems indicate how powerful computer based systems are at manipulating large amounts of information. As the Secure Flight, MATRIX and ADVISE examples illustrate, data can be aggregated and inter-related over a wide range of activities. While such databases present a number of prospective benefits for law enforcement, they also raise the prospect of potential abuse.

Secondly, the construction and operation of these databases will engender significant opposition from privacy advocacy groups. As the MATRIX program demonstrates, that opposition can come even when the information utilized in the database is "public" information that is already routinely accessed by governmental entities. The power of these systems and their potential for abuse require attention to privacy protections. The failure to do so may result in project cancellation and reformulation. The postponement of the ADVISE pilot demonstrates, the importance of incorporating privacy considerations early in the planning process. Moreover, as Carnivore demonstrates calls for additional privacy protections can even occur in

[335] U. S. Dept. of Homeland Security, Office of the Inspector General, *ADVISE Could Support Intelligence Analysis More Effectively,* 6.

programs that are administered under court supervision. The placement of access control and accountability mechanisms into complex surveillance database management is crucial.

The failure to adequately address privacy management in the operation of surveillance databases can be quite costly. As noted above the federal government invested some $12 million in the now disbanded MATRIX system. The Electronic Privacy Information Center (EPIC), a privacy advocacy group, reports that the TSA has allocated $38 million in federal fiscal year 2008 for Secure Flight. This amount in addition to the $144 million expended since 2004.[336] This sum is in addition to the funds allocated for CAPPS II. All these federal funds have been expended for computerized analytic systems that have yet to proceed out of the pilot stage. The ADVISE program with a reported cost of $42 million to date is also on hold.[337] Yet the cost should not only be measured in dollars. The failure to accommodate privacy concerns has resulted in postponement, and in some cases, elimination of programs that had potential to assist government in addressing terror threats. Moreover, as the CAPPS II experience demonstrates, the failure to properly account for privacy concerns may prove to be an impediment to international cooperation.

Perhaps the most significant lesson that can be drawn from analysis of the Carnivore, ADVISE, Secure Flight, and MATRIX systems is the fact that that where there is commitment to privacy the programs are moving forward. The Carnivore program, while perhaps not perfect, has a much greater degree of protection in place. Although it should be noted that even where the application of the technology is controlled by a court supervised order, there is a need for privacy protections to be an integral part of operational policies and procedures.

---

[336] Electronic Privacy Information Center (EPIC), "Spotlight on Surveillance: Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved," *EPIC Website*, August 2007, http://epic.org/privacy/surveillance/spotlight/0807/default.html (accessed January 26, 2008).

[337] U. S. Dept. of Homeland Security, Office of the Inspector General, *ADVISE Could Support Intelligence Analysis More Effectively*, 7.

VI. FOREIGN APPROACHES TO PRIVACY PROTECTION

As many jurisdictions in the United States look to develop enhanced surveillance systems to deal with complex problems of homeland security, crime, and even traffic management, the experience of the United Kingdom and on the European Continent in governance of those systems may prove instructive. This is particularly true with respect to addressing privacy concerns in system operation. Moreover, as the U.S. seeks to engage with the United Kingdom and other European partners to combat the terror threat through the sharing of information about individuals, understanding and meeting the privacy concerns of those nations will facilitate information flow.

Examining debate, or perhaps more appropriately in countries like the UK, the absence of debate, over the implementation of CCTV systems demonstrates different philosophies of how those systems should be operated and their relationship to protecting elements of individual privacy. Comparing these philosophic differences, the governance structures developed to effectuate them and the effect they have on CCTV programs can help U.S. policymakers better understand how privacy oriented regulation will influence American use of CCTV. It can also provide a roadmap for addressing legitimate privacy concerns and avoiding potential roadblocks to the successful implementation of CCTV programs.

A. DEVELOPMENT OF CCTV IN THE UNITED KINGDOM

The United Kingdom has perhaps the most highly developed camera system in the world. Beginning in 1993, the United Kingdom, in response to an Irish Republican Army attack at Bishopgate in central London, developed a strategy to use CCTV camera surveillance to enhance security of the area. [338] The strategy was to use CCTV surveillance at all entry points into central London to create a "ring of steel" checking the

[338] McCahill and Norris, *CCTV Systems in London*.

license tags of all vehicles entering the area. The project involved not only installing a network of cameras throughout the City, but integrating those cameras with databases containing vehicle registration data.

From these beginnings, the use of CCTV in the United Kingdom has expanded exponentially. The "ring of steel" was subsequently integrated with cameras operating in institutions like banks and offices in London.[339] The expansion of the CCTV network, referred to as "Camerawatch," was the product of a meeting with over 400 organizations involving 373 different systems with over 1200 cameras.[340] Significantly, the U.K.'s CCTV system is a blend of public and private cameras that focus on publicly accessed areas.

The expansion of cameras was not limited to the issue of terrorist prevention in the City center. It has expanded to an extensive network of speed monitoring cameras on roads throughout Great Britain. This network has expanded from a network that produced 300,000 enforcement actions in 1996 to over two million actions in 2004.[341] In addition to enhancing traffic safety, this increase in enforcement activity raises over 113 million pounds in revenue per year. Significantly, just as the network of cameras has expanded the British government has also sought to expand its capabilities in reading the license registration of vehicles from thirty-five million reads per day to fifty million by 2008.[342]

Expansion of the camera system in the United Kingdom is a high priority of the government. Throughout the 1990s, the government spent over 78 percent of the available funds for crime prevention on CCTV systems,[343] but funding for camera initiatives has not come solely from the government. For example, in the period from

---

339 McCahill and Norris, *CCTV Systems in London*.

340 Ibid.

341 Kristie Ball and David Murakami Wood, eds., *A Report on the Surveillance Society: Summary Report*, Report for the Information Commissioner, by the Surveillance Studies Network (London, United Kingdom 2006), http://www.privacyconference2006.co.uk/files/report_eng.pdf (accessed September 16, 2007).

342 Ibid.

343 Ibid.

1994 to 1999 the government's "CCTV Challenge" generated 31 million pounds in government funds with 58 million pounds of private funds to install some 580 camera systems.[344]

The result of the efforts in the United Kingdom is the development of perhaps the most sophisticated camera networks in the world. Current estimates place the camera coverage in the United Kingdom at as many as 4.2 million cameras. This amounts to one camera for every 14 people in the country.[345]

The increase in surveillance capability through use of CCTV cameras parallels developments in other areas of surveillance technology like, biometrics, GPS and RFID. Developments in these tracking and monitoring technologies, combined with enhanced ability to integrate these data sources through digitization and computer technology, has caused the British government to implement measures to control the collection and use of surveillance data.

B. DEVELOPMENT OF CCTV IN CONTINENTAL EUROPE

Unlike the United Kingdom, CCTV camera usage on the European continent has to date been significantly less robust. In their work surveying European use of CCTV, Hempel and Topfer, chronicle the use of CCTV in cities in Germany, Denmark, France, Austria, Hungary and Italy as of their studies publication in 2002. [346] That study shows that governmental use of CCTV on the European continent is primarily confined to areas like transit centers (airports, train stations and light rail systems). Other areas commonly covered include government buildings and museums. In the private sphere, CCTV is common in monitoring financial institutions, retail chain stores, gas stations, shopping malls and hospitals. Of 1400 such locations surveyed in six European capitals (including the UK), a third were monitored by CCTV.[347]

---

344 McCahill and Norris, *CCTV in London*, 3.

345 Ball and Wood, *A Report on the Surveillance Society*, 8.

346 Hempel and Topfer, *CCTV in Europe*.

347 Ibid., 60.

While there is common use of CCTV outside the U.K. to monitor critical buildings and centers, the use of CCTV to monitor activity (exclusive of traffic) in public areas like city streets is greatly reduced. While the U.K. was reported by Hempel and Topfer to have 400,000 cameras monitoring such areas in over 500 cities the numbers are much lower on the continent.[348] In 2005, France was reported to have only 40,000 cameras in the public areas.[349] They report 300 towns in France with CCTV systems to monitor public areas and 20 cities in Germany. In some countries like Denmark, there are no CCTV systems in place to conduct surveillance of public streets.[350]

The degree of CCTV utilization does fluctuate significantly between countries. For example, while 40% of the accessible public space studied in the U.K. was monitored by CCTV, that number was only 18 % in Austria.[351] The significantly lower utilization rates for CCTV across Europe is likely due to concerns over privacy and a considerably more well developed body of law on this subject when compared to the U.K. However, in the future, the continental use of CCTV may see some significant expansion. In recent years, the governments in Germany[352] and France[353] have indicated an interest in expanding CCTV surveillance systems, primarily in response to terror threats. In Denmark, the government has opened for public debate the issue of expansion of CCTV coverage to public areas.[354]

While government proposed expansion in Germany is envisioned along current lines of CCTV coverage (at transit centers), the expansion proposed by the French

---

348 Hempel and Topfer, *CCTV in Europe*, 61.

349 Xinhua, "French Parliament Approves Video Surveillance Powers," *Peoples Daily Online*, November 11, 2005, http://english.people.com.cn/200511/25/eng20051125_223757.html (accessed September 28, 2007).

350 Hempel and Topfer, *CCTV in Europe*, 61.

351 Ibid.

352 British Broadcasting Company, "Germany Plans Surveillance Boost," *News*, August 21, 2006, http://news.bbc.co.uk/2/hi/europe/5272638.stm (accessed September 17, 2007).

353 Xinhua, "France to Triple CCTV Surveillance Across the Country," *Peoples Daily Online*, July 27, 2007, http://english.peopledaily.com.cn/90001/90777/6225229.html (March 14, 2008).

354 European Digital Rights, "Public Debate on Draft Anti-Terror Act in Denmark," *EDRI-gram*, European Digital Rights, May 10, 2006, http://www.edri.org/edrigram/number4.9/denmark (accessed September 28, 2007).

government is far greater.[355] In July 2007, the French government announced its intent to triple CCTV coverage across France. The goal of the government is to combat terrorism by covering as much area as possible with CCTV. Video images from the expanded system would be maintained from 48 hours to one week depending on CCTV site.[356] This policy shift represents a departure from the more cautious expansion of CCTV in France that has characterized that country to date.

C. GOVERNANCE OF CCTV SYSTEMS IN THE UNITED KINGDOM

Comparing the U.K.'s experience in CCTV implementation with development in the regulatory environment provides helpful insights not just for the management of CCTV networks themselves, but across the field of information technology. The U.K. system has developed in an environment with little initial regulation.[357] Even now, much of the control constitutes self-regulation with little concentrated central governmental controls.[358]

1. Development of UK Governance

In his work on development of regulation in the U.K., Webster notes three phases in implementation of CCTV.[359] The first phase characterized as the "Era of Innovation" extended from early to mid-1990s.[360] During this period there was little in the way of regulation of CCTV. As CCTV networks began to propagate rapidly in the U.K. in the mid-to-late 1990s use of the systems was largely controlled by self-regulation. Webster

---

355 British Broadcasting Company, "Germany Plans Surveillance Boost."

356 Ibid.

357 Mark Cole, "Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK," *Surveillance and Society*, 2004, 2(2/2), http://www.surveillance-and-society.org/articles2(2)/signage.pdf (accessed September 23, 2007).

358 William R. Webster, "The Diffusion of Closed Circuit Television in the UK," *Surveillance and Society*, 2004, 2(2/3), http://www.surveillance-and-society.org/articles2(2)/diffusion.pdf (accessed September 20, 2007).

359 Ibid., 237.

360 Ibid., 238.

characterizes this as the "Era of Uptake."[361] As CCTV users developed their systems, they developed their own governing rules and began sharing best practices. The national government through the Home Office supported this development through funding programs designed to create partnerships between police and local officials. The final phase outlined in Webster's work is the "Era of Sophistication" from the late 1990's forward.[362] This period is marked by some nonspecific legislation addressing the issue of privacy protection, the development of a CCTV Code of Practice that finds force in the Home Office funding process, and "agreed purpose/working practices /technical standards of systems."[363] The former two measures are government initiatives. The latter measures are products of the self regulation process by camera networks.

a. Co-Regulation and the Code of Practice

This process of regulation both from the government and from the networks themselves is characterized by Webster as "co-regulation." He defines the term as follows:

> Co-regulation implies a development of self-regulation. It implies the coexistence of traditional regulation and self-regulation in such a way that responsibilities about the provision of the technology are shared between the regulating and providing agencies [citations omitted]. Co-regulation therefore implies a new set of relationships in the policy arena, between government, industry and service providers, as all 'stakeholders' are involved in forming and implementing the rules that are to be applied as regulation. Co-regulation also allows for the possibility of formal and legislative regulatory measures. However, instead of formal measures being imposed on service providers it emerges from within the policy environment via negotiation with interested parties in the policy network.

---

361 William R. Webster, "The Diffusion of Closed Circuit Television in the UK," *Surveillance and Society*, 2004, 2(2/3), http://www.surveillance-and-society.org/articles2(2)/diffusion.pdf (accessed September 20, 2007). The DPA was not effective in the UK until March, 2000 (Cole, "Signage and Surveillance," 431).

362 Ibid. The HRA was not effective in the UK until October 2000 (Elizabeth France, CCTV Code of Practice (London, U.K. Government, 2000), http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf (accessed September 23, 2007).

363 Ibid.

It is through this co-regulatory process that the CCTV networks of the UK are being governed.

The three legislative pieces that contribute to this co-regulation system were promulgated largely after the exponential proliferation in CCTV systems had already occurred. Those statutes include: "The Data Protection Act of 1998 (DPA);" "The Human Rights Act 0f 1998 (HRA);" and "The Crime and Disorder Act (CDA)." Importantly, none of those statutes specifically refers to CCTV. The provisions of Article 8 of the HRA only address the privacy implication of CCTV in a general fashion. The article provides generically to protect individual rights to privacy by requiring public agencies to respect those rights. The CDA simply requires police and local authorities to work together to develop and implement crime fighting strategies. It also mandates community consultation and information sharing. While many CCTV systems were implemented pursuant to these strategies, there are no specific CCTV requirements.

Perhaps the most important of the statutes from a regulatory perspective is the DPA. The DPA generally refers to privacy rights of individual in collected data of a personal nature. Any question that CCTV images come under DPA protections was resolved in 2000 with the issuance of specific regulatory guidance. To effectuate the terms of the DPA with respect to CCTV the British Data Protection Commissioner promulgated a CCTV Code of Practice. This Code of Practice is a mechanism for legally enforceable regulation of CCTV under the DPA. In developing the guidance the Data Protection Commissioner noted:

> This Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place. It sets out the measures which must be adopted to comply with the Data Protection Act 1998, and goes on to set out guidance for the following of good data protection practice. The Code makes clear the standards which must be followed to ensure compliance with the Data Protection Act 1998 and then indicates those which are not a strict legal requirement but do represent the following of good practice. [364]

364 France, CCTV Code of Practice.

To ensure compliance with the DPA requirements the Code of Practice sets out to address the following principles for regarding data:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary
- processed in accordance with individuals' rights;
- secure;
- not transferred to countries without adequate protection.[365]

The Code of Practice accomplishes its objectives by providing general standards for implementation of both public and private CCTV systems. These standards address: "Initial Assessment Procedures" (outlining the purpose of the scheme and the persons/organizations responsible for implementation)[366]; "Siting the Cameras" (outlining the process for ensuring camera placement supports scheme design, minimizes unintended impact, and notifies the public of camera placement)[367]; "Quality of Images" (ensuring the image quality can be used for law enforcement purposes)[368]; "Processing the Images" (ensuring proper security during retention periods and destruction in accordance with schedules)[369]; "Disclosure to Third Parties" (limited and only under specified circumstances)[370]; "Access by Data Subjects" (providing data subjects with

365 France, CCTV Code of Practice, 2.

366 Ibid., Part II, 6.

367 Ibid., Part II, 7.

368 Ibid., Part II, 9.

369 Ibid., Part II, 11.

370 Ibid., Part II, 13.

information on the purpose of surveillance and the ability to access their data)[371]; and "Other Rights" (measures to minimize damage caused by data subjects in processing data)[372].

Consistent with Webster's theory of co-regulation, the Data Protection Commissioner notes that the Code of Practice was prepared in consultation with operators of CCTV systems. It was posted in draft on the Commission website for comment before being finalized. Additionally, the Commissioner notes the need to keep the Code under constant review in light of "changing technology."[373]

In addition to the regulation of the CCTV systems provided by the Data Protection Commissioner, regulatory guidance is provided by the following entities: Police Scientific Development Branch (technical advice on camera/system configuration); British Standards Institute (administrative standards for CCTV system operation); Home Office "CCTV Initiative" (funding guidance for support for CCTV systems) ; CCTV User Group (industry designed model practice and procedure guides for CCTV operation); Local Government Information Unit (model code for CCTV operation collected from local governments); and Home Office Research Group (studies of CCTV efficacy). These organizations serve as resources for cities and villages as they develop and implement their CCTV strategies.[374]

While these regulations in the Code of Practice address the major issues of privacy protection, they are not overly restrictive. Perhaps the most burdensome requirements fall in the areas of signage, access by third parties and access by data subjects. As to the first two provisions, efforts at achieving regulatory compliance are questionable.

---

371 France, CCTV Code of Practice, Part II, 15.

372 Ibid., Part II, 17.

373 France, CCTV Code of Practice, 3.

374 Webster, "Diffusion …of Closed Circuit Television in the UK," 243.

b. Signage, Third Party Access, and Subject Access

As to the Signage requirements, the provisions of the Code of Practice are fairly specific. Signs must be clearly "legible" and "visible"[375] notifying persons they are entering an area monitored by CCTV equipment.[376] The signage is required to advise individuals the purpose of the CCTV scheme, the person or organization operating it and contact information. While it has some exception for signage the operator must make a factual showing that such covert surveillance is required. Such activity is anticipated to be limited in scope and duration.[377]

While the regulations are quite clear, strict regulatory enforcement of the signage requirements appears to be lacking. In his work examining the issue of signage and CCTV surveillance in London, Cole, notes that only a quarter of the signs observed meet the Code of Practice requirements. This may be a function of the fact that the Code of Practice did not come into effect until well after many of London's CCTV systems had been activated. It also may be a function of what Gras refers to in her work as a lack of "*effective* regulation.[378]" With regard to the UK's regulatory structure Gras observes:

> Regulatory bodies in the UK notoriously lack resources and are reliant upon the good-will and co-operation of those they are regulating and their activities are frequently triggered by a specific complaint…[citation omitted]. These issues become all the more relevant in the data protection field where breaches of regulation will not leave any physical trace.[379]

Aside from the issue of regulatory compliance, there is some question about the real purpose of the signage requirements. Cole posits in his work that the signage requirement is not really a measure to protect individual rights. Rather, it is a method to enhance the designed effect of government to alter public conduct. Cole observes:

---

375 France, Code of Practice, Part II, 8.

376 Ibid., Part II, 7.

377 France, Code of Practice, Part II,. 8.

378 Marianne L. Gras, "The Legal Regulation of CCTV in Europe," *Surveillance and Society*, 2004, 2(2/2), www.surveillance-and-society.org/articles2(2)/regulation.pdf (accessed September 23, 2007).

379 Ibid.

> At a more theoretical level, it is the view of this paper that the signage used to advise of the presence of CCTV – whether it complies with the code or not – has another and altogether different effect, namely, it [sic] emphasizes the existence of surveillance and thereby amplifies its effect. In fact, the signage that does not comply with the code might be said to have greater influence in this respect.[380]

In addition to the question of UK compliance with its own signage requirements in the operation of the system there also questions of compliance with the HRA. Under Article 8, privacy protection may well apply to certain aspects of public conduct, particularly where a photographic record was retained. In the case of *Peck v. United Kingdom*,[381] the European Commission on Human Rights (ECHR) concluded a government release of CCTV images of a person attempting suicide in public constituted a violation of Article 8 of the HRA.

In reaching its conclusions the ECHR noted that it had previously concluded that the actions of merely monitoring conduct in public places through the application of CCTV did not implicate individual privacy concerns. However, the court noted that recording and release of data regarding individual conduct raised different issues. As to the release of that data, the ECHR found clear impairment of protected privacy interests. In a unanimous opinion, the ECHR held that the actions of the local city council in releasing the data images of Mr. Peck's 1995 suicide attempt to the local media was a violation of protected privacy rights. [382]

Whether and to what extent the ECHR policy will affect UK policy with respect to cameras remains to be seen. Gallagher notes that even after the *Peck* decision, the media continues to broadcast images captured on CCTV. He also observes that advisories sent to police agencies and the Home Office' webpage continue to suggest that CCTV surveillance in public places affects no protected privacy interest.[383]

---

380 Cole, "Signage and Surveillance," 218.

381 *Peck v. United Kingdom*, 36 E.H.R.R. 41 (2003).

382 Caoilfhion Gallagher, "CCTV and Human Rights: The Fish and the Bicycle? An Examination of *Peck v. United Kingdom* (2003) 36 E.H.R.R. 41," *Surveillance and Society*, 2004, 2(2/3), http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf (accessed September 23, 2007).

383 Ibid., 285-6.

With regard to individual subject access to the CCTV system, the Code of Practice clearly provides comprehensive rights for subject access to CCTV maintained about them. In practice, these provisions seem largely underutilized. As the Data Protection Commissioner notes in the Full Report on the "Surveillance Society":

> This right requires a 'data controller' to provide to each individual information on all the data they hold on her and details of any processing it has been subject to. This goes some way to rectifying the asymmetry of power of the surveillance gaze, particularly where consent to use our personal data has been implied, rather than positively granted. However, large numbers of people do not know their rights, fail to exercise them, and receive little help from others in doing so.[384]

Given the extensive requirements for subject access, it is questionable whether such provisions could be complied with if there were a high volume of individual requests for information on data collection by the CCTV system.

c. Public Opinion

Despite the issues of instances of non-compliance with the regulatory requirements, public support for CCTV systems seems to remain high. Perhaps these attitudes even encourage some of the questionable government conduct. All the commentators that have evaluated the issue have concluded that British public solidly accepts video surveillance. In a recent Home Office Study on the matter it was noted that between 69% and 96% of the surveyed populations with CCTV favored its use. [385] Members of the public concerned about civil liberties abuses were rather low between 12% and 19%. While there was a small decrease in support of CCTV cameras after installation, that decrease seemed to be a function of concerns about efficacy rather than ones related to civil liberties.[386]

---

[384] Wood, *A Report on the Surveillance Society*.

[385] Martin Gill and Angela Spriggs, "Assessing the Impact of CCTV," *Home Office Research Study 29*, (London: Home Office Research, Development and Statistics Directorate, February 2005), http://www.homeoffice.gov.uk/rds/surveys/hors292_survey.html (accessed September 25, 2007).

[386] Ibid., 58.

2. Conclusions

While the U.K.'s experience in implementation of CCTV systems has not been without criticism both from the perspectives of efficacy and civil liberty implications, the system remains strong, popular and is expanding. The U.K. has moved from a totally unregulated system to one that relies extensively on the concept of co-regulation. The Full Report on the "Surveillance Society" notes that as the CCTV systems develop and integrate with other technologies that impact individual privacy there may be a need to enhance privacy protections, perhaps through the requirement of "privacy impact assessments"[387] or "surveillance impact assessment."[388] These processes are akin to environmental impact assessments except they are focused on the privacy and societal effects of the implementation of surveillance systems. The Report also notes that the U.K. should look to developments in other countries for best practices in regulating rapidly developing surveillance technology.[389] In this regard, at least from the perspective of the Data Protection Commissioner, the development of future systems may be closer to European models that place greater focus on CCTV system impact.

D. CONTINENTAL EUROPEAN CCTV GOVERNANCE STRATEGIES

While each European country has slightly differing models of governance, they all seem to follow a general scheme focused on privacy protection. Examining the German and French governance systems, demonstrates an approach to CCTV that is fundamentally different from the UK scheme. Both systems have more restrictive approaches to the use of CCTV in public places. The German system is generally more restrictive than the French. As noted above, in response to potential terrorist threats, both systems are moving to expand the use of CCTV. The French seem to be taking steps to alter their governance structures to accommodate this. The Germans seem only to be expanding CCTV in the areas in which it currently operates.

---

387 Wood, *A Report on the Surveillance Society,* 89-97.

388 Ibid., 97-99.

389 Ibid., 86-87.

1. Germany

Perhaps the most extreme protections for privacy are found in Germany. In fact, Privacy International, an international privacy rights advocacy group, rates Germany as the most protective nation for privacy rights.[390] Under German law there is a strong constitutional argument that "…mere observation of a scene in which no individual is identifiable via camera, is an interference with a German citizen's basic rights and therefore requires specific legislation."[391] Such provisions exceed the protections of the HRA, which as noted in the *Peck* case, extends no protections to the mere surveillance by camera of conduct in public places. The effect of the German constitutional provisions is to make public camera surveillance arguably unlawful in the absence of specific statutory authority permitting it.

Gras notes most of the German states (Länder) have enacted legislation to permit the use of CCTV systems by police. However these 16 Länder codes vary in the authority they grant to police and local authorities. Those differences are characterized as follows:

> a) Länder with no legal basis for CCTV surveillance as British people know it, b) states allowing video surveillance by the police in certain, relatively well-defined situations and c) states with a wider ranging legal permit for police and occasionally other public authorities, to install CCTV systems, to make recordings and to store these for a relatively long period of time [citation omitted].[392]

This legal structure not only makes for uneven application of CCTV systems across Germany, it also constrains system implementation because positive legislative permissions are required before systems can be implemented.

In addition to requiring specific statutory authority before a CCTV system can be implemented, the German constitution requires that concepts of proportionality and

---

390 Privacy International, National Privacy Ranking 2006-European Union and Leading Surveillance Societies, 2006, http://www.privacyinternational.org/survey/phr2005/phr2005spread.jpg (March 14, 2008).

391 Gras, "Legal Regulation of CCTV in Europe," 219.

392 Ibid.

appropriateness be met. Proportionality requires that the level of intrusion be gauged in accordance with the problem to be addressed. CCTV designed to address minor disorder problems would likely not withstand scrutiny under this constitutional provision.[393] The appropriateness requirement means that the use of CCTV cameras must be shown to be effective against the type of harm sought to be remedied. Moreover, this principle of German constitutional law requires that the method be "… the mildest possible method in the sense that it interferes as little as possible with the rights of those affected."[394]

The requirements of proportionality and appropriateness have served to compel police agencies seeking to install CCTV systems to engage in crime analysis prior to placing the systems. Gras, speculates that while such analysis may not be mandated by law, it has made police administrators cautious in implementing systems. This, in turn, has kept German systems relatively small and few in number.[395]

In addition to placing restrictions on government use of cameras in public areas, the German constitutional protections also serve to restrict private camera use. In addressing the legitimate concerns of property owners, German law recognizes differentiation in protections that should be afforded personal privacy expectations. In essence, German law recognizes three levels or spheres of privacy including intimacy—which is afforded absolute protection. The two other spheres, the private and the individual spheres, are subject to some protections but those are absolute. In cases where there is to be allowance for interference with a privacy right, the actions of the private party in installing the CCTV must be proportional to the harm sought to be prevented.[396]

In measuring proportionality under German law, certain factors are important to consider. Surveillance limited to a certain defined space is more likely to be found acceptable, if the surveillance is placed in such a way and marked so that persons not choosing to be observed can avoid observation. While some systems such as those at train stations cannot be avoided, without forgoing the right to travel, the ability of persons

393 Gras, "Legal Regulation of CCTV in Europe," 221.

394 Ibid.

395 Gras, "Legal Regulation of CCTV in Europe."

396 Ibid., 219-20.

to protect their privacy is important. This, of course, means that there needs to be signage or some form of notification of the presence of CCTV.[397]

Where the requirements of proportionality, particularly notice, have not been met, German courts have been reluctant to use the CCTV evidence. For example, in one case where a retail customer was charged with theft by changing price tags on merchandise to secure lower prices, the court declined to admit the CCTV films. The store's use of CCTV without notice to the customers was determined to be an action "…to secure evidence of a crime and not to prevent damage to the owner."[398] Because the CCTV usage did not advance the interest of preventing damage, its use was deemed outweighed by privacy concerns.

While Germany is experiencing pressures to expand its CCTV networks, its commitment to privacy protection remains strong. The continuing focus on privacy has undoubtedly contributed to the small size of German CCTV networks. Even where Germany has announced plans to expand surveillance that expansion is limited to the public areas, like transportation centers, where it is already permitted and relatively uncontroversial.[399]

2. France

While French protections for privacy are less than those provided under German law, there are still significant impediments to the operation of CCTV systems in France. Under the provisions of French legal decrees in 1995 and 1996, prior approval must be secured from the local prefect in each of France's administrative regions prior to installations of non-police CCTV cameras. Decisions are made through the following process:

---

397 Gras, "Legal Regulation of CCTV in Europe," 220.

398 Gras, "Legal Regulation of CCTV in Europe."

399 British Broadcasting Company, Germany Plans Surveillance Boost, http://news.bbc.co.uk/2/hi/europe/5272638.stm (accessed September 17, 2007).

> In making this decision, the Prefect must consult a local committee, the CDV, which is presided over by a judge. Alongside the judge, the CDV is manned by another magistrate, a representative elected by the local trade chamber, an elected politician such as the mayor and a person with technical knowledge (who may, however, not be a serving police officer). Their decision is made by majority vote and is a recommendation to the Prefect, which he or she will, however, almost always go by, because the CDV is more competent to make the decision than he or she is. The Prefect's decision is final but can be contested before an administrative court (i.e., is subject to judicial review). An applicant must prove that the area one wishes to protect by CCTV is an object particularly liable to theft or attack.[400]

Under this process, some 38,250 CCTV installations were approved by 1999. Gras notes that in 1999 alone 4500 requests were received with 4200 approved. However, most of the installations were for locations like banks, gas stations, and retail stores that had traditionally operated such camera systems. Gras concludes that while the French legal system could be successful in regulating CCTV, it is not clear how the system will work especially since police cameras are excluded.[401]

French restrictions on CCTV installation and usage may well be eroded by recent changes in French law. In September 2005, anti-terrorism legislation was introduced to expand the ability to use CCTV. One measure would permit CCTV surveillance of public streets in the vicinity of potential terrorist targets, like synagogues, mosques, power plants and transportation centers.[402] Under the new law, CCTV images would be retained for one month.[403] The legislation also served to undermine the process of requiring licensure for CCTV systems operated in public places by private parties. Under the provisions of the new law, private parties would be permitted to install CCTV

---

400 Gras, "Legal Regulation of CCTV in Europe," 222-23.

401 Gras, "Legal Regulation of CCTV in Europe," 223.

402 Meryem Marzouki, "New French Anti-Terrorism Surveillance Plan," *EDRI-gram*, European Digital Rights, September 8, 2005, http://www.edri.org/edrigram/number3.18/France (accessed September 28, 2007); and European Digital Rights, "France Adopts Anti-Terrorism Law," *EDRI-gram*, European Digital Rights, January 18, 2006, http://www.edri.org/edrigram/number4.1/frenchlaw (accessed September 28, 2007).

403 Ibid.

> in public places "likely to be exposed to terrorist acts", and in places open to the public when they are "particularly exposed to risks of aggression or theft". Obviously, this covers almost any public or privately-owned place, including shops. In case of emergency, CCTV cameras may be installed prior to any [sic] authorisation.[404]

The French Constitutional Court upheld the constitutionality of these measures which greatly undermine the protections afforded by the CDV process.[405] Opposing this legislation proposed by the Interior Ministry was a collection of groups including: The French Data Protection Authority; the French Human Rights League and the trade union representing lawyers and magistrates.[406]

The recent developments in French law evidence a dissatisfaction with constraints placed on CCTV development. Despite opposition from civil rights groups and even those agencies of the French government charged with enforcement of data protection laws, these changes reflect a movement toward a less regulated model of CCTV system implementation. Despite this opposition, public support seems to favor expansion. Recent polling data indicates that some 73% of the population support the government proposals to dramatically increase CCTV in France.[407]

The changes in the French system in governance and the public opinion favoring the use of CCTV will likely usher in a significant expansion of CCTV systems. Less clear is the issue of the use of that data. Like the U.K., France is bound by privacy and data protection laws. The changes in French law may serve to increase the coverage of CCTV, but expansion in the use of data gathered from CCTV is less clear. The time frames for data retention remain conspicuously short.

---

404 Meryem Marzouki, "Urgency Procedure for Draft French Anti-Terrorism Law," *EDRI-gram*, European Digital Rights, December 5, 2005, http://www.edri.org/edrigram/number3.24/French_antiterror (accessed September 28, 2007).

405 European Digital Rights, "French Adopts Anti-Terror Law Not Anti-Constitutional," *EDRI-gram*, European Digital Rights, February 2, 2006, http://www.edri.org/edrigram/number4.2/frenchlaw (accessed September 28, 2007).

406 Marzouki, Urgency Procedure for Draft Anti-Terrorism Law.

407 Angus Reid, "French Want Increase in Surveillance Cameras," *Prison Planet.com*, September 6, 2007, http://www.prisonplanet.com/articles/september2007/060907Cameras.htm (accessed September 28, 2007).

3. Conclusions

In contrast to the more freewheeling approach in the U.K., the continental European systems, exemplified by France and Germany, are ones predominated by legislative approaches for regulation. They begin from a perspective that CCTV is intrusive and constitutes an interference with protected privacy interests. The systems seem to have differing perspectives on the degree of interference. While as in the U.K., the continental European countries all adopt the DPA and HRA, the legal traditions in those countries is to interpret the provisions of those acts more strictly than in the U.K. Moreover, the protections of those acts are bolstered by laws that enhance individual privacy protections.

The net result of the continental European scheme of legislative regulation to protect privacy rights has been to restrict the use of CCTV. However, in recent years, as governments have grown increasingly concerned over the threat of terrorism, some countries are reviewing the restrictive nature of their privacy laws and carving out exemptions to permit CCTV expansion. France, and to a lesser extent Germany, are examples of this trend. This movement raises a larger question of whether legislative or statutory based solutions are sufficiently flexible to address rapidly developing technology like CCTV.

E. LESSONS LEARNED FOR GOVERNANCE OF U.S. SURVEILLANCE SYSTEMS

The governance trends in the U.K. and on the European Continent can probably best be characterized as systems that initiated development from almost completely opposite points and are slowly moving toward a point of convergence. The governance in the U.K. which started out essentially where the U.S. currently rests began with little or no systematic protections for privacy in public and with no legislative requirements for CCTV governance. It has moved to a co-regulated system that has some general legislative protection for privacy. In contrast, the continental European systems, like France and Germany, have started from a point where privacy protections have been extensive. The French are apparently moving to embrace more relaxed regulation of

public surveillance systems that will allow for greater surveillance of streets parks and other public locations. Similarly, it appears that German authorities are looking to expand CCTV networks, but primarily at locations like transportation hubs.

1. Learning from the U.K.

Perhaps the principal lesson that American policymakers can draw from experiences in the U.K. is that a flexible system of co-regulation may promise the most responsive way to address competing concerns of privacy and security in the development of rapidly growing technology like CCTV. While the initial unregulated approach utilized by the U.K. afforded an opportunity for rapid expansion of CCTV systems, the need for some regulation became apparent. The scheme of working with CCTV developers and users in identifying best practices as a basis for regulation seems to be an effective way to manage rapidly developing technology. The failure to develop this scheme early in the U.K.'s development process may mean that systems that cannot be made to conform to the new regulations may need to be dismantled. While there is no evidence of this to date, the late development of a regulatory scheme creates that risk.

The guidelines in the U.K.'s CCTV Code of Practice might provide a good starting point for U.S. policy development. These regulations seem to address many of the privacy concerns raised by CCTV systems. The general nature of the Code of Practices provides great latitude to local governments in system development. It allows for the development of best practices that can be shared among CCTV system developers and users. While some of the concepts may have to be adjusted to conform to legislative realities in the U.S., the solutions envisioned by the Code of Practice may result in the rethinking of some U.S. legal concepts. For example, development of policies to protect individual privacy may intersect with issues of freedom of information. Even in the U.K. where privacy was not initially viewed as a legal requirement, similar to current jurisprudence in the U.S., there is a growing sense that CCTV and the growing capability for surveillance of activity in public space has some implication on privacy. Addressing those concerns is essential to continued expansion of surveillance technology in public space.

The ability of third parties to access public surveillance data may need to be more restricted as it is under the U.K.'s Code of Practice. Such a concept would require revision of provisions of many freedom of information laws in the U.S. which make no distinction between requestors who are the subject of data and other third party requestors. Additionally, the distinction between actions viewed on camera and the recording of those actions with respect to privacy protection may be instructive for the U.S.

Also instructive from the U.K. perspective is the system by which regulation can be implemented. As in the U.K., much of the development of public CCTV systems is funded by grant programs issued by central government authorities. In the U.K., it is the Home Office. In the U.S., the primary grant funding source is the Department of Homeland Security (DHS). Like the Home Office, DHS can use its funding authority to impose technical and procedural requirements on fund recipients in the operation of their CCTV systems. Careful use of this authority can develop a co-regulation environment in the U.S. that has the same flexibility as in the U.K.

In addition to the scale of the scope of the U.K. CCTV system, the U.S. can also draw lessons for the versatility of that system to address a range of societal issues. While anti-terrorism is certainly a major concern driving the implementation of CCTV systems, they also have differing uses in the U.K. Ordinary crime control is clearly one of those uses. While the success of CCTV in crime control has not been clearly demonstrated, the public confidence in those measures clearly remains high. Certainly, the enhanced community perceptions of safety are of value. The use of such systems to enhance the economy of flagging intercity shopping areas is one tangible example of the benefits of such community confidence.

In addition to anti-terrorism and crime control the traffic control and enforcement use of cameras is also extremely high in the U.K. This serves to not only enhance public safety, but also provides a significant government revenue stream through enforcement activity. Such a use in the U.S., providing similar revenue benefits, would afford government a revenue stream to support CCTV system maintenance and expansion.

A final lesson from the U.K. would be in the power of the private sector cooperation in the establishment of comprehensive CCTV networks. The CCTV systems in the U.K., have from the start been cooperative arrangements between government and the private sector. This doubtless has allowed increased expansion with limited investment of government dollars. While such a system certainly raise information and privacy concerns for the U.S., it also offers the prospect of increased surveillance capacity without government being forced to bear the entire burden.

2. Learning from the Continental Experience

The experience of the continental countries like France and Germany in recognizing potential privacy impact in the data collected through CCTV and the need to protect it provides a valuable example for the U.S. It is a lesson currently being learned in the U.K. While the U.K. seems to strongly maintain the notion that activity on any given day in the public space is afforded no protection from government scrutiny through CCTV, the recording and subsequent use of that data does present issues long recognized on the continent. This is exactly the lesson of the *Peck* case which follows strongly in the legal traditions of the European Continent.

The emphasis on privacy protection, particularly in German law, will help attune U.S. policymakers to the potential long term impacts on individual privacy rights of data gathered from comprehensive CCTV systems. This concern over data, rather than simply the surveillance systems themselves, is an important concept. This is particularly true as surveillance systems become more advanced. Addressing the use of compiled data gathered through surveillance requires a comprehensive approach to the issue of CCTV use, as well as the use of other technology enhanced surveillance techniques.

The German concept of spheres of privacy subject to protection in differing manners provides an interesting analytic model for assessing both surveillance techniques and measures for preserving and safeguarding data. Acceptance of differing levels of privacy subject to differing levels of protection is not inconsistent with American jurisprudence. These concepts could be easily incorporated into legislative or regulatory schemes for CCTV governance.

With regard to the process of governance, the legislative approaches taken in both Germany and France, demonstrate the constraining nature such approach has on technology. Unlike the system in the U.K. which has greater ability to adapt to the change in technology, the continental systems do not allow for rapid response to technology changes. Doubtless that is why the CCTV systems on the Continent are significantly underdeveloped when compared to the U.K. The recent movement by the French government away from its legislatively imposed control system for CCTV placement suggests the government perceives it is interfering with legitimate anti-terror tools. Requirements for advance showing of such benefits will likely doom most CCTV projects. The recent French legislative changes seem to be an expression of understanding that in some areas CCTV surveillance is acceptable without further evidence or support. However, the relatively short retention period for gathered data suggests a balance with concerns over data protections.

3. Summary

The experiences from the U.K. and Europe provide some interesting perspectives on how CCTV can be managed in the U.S. They provide insights on issues like:

- Privacy in public places and in the collection and maintenance of CCTV surveillance data.
- Rights of data subjects
  - Notice (signage)
  - Access
- Rights of the public and third parties
- Regulatory versus legislative governance of CCTV
- Management of CCTV camera installation (appropriate siting and uses for CCTV)

As jurisdictions in the U.S. move forward with their programs for development of CCTV, these issues will need to be addressed. Moreover, these issues are common to a range of technologies developed and applicable to surveillance of public activity. While discussions of the experiences and solutions developed in the U.K. and Europe should not

be read to be determinative of the same result in the U.S., the issues are the same and the range of solutions are relatively limited. Thus, by examining the application of policy and its result in foreign contexts, U.S. policymakers will be better able to manage CCTV development in the U.S.

VII. CHICAGO EXPERIENCE IN SURVEILLANCE

Chicago has had a long and checkered history with respect to the issue of surveillance. The experience of the city provides valuable lessons in both the operation of unregulated and over regulated surveillance programs. This experience provides an example of consequences that can befall jurisdictions that do not act to properly govern surveillance programs. It also provides insights into the operation of a large CCTV surveillance system under the provisions of a court sanctioned consent decree.

The story of the surveillance in Chicago is succinctly outlined by the U.S. Court of Appeals. Judge Posner, in the 2001 opinion in *Alliance to End Repression, et al., v. City of Chicago,* observed the following about the history of surveillance in Chicago.

> From the 1920s to the 1970s, the intelligence division of the Chicago Police Department contained a unit nicknamed the "Red Squad" which spied on, infiltrated, and harassed a wide variety of political groups that included but were not limited to left- and right-wing extremists. Most of the groups, including most of the politically extreme groups, were not only lawful, and engaged in expressive activities protected by the First Amendment, but also harmless. The motives of the Red Squad were largely political and ideological, though they included a legitimate concern with genuine threats to public order. Demonstrations against U.S. participation in the Vietnam War that climaxed in the disruption of the Democratic National Convention in Chicago in 1968, race riots in Chicago and other major cities in the same period, and the contemporaneous criminal activities of the Black Panthers, the Weathermen, and Puerto Rican separatists, all against a backdrop of acute racial and Cold War tensions, political assassinations (notably of President Kennedy, Senator Robert Kennedy, and Martin Luther King, Jr.), and communist subversion, fueled a widespread belief in the need for zealous police activity directed against political militants.[408]

Judge Posner later characterized the surveillance program of the City as "organized systemic and protracted."[409]

---

[408] *Alliance to End Repression v. City of Chicago*, 237 F.3d 799, 801 (7th Cir. 2001) (*Alliance II*).

[409] Ibid.

Litigation over Chicago's surveillance practices began with a complaint filed as a class action in November 1974 by a confederation of religious community civil rights and civil liberties groups called the Alliance to End Repression (Alliance).[410] Eleven months later a similar action was filed by the ACLU and the two actions were joined. In all, the actions represented the interests of 24 organizations and 32 individuals. Defendants named in the two suits included the City of Chicago and various city officials.[411] In the seven years of litigation that followed over half a million documents were produced by the City and approximately 100 depositions were taken of city employees and other witnesses. The district court in summarizing the litigation characterized it as "the whole history of this lawsuit is one of vigorous hotly contested litigation."[412]

The unrestrained surveillance activity of the Chicago Police Department was ended in March, 1982, when the City entered into a settlement agreement and an expansive consent decree. That decree provided for extensive regulation on the City's use of investigative techniques. The protections of the consent decree went well beyond the protections afforded by the First Amendment. In fact, the court in approving the settlement and entering the decree noted that legal relief granted went well beyond the "… legal relief that plaintiff would have obtained if the case had gone to trial."[413] Judge Posner later characterized the decree as one containing a "…dizzying array of highly specific restrictions on investigations… ."[414]

The initial consent decree contained restrictions on a range of investigative techniques including the use of electronic technology. The minimization requirements of the decree made the use of any electronic surveillance impossible in the absence of suspicion of criminal conduct. Even in circumstances where the investigation targeted criminal conduct, if it also related in any way to first amendment conduct, as that term

410 *Alliance to end Repression v. City of Chicago*, 561 F. Supp. 537, 539 (N.D. Ill. 1982) (*Alliance I*).

411 Ibid. at 540.

412 Ibid.

413 Ibid. at 541.

414 *Alliance II*, 237 F. 3d at 800.

was broadly defined in the decree, extensive administrative approvals were required for the investigations to be initiated. Documentation collected pursuant to investigations could only be held for a limited period. [415]

The consent decree also contained provisions requiring that notice and training be provided to all employees so they would understand their obligations under the decree. It also provided for internal and independent external compliance audits. Audit results were to be made public.[416]

The restrictive provisions of the consent decree severely curtailed the ability of the City to use surveillance technologies. The City operated under the decree for over 20 years with regular audits being conducted and no significant findings. However as concerns about domestic and international threats increased, it sought to modify the decree. Noting that the provisions of the decree were more restrictive than the provisions of the first amendment, the Seventh Circuit Court of Appeals granted the requested relief in January 2001. In doing so the court noted

> The decree impedes efforts by the police to cope with the problems of today because earlier generations of police coped improperly with the problems of yesterday. Because of what the Red Squad did many years ago, today's Chicago police are fated unless the decree is modified to labor indefinitely under severe handicaps that other American police are free from. First Amendment rights are secure. But under the decree as written and interpreted, the public safety is insecure and the prerogatives of local government scorned. To continue federal judicial micromanagement of local investigations of domestic and international terrorist activities in Chicago is to undermine the federal system and to trifle with the public safety. Every consideration favors modification; the City has made a compelling case for the modification that it seeks.[417]

While the decision freed the City from many of the procedural restrictions of the earlier consent decree, the City remained bound by decree to ensure compliance with first amendment protections in any surveillance activities it conducted. Moreover the failure to meet first amendment requirements would also be punishable under the decree. Also

---

415 *Alliance I*, 561 F. Supp. at 561-70.

416 Ibid.

417 *Alliance II*, 237 F. 3d at 802.

significant to the court was the fact that the City was not seeking to remove the audit requirement from the modified decree. It noted that "…the requirement of outside audits will make it more difficult for the Chicago police than for their counterparts in the other big cities to commit constitutional violations undetected."[418]

Subsequent to the entry of the modified consent decree, the City initiated an expansive camera program. In a recent *Chicago Tribune* editorial, the following observation is made of the camera program.

> Aware of it or not, you stroll and drive through Chicago in the web of a virtual dragnet. City of Chicago cameras monitor you and those around you. How many cameras? The official answer? "In the thousands."
>
> Chicago's five years of experience have established that those cameras can be as effective as they are inhibiting. They're reliable, unbiased witnesses, capable of checking authority as well as those who wrongly accuse authority of misdeeds.[419]

This program was fully implemented under the terms of the modified consent decree with its audit features to protect the first amendment rights of citizens from intrusion by surveillance.

The experience of Chicago provides three significant lessons for policymakers. The first lesson is that unregulated surveillance activity can have disastrous consequences. The conduct of the Chicago Police Department's Red Squad resulted in protracted litigation against the City and entry of a consent decree the severely constrained legitimate police surveillance activity.

The second lesson from the Chicago experience is that complex and restrictive regulation will retard the use of surveillance technology like CCTV. Prior to the modification of the consent decree, little use was made of surveillance technology like

---

418 *Alliance II*, 237 F. 3d at 802.

419 Chicago Tribune Editorial Board, "Wave and Behave," *Chicago Tribune*, February 10, 2008, http://www.chicagotribune.com/news/opinion/chi-0210edit2feb10,0,1048507.story (accessed February 24, 2008).

CCTV except in connection with criminal investigation. As the court noted in *Alliance II*, Chicago operated under "…considerably greater constraints than police officers in other cities."[420]

The final lesson is that some regulation and external oversight to ensure compliance will not impede development of digital sensor systems. Chicago is still operating under a modified decree with the same audit requirements it has had since the mid 1980s. Those restrictions have not impeded progress in developing complex CCTV surveillance network. In fact, the external audit function may well be contributing to the system accountability noted by the *Chicago Tribune* editorial.

[420] Chicago Tribune Editorial Board, "Wave and Behave," *Chicago Tribune*, February 10, 2008, http://www.chicagotribune.com/news/opinion/chi-0210edit2feb10,0,1048507.story (accessed February 24, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSIONS, GOVERNING SURVEILLANCE TECHNOLOGY

The technology assessment in this paper recounts a dizzying array of technological developments that have occurred in recent years in the field of surveillance. Those advances have occurred in both the areas of collection and management of surveillance data. The question confronting citizens and policymakers alike is how to square those developments with existing protections for privacy and assess where there are gaps requiring additional protections. In short, the question is how to govern this growing technological development.

Governance will require a flexible system that can expand and address a range of both collection and analytic tools. While CCTV is the first of the collection technologies to spread across the U.S., it will hardly be the last. The digitization of information allows multiple surveillance platforms to provide information to common or related databases. Developing a method to govern that information is likely the key to a successful governance strategy.

A. PROBLEMS POSED BY TECHNOLOGICAL CHANGE

As a starting point, it is important to consider that the advent of technological development affecting privacy is not something new. Courts, legislatures and administrators have been wrestling with these issues for a long time. Many technologic developments over time have affected how we view privacy and personal space. Those developments have served to reduce the spheres of separation that many have characterized as privacy.

The development of modern modes of transportation issues like trains, cars and airplanes has reduced the physical distances that formerly facilitated seclusion. Development of the telephone has moved communication into areas once thought private and apart. Laws have had to be passed to prevent the unauthorized intrusion of

telemarketers in our homes. The fact that some aspects of technology may limit some of the states of privacy may be acceptable so long as the essential function that privacy provides to a free society is not lost.

Privacy advocates have long warned of the impending danger that technology poses to privacy. Consider the words of Warren and Brandeis writing in the 1890's for the Harvard Law Review:

> Recent inventions and business methods call attention to the next step which must be the protection of the person, and for securing to the individual what Judge Cooley calls "the right to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devises threaten to make good the prediction that "what is whispered in the closet shall some day be proclaimed from the house-tops."[421]

Despite the concerns raised by Warren and Brandeis, the advent of photography did not result in the destruction of privacy. Nor did it result in criminal or civil liability for those who took photographs of persons in public places.

The opponents to application of developing surveillance technology today raise similar concerns about the effects of technology on privacy. While attention should be paid to the power of modern technology, there is no reason to believe that privacy will be severely limited or destroyed in the way privacy advocates contend. Many of the important aspects of privacy are well protected even in the face of new technology. Deconstructing privacy as the monolithic concept that some commentators offer is helpful in analyzing the steps government policymakers should take to preserve the essential elements of privacy.

If privacy is broken down and analyzed in the four states that Westin proffers, the advent of much of modern surveillance technology really would be found to have little effect on two of those states of privacy. Constitutional protections of the home and intimate relationships are very strong. There is little to suggest that developments in

421 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard L. Rev.*, IV, December 15, 1890.

public surveillance technology will affect the states of privacy of seclusion and intimate relationships. The states of privacy threatened by recent developments in surveillance technology are those of anonymity and reserve.

1. Threats to Anonymity

As to anonymity, three observations are important. First, it should be noted that there is already some degree of protection for that state of privacy. As many privacy advocates correctly point out, anonymity does have value in promoting speech and assembly. These important components to democratic governance are values recognized and protected by the Constitution. To that end, courts have rejected government programs and requirements that have been shown to chill the exercise of rights to speech and assembly protected by the first amendment. Thus, the protection that privacy advocates seek is already provided by the Constitution. Where surveillance techniques are used by government to undermine anonymity and chill the first amendment rights of individuals, such practices are already prohibited by existing first amendment jurisprudence.

A second argument against the impact of surveillance on anonymity, particularly visual surveillance, is that such surveillance compels social conformance. This is the Panopticon effect that Foucault discusses. The degree to which the phenomena of the Panopticon affects behavior is not one that has been adequately quantified and warrants further study. Privacy advocates seem to suggest that the effect would be significant. However, those same advocates suggest that CCTV is ineffective in limiting criminal behavior. It seems counterintuitive that surveillance would have no effect on criminal behavior where there can be a substantial penalty for nonconformance and yet have significant effects on other types of behavior. Moreover, it is unclear why a degree of social conformance in public, even it is shown to be fostered by surveillance, is necessarily an undesirable thing.

The fact that anonymity can lead to some extremely undesirable and anti-social activity seems well documented in social psychology literature. The work of Zimbardo and others suggest that anonymity has negative aspects. That surveillance can have some positive effects on social conformance and compliance with law seems well proved by

initial use of such cameras in monitoring traffic and issuing citations. For example, some jurisdictions have found substantial reductions in dangerous traffic infractions like red light running when cameras are emplaced. As Foucault notes, the effect of the Panopticon is not necessarily a negative. The Panopticon does more than reinforce positive behavior. Beyond the issue of social conformance, the concept of the Panopticon offers a prospect of true government accountability. If the system in which the Panopticon operated provides adequate transparency, it allows citizens a mechanism of observing and placing a check on their government.

A final note with regard to concerns over anonymity is drawn from the availability of technology in society at large. While privacy advocates raise concerns about government use of surveillance technology and its impact on expectations of anonymity in public those concerns do not seem to account for the widespread use of a range of surveillance technology already existing in the public sector. The existence of CCTV has long been a feature in retail establishments across the country. The development and proliferation of video recorders and even cell phones capable of taking video makes CCTV surveillance controlled by private individuals and entities almost commonplace. The existence of a privately controlled surveillance society seems already at hand.

It is difficult to see how in the face of this expansion of surveillance technology, completely uncontrolled by the government, that anonymity is not already affected. If anonymity is affected simply by the capture of one's likeness on a CCTV camera, what difference does it make that it is a government or private camera? How is it that the imposition of government surveillance should be more impactful? The physical act of capturing the image is the same.

The only reason why there may be more concern about capture of images by government cameras than private ones seems to be in the ability of the government to use that information. It seems then that it is the ability of government to relate the image to other information that establishes identity. In short it is not the surveillance itself that destroys anonymity it is the capacity of government to use databases and relate CCTV

surveillance information to other sources that destroys anonymity. Thus, it would seem the key to mitigating the effect of surveillance on anonymity is placing controls on the use of surveillance data not on its collection.

2. Threats to Reserve

In addition to affecting anonymity, it also seems clear that modern surveillance technology constitutes a threat to reserve. In fact, it is this threat to reserve that is perhaps the most disturbing feature of technology. The ability to individuate massive amounts of information gathered from a variety of sources and relate it all back to a specific individual is a distinguishing feature of modern surveillance technology. As computers and digital systems become more sophisticated the amounts of information that can be amassed and analyzed quickly is growing exponentially. Unchecked and unregulated growth of government's capacity to control and manipulate information about individuals leaves them unable to control what information will be shared and with whom it will be shared. This is the essence of reserve.

The types of technology for collection of data on individuals are widespread and growing. CCTV, especially combined with biometrics, RFID or GPS technology allows for extensive tracking of individual movement. The ability to interrelate different surveillance technologies through sophisticated databases allows individuals to be tracked almost anywhere. That tracking ability even applies to movement on the internet. The databases that contain information about individual movement take significant control over the ability of individuals to regulate the dissemination of information about themselves.

As with anonymity, the key to preserving reserve would seem to lay more in the control over databases containing information than in the control over techniques of collection. The threat to reserve rests not in any one recorded event or public record, but rather, in groups of records or recorded events collected over time. Arrayed against the growth of databases that can do just that, incorporating large amounts of disparate data over time, there is little in the way of legal protections.

The Supreme Court has, on two occasions, noted the existence of this problem without specifically addressing its constitutional implications. It has, however, suggested an analytical framework that would be helpful to administrators who are attempting to design surveillance database systems that are consistent with legal precedent. That framework focuses on two basic elements: a legitimate governmental need to collect the data; and adequate safeguards to protect the privacy rights of individuals in the information maintained by the government.

B. ASSESSING GOVERNMENT USE STRATEGIES AND TAILORING GOVERNANCE

An interesting feature of the *Whalen* decision is the Court's examination of the government use of the information. The Court in upholding the scheme seemed persuaded by the important government purpose to be accomplished, not merely the individual expectation of privacy. The Court also seemed satisfied that the government's collection efforts were designed to support the use strategy. In the areas of public surveillance where the Court has previously indicated that privacy expectations are not implicated, it might be helpful to construct differing rules based on the government's interest in conducting surveillance or its use of the surveillance data.

Where the government is conducting surveillance for purpose of determining the existence of dangerous contraband, especially in areas where the contraband may have disastrous or catastrophic consequences, the government surveillance collection efforts should be given greater latitude. In fact, the Supreme Court seems to have already made such an accommodation through its "special needs doctrine". Moreover, where the intrusiveness of such searches can be minimized through application of accurate binary technology, use of surveillance technology may also be acceptable even where the contraband sought is less of an immediate danger.

Application of surveillance technology consistent with this governmental use has implications for data collection in connection with those programs. Surveillance programs consistent with government use, data gathered to detect the presence of

contraband or wanted persons has little or no utility after the individual or contraband is gone. Thus, the retention period for maintaining this data should be relatively short.

The same is true of surveillance technology designed for observation of areas. If the governmental purpose is to use technology to guide response or secure those areas against dangerous behavior, there is little need for extensive retention of data. While some retention may be required to look for pattern behaviors over a period of time (i.e., behavior that might suggest surveillance of a critical facility or testing of security procedures) retention should be relatively short. Where suspect behaviors are identified and there is a desire for longer retention, some enhanced standard like reasonable suspicion should be applied to requests to extend retention. Retention might also be extended where the area of observation occurs around critical facilities or critical portions of facilities that may potentially serve as targets for terrorist (e.g., airport perimeters or areas around air intake systems of large buildings).

Where governmental use of surveillance data is just for observation related to activities in directing response or looking for suspicious or dangerous conduct, and retention of data is for a limited period, it is difficult to see how the privacy interests of anonymity or reserve are significantly impacted. To ensure that this type of area surveillance technology is utilized only for the purposes of general observation to direct response or secure areas against dangerous behavior there are a number of developing technologies that can be employed to enhance privacy protection. Application of technologies for anonymizing information, particularly CCTV data as it is taken or stored, provides an enhancement to protect both anonymity and reserve interests of individuals. Limiting through intelligent or smart video technology the collection or storage of data to only that which is determined to be dangerous is another technology solution that may mitigate privacy concerns.

Granted, defining suspicious or dangerous conduct may not always be easy, but some conduct surely can be agreed to warrant attention (i.e., individuals who enter posted areas for no trespassing or throwing items over perimeter fencing at a secure facility). Other types of conduct such as loitering around a facility or standing in public area observing activity at a given place over time are more ambiguous. The exercise of law

enforcement discretion in determining what behaviors will be monitored or declared "dangerous" or "suspicious" will no doubt be the subject of some controversy.

The advantage of using technology for monitoring such conduct is that there will be a clear auditable trail of behavior that has been identified for monitoring. That conduct will be reduced to algorithms for entry into the monitoring system. The existence of an auditable trail of exactly what the government has been watching is a part of the positive feature of the Panopticon that Foucault mentions in his work.

It is in the cases where the government is utilizing surveillance technology to track individuals either physically, on the internet or over time through database analysis that real issues of impairment to the privacy interests of anonymity and particularly reserve are impaired. While the use of technology to follow individuals through public space has been approved by the U.S. Supreme Court in *Knotts*, it is not clear whether that ruling would be applicable to widespread application of such technology without a warrant issued based on probable cause or at that very least on some reasonable suspicion on the part of law enforcement officers that the subject of such surveillance is or has been involved in some critical conduct.

In examining the governmental uses for surveillance technology it seems that only the use of technology for individual tracking warrants more detailed procedures to guard against misuse. Only tracking is predicated on the maintenance of extensive amounts of data over extended periods of time. It is the data rather than the collection mechanisms that is the matter of most concerns with respect to privacy.

C. APPROACHES TO GOVERNANCE

The strategies for managing technologic developments in surveillance run the gamut from approaches that essentially involve doing nothing to extremely restrictive strategies. It seems there are two significant areas that need to be addressed in developing or assessing governance strategies. The first is focused on what restrictions should be placed on collection activities. The second approach focuses not so much on collection but on use of information gathered. Approaching the problem from the

perspective of regulating and controlling the use of information gathered rather than extensive concern over the collection mechanisms seems to provide a more flexible and comprehensive governance strategy that protects the main privacy interests of individuals.

On one end of the spectrum is the position that administrators need do nothing to regulate surveillance of public sector cameras. So long as collection is limited to activity in public space, the existing case law does currently support such an approach. However, as the scope of such surveillance expands and databases with the information become more sophisticated, the protections from current case law become more and more attenuated.

Moreover, courts are not the only source of potential opposition to the introduction of advancing surveillance technology. While oftentimes individuals subjected to surveillance at any given time will take the attitude of "I've got nothing to hide," as Daniel Solove and other privacy scholars note, as pieces of trivial information become catalogued and organized, public perception and concerns about threats to privacy may well turn. The need to hold this aggregated information private is important. In this regard, Solove discusses the private civil action filed by customers of Northwest Airlines when their passenger data was supplied to the government's CAPPS II project.[422] Solove argues the unsuccessful attempt to enforce the privacy policy of Northwest Airlines illustrates the need for some legal mechanism to enforce privacy promises for collected information.

The failure of government to realize that aggregated data may raise concerns that discreet pieces of information do not; may result in building large and complex surveillance collection and analysis tools that are delayed in implementation or ultimately cannot be used. Such a reality has already been experienced by government with respect to a number of projects like MATRIX, CAPPS II and ADVISE. The failure to properly

[422] Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," 44 *San Diego L. Rev*. (2007), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565#PaperDownload (accessed February 1, 2007).

account for privacy concerns can cost millions of dollars in project delays and revisions. It also results in the inability to utilize technologies that may be helpful in securing public safety.

While there are differing approaches to how surveillance technology and the information from it should be governed, those proposals generally coalesce around a few central principles. Perhaps the best exposition of principles to guide development and use of surveillance technology are the Fair Information Practice Principles (FIPP) developed in the late 1970s. These principles, designed in conjunction with governmental agencies in Europe and Canada, provide a basis for governmental programs designed to protect individual privacy. These principles have the advantage of being flexible and are internationally accepted. In fact, they form the basis for the European Union's Data Protection Act of 1995 and the Canadian Standards Association's Model Code for the Protection of Personal Information.[423] Because these principles have wide acceptance for privacy management, they provide key insight for the development of governance structures.

The FIPP operates on five principles with respect to organizations that receive and collect personal data of individuals. Those principles include: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress. While the FIPP are designed to address personal information given in relation to consumer practices, for example credit card purchases, these core principles provide an evaluative tool that has can be applied to surveillance data.

1. Notice/ Awareness

This principle addresses the need for organizations involved in information collection to advise the subjects of surveillance regarding its occurrence and the purposes to which data collected will be applied. Information available to the public should include identity of the "…entity collecting data," "… uses to which the data will be put," identity of "…any potential recipients of the data," nature of the data collected and means

[423] U. S. Federal Trade Commission, *Fair Information Practice Principles.*

of doing so, whether compliance is voluntary and the means of assuring confidentiality and quality of the data.[424] The notice provisions may also include providing information as procedures for individual access to the data as well as redress and correction procedures.

The issues of Notice/Awareness raise interesting issues for operators in the areas of: outlining and advising the public generally regarding the purpose of surveillance systems, and specifics regarding the operation of those systems. Looking at a sample of strategies for governance like the Constitutions Projects' Model Legislation for Establishing Public Video Surveillance Systems (the "Model Legislation"), the United Kingdom's CCTV Code of Practice (the "UK CCTV Code"), and the American Bar Association's Criminal Justice Section Standards for Technology-Assisted Physical Surveillance (ABA Standards)[425] provides differing approaches to these three components of Notice/Awareness.

All three of the systems examined would require as an initial matter some assessment of the need for the surveillance measure and the appropriateness of the tool. The Model Legislation would require a relatively detailed and complex process for adoption of a surveillance system.[426] The proposed review requires creation of a legislatively mandated Public Video Impact Assessment that includes assessment of a wide range of items.[427] Many of those items are difficult if not impossible to assess with any real empirical data. In some cases, the standards to be assessed under the Model Legislation are not even clearly defined. Questions like impact on "government accountability" or "'spillover effects,'" i.e., potential issues of crime displacement, can likely never be answered.[428] The net result of the detailed assessment process outlined by the Model Legislation will likely have the same effect that similarly detailed hearing

---

[424] U. S. Federal Trade Commission, *Fair Information Practice Principles,* 1.

[425] American Bar Association, *Criminal Justice Section Standards for Technology-Assisted Physical Surveillance*, http://www.abanet.org/crimjust/standards/taps_blk.html (accessed February 2, 2008).

[426] The Constitution Project, *Guidelines for Public Video Surveillance.*

[427] Ibid., Sec. 208, 51.

[428] Ibid.

requirements have had on CCTV development in France. The process of technology deployment will likely be significantly retarded.

On the other end of the spectrum, the development of a purpose statement suggested in the UK CCTV Code provides little guidance for policymakers. The UK system requires only an assessment of the "appropriateness and reasons for using CCTV or similar surveillance equipment."[429] While there is good argument for conducting and documenting the purpose of CCTV or any surveillance system, more description of considerations to be given to administrators making decisions would be helpful.

A useful middle ground may be the ABA Standards, which recognize the need to examine the law enforcement interests in conducting the surveillance. Those interests include, objectives to be achieved; extent to which surveillance contributes to those objective and nature and extent of crime involved.[430] The ABA Standards also direct examination of the extent to which privacy is invaded by examining factors such as the following:

> (A) The nature of the place, activity, condition, or location to be surveilled;
>
> (B) The care that has been taken to enhance the privacy of such place, activity, condition, or location;
>
> (C) The lawfulness of the vantage point, including whether either the surveillance or installation of surveillance equipment requires a physical intrusion;
>
> (D) The availability and sophistication of the surveillance technology;
>
> (E) The extent to which the surveillance technology enhances the law enforcement officer's natural senses;
>
> (F) The extent to which the surveillance of subjects is minimized in time and space;

---

[429] France, Code of Practice, Part I, 6.

[430] ABA, *Standards for Technology-Assisted Physical Surveillance*, 2-9.1(c)(i).

(G) The extent to which the surveillance of non-subjects is likewise minimized;

(H) Whether the surveillance is covert or overt.[431]

The ABA Standards also recommend decision makers consider the impact of surveillance on the exercise of first amendment rights as well as the availability of effective and efficient alternatives that are less intrusive.[432]

The ABA Standards draw heavily upon the existing Supreme Court fourth amendment jurisprudence. While no formal report or process is required by the ABA Standards, the ABA Standards provide important insights for officials in policy development. The use of considerations based on case law should help ensure development of surveillance systems consistent with constitutionally protected rights. Moreover, the ABA Standards approach seems to have sufficient flexibility to address differing types and combinations of technology.

One limit of the ABA and Model Legislation approaches seems to be that they only seem to recognize a law enforcement purpose as a legitimate basis for surveillance. There needs to be recognition of the fact that a range of surveillance technologies have functions beyond law enforcement. While CCTV may be use in preventing and deterring crime on city streets or identifying offenders once crime occurs, they can have a wide range of other functions. They can be utilized to monitor traffic and where properly programmed issue traffic citations. They can be utilized to direct the resources of police, fire and emergency medical response. They can enhance command and control functions in the event of a disaster. In short, technologies can and frequently do have multiple uses. This includes other technologies examined like GPS for use in dispatch of emergency services in connection with 9-1-1 calls or RFID that is used to expedite the travel process. Purpose statements need to recognize public safety uses of surveillance

[431] ABA, *Standards for Technology-Assisted Physical Surveillance*, 2-9.1(c)(i).

[432] Ibid.

technology divorced from traditional notions of crime-related law enforcement. In this regard, the more generic definition standard of "…purpose of the Scheme" in the UK CCTV Code is perhaps a better standard.[433]

A second issue with respect to notice and awareness centers on the issue of direct notice to individuals in areas where surveillance is being conducted. This brings to the fore the debate over signage requirements. Here both the Model Legislation and the UK CCTV Code require the posting of signage. The ABA Standards offer a more flexible approach only requiring notice when the purpose of the camera is deterrence or where those "…potentially subject to the surveillance should be given the option of avoiding it."[434]

The value of signage in protecting privacy in public places is questionable. Christopher Slobogin's empirical work would seem to suggest "…knowledge that cameras are present triggers a greater feeling of intrusion that knowledge that cameras might be present."[435] Slobogin's research seems to ratify the existence of the Panopticon effect discussed by Foucault. Such an effect would likely increase the type of social conformance that many privacy advocates decry. Moreover, if CCTV cameras or other surveillance devices are placed around critical areas in cities it seems impractical to expect that somehow people can avoid them. If, for example, city streets and transportation centers are subjected to camera surveillance the only option would be for a person to avoid streets and public transportation; such a choice would hardly be an option for most.

While the public should be given notice of the imposition of camera programs and be made aware of the possibility of public activity being filmed by cameras, the requirement of signage seems burdensome and expensive with little benefit. As noted above, it may generally cause more feelings of intrusion than it relieves. Where as the ABA Standards suggest the purpose of the camera is other than deterrence and the

---

433 France, Code of Practice, Part I, 6.

434 ABA, *Standards for Technology-Assisted Physical Surveillance*, 2-9.1(c)(i).

435 Christopher Slobogin, "Camera Surveillance of Public Places and the Right to Anonymity," 279.

surveillance cannot be avoided strong argument can be made that a signage approach is unnecessary. Whatever approach a governmental entity decides to take with respect to signage, the public should be provided notice of the existence of surveillance programs.

One final issue with respect to notice arises when information becomes individuated. When data respecting an individual becomes tagged, categorized or segregated into a separate dossier, both the Model Legislation and The ABA Standards recommend the existence of post surveillance notice to the subject of the existence of a court ordered surveillance. This is consistent with procedures in Title III[436] that governs wiretaps and the provisions of the ECPA[437] for the interception of other electronic communications.

In the absence of a court ruling or some statutory direction, like that offered in the Model Legislation, attempting to seek court approval of government use of public gathered information to create individual files or conduct individual tracking would be futile because the court would not recognize any authority to address the matter. Currently surveillance in public areas (excluding wiretap and surveillance under the Title III and ECPA) requires no court approval. Thus no notification would be required. Nothing, however, precludes local governments from imposing their own oversight processes for individual tracking and individualized data collection and analysis.

Given the power of the data collection and data analysis tools discussed above some review of tracking and individualized data collection and analysis technology schemes is warranted. While courts can and do provide independent review, in the absence of legal authority to support such a review, governmental entities can perform that function internally. Where law enforcement seeks to use technology for tracking or seek to use databases for individualized surveillance there needs to be a process to ensure there is reasonable suspicion or probable cause for the operation to be conducted.

Where government engages in tracking of an identified suspect individual through public space with a CCTV camera tracking technology; or researching databases of

436 Title III, 18 U.S.C. §§ 2510-20.

437 EPCA, 18 U.S.C. §§ 2701-2710.

CCTV regarding an individuals movements, or using other tracking technologies to identify individual prior movements, those actions should be documented. There should be a clearly articulated basis for the tracking activity. There should also be a defined approval process preferably with review by at least some authority in the law enforcement organization that is separate from the individuals conducting the investigation. That reviewing authority should ensure that surveillance is only conducted for a specified time. Moreover, once the surveillance operation is concluded the subject should be advised so that they may exercise access rights to review information gathered. Providing notice to the subject of the investigation allows the subject an opportunity to take action to ensure that proper investigative procedures were followed. This outline follows the essential protections currently given to wiretap activities.[438]

2. Choice/Consent

This principle of the FIPP means "…giving consumers options as to how any personal information collected by them will be used."[439] At first blush, it may seem inapposite to management of developing surveillance technologies. However, if we accept a properly scoped public purpose for surveillance systems, it may prove to be the most important, particularly with regard to the data produced by those programs.

The choice/consent addressed by the FIPP really concerns the secondary use of consumer information. For example, an individual who presents a credit card and the attendant information associated with it for purposes of making a purchase is not consenting to the secondary market research purposes that a vendor may have for the information. Citizens should be allowed the same expectations with regard to surveillance systems. The use of data gathered from CCTV cameras used to secure a transit station hub should not, absent the presence of reasonable suspicion or probable cause of criminal activity, be used for the secondary purpose of tracking activity.

---

[438] The Title III and ECPA requirements require review by a neutral and detached magistrate. The same requirement of magistrate review is applied for detention without a warrant under *Gerstein v. Pugh*, 420 U.S. 103 (1975). However, here, where the conduct observed is public activity and there is no threat to important liberty interests as existed in *Gerstein*, the need for a neutral and detached magistrate may be more than what is required to reasonably protect the interests at stake.

[439] Federal Trade Commission, *Fair Information Practices Principles*, 1.

Similarly, GPS data used to ensure availability of 9-1-1 response or RFID data from atoll way pass should not be utilized for tracking, absent some evidence of criminal activity. Use and dissemination of data gathered from surveillance mechanisms should only be for the governmental purposes that required the data to be gathered. This restriction on use is a common feature of the Model Legislation, the ABA Standards and the UK CCTV Code. Implementation of this principle will likely require legislative action to eliminate court subpoena power and freedom of information access to the data.

3. Access/Participation

This principle primarily concerns the right of the individual with respect to data gathered concerning him or her. It allows the individual to ensure that data collected about one's self is accurate and is being held in accordance with the systems requirements. The FIPP notes that this principle requires simple, timely, inexpensive procedures to access and contest inaccuracy. This measure is found in the UK CCTV Code and to a more limited degree in the Model Legislation. The UK CCTV Code affords individuals who are subject to CCTV surveillance broad rights to review data retained by the system. It sets forth the right of the individual to simply make an application to review data of himself or herself. Compliance can be accomplished by providing the requesting individual with a copy of the images depicting him or her or by allowing them to view the images. Brochures are prepared for the public advising them how to make requests.

The Model Legislation affords more limited individual access rights. Individual access is afforded in circumstances such as when the individual is provided notice that he or she has been subject to individualized data collection or when the individual is accused of a criminal act. The ABA Standards do not require any individual access.

While affording individual access can serve as a check against government abuse, providing access presents a number of technical problems. Where the data has already been segregated providing access might be easy. This would be the circumstance envisioned when a separate investigative file has been created and the individual subject notified of its existence. However, review of data that has not been individuated poses a

range of problems. For example, how do technicians produce images of an individual when he or she is part of a crowd, without compromising the confidentiality of others? The process of redacting or masking other visual or surveillance information may prove to be extremely cumbersome, time consuming and expensive. While individuals should have the ability to review data maintained by government once it has been individuated, it seems wasteful and unnecessary for government to be required to individuate information and produce it for individual review. In this regard, the more limited review approach offered in the Model Legislation seems to be more workable.

Affording individuals access to data especially when it is individuated and categorized is important to privacy interests of anonymity and reserve. It is important for individuals to understand exactly what type of information the government is maintaining about them. Accessing this information allows individuals some understanding of the degree to which their privacy interests may be compromised by government activity.

4. Integrity/Security

Integrity and security is about assuring that the data collected is uncompromised and accurate. It also provides assurance that the data will only be used for the authorized government purposes that supported its collection and maintenance. All three of the examples of governance strategies, the Model Legislation, ABA Standards and UK CCTV Code, discuss the importance of integrity and security. With regard to integrity, it is important to understand that some of the data collected may serve as evidence in criminal proceedings. As such, ensuring data integrity is a critical matter. The ABA Standards discuss the need for ensuring that only surveillance techniques suitable to the task should be used to generate data.[440]

The Model Legislation mandates a range of integrity and security measures. These include: restricted access to surveillance systems and data storage; technical training for operators; and extensive recordkeeping functions to log system access by

[440] ABA, *Standards for Technology-Assisted Physical Surveillance*, 2-9.1(d) (iv).

those who "…maintain, operate, observe, inspect or access…" the system.[441] The UK CCTV Code imposes similar proposed requirements on system designers and operators.[442]

One area of common agreement is the need to restrict access of information to third parties. The general tenor of all three of the templates for governance, third party access should be limited. Perhaps the most limiting of the three templates is the Model Legislation. That legislation would only allow access to third parties based on some court finding of need. Need is defined in extremely limited circumstances in the event of non-governmental parties like private litigants in civil court, it requires findings of "imminent harm to life or limb." Even as to governmental entities, the Model Legislation would require a finding of probable cause. Significantly, the Model Legislation would exempt surveillance data from local public disclosure laws that apply to most public records. Inclusion of limitations on access to data through mechanisms like court ordered discovery in civil proceedings or state freedom of information or open records acts points out a significant limitation on the ability of government agencies limiting third party access. Unless specific statutory relief is provided, local governments may be compelled by open records laws or court procedures to provide information to third parties.

The UK CCTV Code contains similar limitations of disclosure to third parities. One notable exception is to allow for dissemination of information or images where law enforcement finds itself in need of identifying victims, witnesses or perpetrators of criminal acts. Law enforcement use of video tape information to catch individuals filmed in the act of committing a crime is not an unusual occurrence. It is difficult to square such a practice with the provisions of the highly restrictive Model Legislation. With regard to dissemination decisions, the UK CCTV Code outlines the importance of documenting disclosure decisions and logging access. In light of the *Peck* decision the UK seems to be much more circumspect about release of third party information without a proper purpose.

---

441 The Constitution Project, *Guidelines for Public Video Surveillance.*

442 France, Code of Practice, Part I, 13-4.

A final issue with regard to integrity and security is the issue of retention. The establishment of a retention schedule and the elimination of data at the conclusion of retention are universally accepted requirements. Also excepted is the notion that retention beyond the schedule may be appropriate for certain data (i.e., data to be used as evidence in a criminal proceeding). The setting of retention schedules and the procedures for preserving data beyond a retention schedule varies widely. The Model Legislation suggests a seven day period for retention of data. It provides for an extension of the period of time based on request from the operator and finding of reasonable suspicion or probable cause on the part of the chief administrative officer of the law enforcement agency.

The UK CCTV Code offers a more flexible process that is dependent upon the need for retention. As an example, retention is seven days for ordinary crime control cameras based on the notion that evidence of criminal activity will be readily apparent within that time. Images taken in City centers are kept for up to 31 days (unless extended for legal proceedings). ATM cameras are kept for up to three months based on when account statements are received so discrepancies on withdrawals can be resolved.

With regard to the objectives of surveillance outlined in the technology assessment portion of this paper, a differential schedule for retention seems to make a great deal of sense. For example, where the purpose of surveillance is detecting suspect objects or contraband a relatively short time period for retention of 72 hours to seven days makes sense. Where the object of surveillance is to observe a critical facility, a 30 to 60 day retention period might be needed to ascertain patterns that might suggest the location was being scouted. Where tracking activities are occurring retention may need to be longer than 30 days but here there should be some reasonable suspicion or probable cause to believe there is criminal activity and an extended retention can be authorized by a supervision authority, whether that authority is a court or senior law enforcement official. The ABA Standards also noted the importance of retention.

The integrity and security of the system is of critical importance to reserve. While the individual may feel discomfort in knowing that information is in the possession of the government, an understanding of the rules for release of the information and the

fact that it will not generally be released to others allows for some restoration of the sense of reserve. If the surveillance system is secure, individuals can rely on the fact that confidential information will generally remain confidential.

5. Enforcement/Redress

The final FIPP principle is for there to be some mechanism for enforcement and redress to be incorporated into the system. The reasoning behind these provisions is that they will ensure government compliance with its own rules. Without them there is concern that regulations will be "…Suggestive rather than prescriptive."[443] The FIPP notes that compliance can come from self regulation or externally imposed in the form of civil actions or civil and criminal penalties through government action.

The Model Legislation utilizes all three mechanisms to ensure compliance. It recommends audits of the operation of CCTV systems, private causes of action for individuals whose rights are violated by government misuses of data or improper collection, as well as a range of civil and criminal penalties. The Model Legislation also contains provisions for discipline of employees who misuse the video system and provisions that would exclude from evidence any information acquired in violation of the Model Legislation.

The UK CCTV Code and the ABA Standards are somewhat more circumspect in the recommendations they make with respect to enforcement and redress. Both recommend the importance of audit and review to ensure compliance with written direction for system operation. Both the ABA Standards and the UK CCTV Code suggest that information about the system and assessments of it should be open for public scrutiny. Neither recommends a private right of action. The ABA Standards do suggest that government accountability can be satisfied by internal rules and application of exclusionary relief where appropriate under state or federal law.

The goal of these enforcement and redress measures is to not just to enhance compliance. It should also be to instill public confidence in the fact that surveillance

[443] U. S. Federal Trade Commission, *Fair Information Practice Principles.*

systems are operating within established guidelines to accomplish their stated purposes. If organizations have detailed written polices that detail operational requirements, combined with audits and assessments made available to the public that should serve to assist in accomplishing those goals. Those measures, combined with the ability of citizens to correct errors with regard to their records and discipline for government employees who misuse the system would seem to be adequate to address compliance issues. The extensive civil remedy provisions in the Model Legislation providing for damages and attorneys fees seem excessive especially in light of existing remedies for violations of constitutionally protected rights under 42 U.S.C. § 1983.

D. SELF-REGULATORY OR LEGISLATIVE SOLUTIONS

While either a self-regulatory or legislative scheme would work to establish governance, it is likely that a combination of the two approaches would likely be the best strategy in developing governance. The advantage of self-regulation is that it is generally more effective in addressing complex and fast developing technology. Self-regulatory solutions allow for quicker ability to adapt to new developments in technology and adopt the best practices from other jurisdictions.

The experiences in the UK compared to France or Germany seem to ratify the fact that self-regulation provides a more flexible environment for CCTV to flourish. The strict legislative procedures in France and Germany have constrained the development of CCTV surveillance. While comparing the effect of regulation to legislative solutions across differing national and legal systems provides much room for error, it would seem that self –regulatory approaches would provide a more fertile basis for CCTV growth.

The more significant question is whether a self-regulatory system will adequately protect privacy interests. The experience in the UK provides a mixed result on this point. The *Peck* case certainly demonstrates a weakness in protection occasioned by that self regulatory environment. Similar evidence of weakness is seen in the apparent lack of compliance with regulatory signage requirements. This is not necessarily a failure of a regulatory approach as much as it is a suggestion that insufficient resources are dedicated to enforcement and compliance.

An effective approach in governance will likely require a combination of legislative and self-regulatory measures. Only legislation can provide for exemption of CCTV and surveillance data from dissemination under public records law. Only legislative solutions can restrict the application of court rules for production of information in connection with civil proceedings. Legislation might also be useful to provide an oversight structure to independently audit or monitor CCTV or surveillance operations in a state.

As to the development and day-to-day operation of a system, self- regulation likely provides a more effective tool for management. With effective enforcement and compliance mechanisms in place abuses can be prevented. Operation in a self-regulatory environment is more consistent with current law enforcement operational practices.

E. RECOMMENDATIONS FOR ADMINISTRATORS

This thesis likely raises more questions for addressing developing surveillance technology than it provides answers. That is because some of the clear answers administers seek do not exist or compete with other claims and values. What this thesis does present is a range of issues that administrators will certainly confront as well as some approaches, successful and unsuccessful, in addressing those problems.

Two issues seem to be almost universally established and accepted by all the commentators who have addressed the issue of developing surveillance technology. First, developing surveillance technologies are growing in power both with respect to ability to collect and manipulate data. While this thesis has examined some of those technologies there are many others in development. Second, these technologies will require some controls or regulation to ensure that privacy interests are protected. Failure to provide for adequate governance will likely lead to some form of legal intervention and loss of public support for surveillance programs. With those two facts in mind, the following are recommendations for consideration by policymakers exploring the implementation of CCTV or developing surveillance technology.

1. Privacy is not a Monolithic Concept

Privacy has several aspects and functions in society. Certain aspects or states of privacy like seclusion and intimacy have significant protections. Other states like anonymity and reserve have lesser protections. Moreover, the function of anonymity can serve both positive and negative societal functions. In developing and applying technology, administrators should be aware of what aspects of privacy are being affected and how those effects can be mitigated.

2. Privacy is Constitutionally Protected

Despite suggestions of some commentators, privacy is afforded significant protection by the U.S. Constitution and those protections can and do extend into public areas. In designing and implementing surveillance systems, administrators must be mindful that if those systems are shown to chill first amendment speech through destruction of anonymity, they will not be permitted. Administrators also need to understand that if systems are designed or operated in a discriminatory fashion, they may well be shut down for violating the equal protection provisions of the fourteenth amendment. Accordingly, governance of technologically enhanced surveillance programs should include clear statements prohibiting operator conduct that violates first and fourteenth amendment protected rights and ensure proper training for operators in that regard.

3. Fourth Amendment Concerns in Public Surveillance must be Addressed

The contours of the fourth amendment have evolved over time and will likely continue to evolve with respect to use of surveillance technology. The ABA Standards provide an excellent exposition of factors that administrators should consider in application of technology.[444] In addition to those factors, administrators should focus on the following fourth amendment principles in developing strategies. First, the notion that the Constitution does not afford privacy protection to contraband can shape development

[444] ABA, *Standards for Technology-Assisted Physical Surveillance*, 2-9.1(c)(ii).

of procedures for surveillance designed to find suspect items or persons where surveillance techniques are accurate and nonintrusive. Second, the special circumstances doctrine may afford greater latitude for implementation of surveillance procedures that can be related to substantial threats. Finally, with respect to human tracking technology, while the Supreme Court has upheld use of this practice in public space, there is serious question as to whether it would approve widespread application of such techniques particularly in the absence of some legal justification like reasonable suspicion or probable cause to believe it was related to criminal conduct.

4. Technology Design Should Seek to Mitigate Privacy Impacts and Enhance Protections

Administrators should look to shape technology development to address constitutional concerns. For example, where possible, technology looking for suspect items or persons should be designed to be binary in nature. When designing observation systems, smart video technologies employing masking, anonymization and behavioral pattern recognition should be explored and where possible employed. Administrators should also be assured that only appropriate technology is employed at locations and that it is properly maintained and operated. The UK Code of Practice provisions on Siting the Camera,[445] Quality of the Images,[446] and Processing the Images,[447] provide helpful insights.

In addition to system designs that mitigate impacts in collection, there are also protections that can be built into systems to provide privacy protection. Aligning automated system design to support governance policies is an important feature. Automated systems can and should be designed to limit access by operators only to the information and functions in collection essential for that person to do his or her job. Access control features should be designed to prevent unauthorized access. The system

445 France, Code of Practice, Part I, 7.

446 Ibid., 9.

447 Ibid., 11.

should also be designed with a reporting function that allows for the generation of audit reports to review access to files or activity by operators.

5. Developing Computer Technology Presents Challenges for Data Management

The development of complex computer systems that can interrelate large amounts of public surveillance data poses significant issues for administrators. It is quite likely that management of the data gathered by surveillance technologies poses the greatest danger to privacy. Review of standards in accordance with the internationally accepted FIPP in the preparation of governance schemes will assist administrators in developing governance schemes that address privacy concerns. Legislative and regulatory templates like the Model Legislation, ABA standards and UK CCTV Code of Conduct provide different ways in which governance can be achieved consistent with the FIPP. While a regulatory versus legislative solution would likely be more flexible and easy to implement, some issues like third party access will likely require at least some legislative action.

6. Ensure that Practice Conforms to Written Policies Through: Supervision, Training, Discipline, and Retraining of Employees; and Internal and External System Audits

The development of policies that provide for safeguarding data, limiting use and surveillance activity to approved governmental purposes and otherwise protecting privacy does not ensure that such activities will actually occur. Policies are not self actuating. A properly governed system ensures that the employees operating it are adequately supervised. Any employee authorized to access the system must be trained particularly in the legal and ethical obligations in using the system and the data it generates. Those employees should be periodically retrained to ensure that the message of proper usage is reinforced. Where employees are found to be violating policies and misusing the system or data it generates, they should be disciplined.

In addition to measures taken to ensure that individuals operate the system consistently with governance requirements, internal and external audits should be

conducted at regular intervals. Given the computerized operation of CCTV and other digitized surveillance systems, the creation of automated audit reports showing actual operation of the system should be relatively easy to create and monitor. The audit results should be publicly available. This will afford some of the transparent system operation that Foucault concluded was one of the beneficial feature of the Panopticon. The use of detailed public audit can help the public to better monitor activity of government even as government is observing them. The inclusion of an external audit, in addition to internal ones, affords the public additional confidence in the rectitude of government conduct. This concept has worked well in Chicago.

7. The Pace of Change in Technology Requires Periodic Review of Policies and Practices to Ensure They are Meeting Governance Goals

One final recommendation concerns the need to ensure that governance strategies keep pace with technological change. The range of technologies that can be linked to and interrelated with CCTV is large and growing. The pace of technology development is extremely rapid. Governance strategies of today will doubtless need to be retooled and recalibrated to address the new features and capacities of tomorrow's technology. Governance structures should include provisions for regular review and update to ensure that technology developments are addressed and that new technologies are introduced to enhance protections for privacy.

F. SUMMARY

As the use of technology enhanced surveillance grows across the country, more and more communities will need to address the issues of data collection and maintenance. Law enforcement and public safety officials will press to ensure that their use of technology to prevent, protect and respond to a range of public safety concerns. Policymakers in developing a scheme to harness the powerful tools that technology is developing must also work to ensure that "the fight to be let alone" is accounted for and respected.

The continuing developments in surveillance technology and information processing are significant. To address the issue of governing surveillance technology and its accompanying databases, there are several approaches offered by both domestic and international sources. A range of these approaches can be found in attempts to address CCTV.

Certainly there needs to be concern in the deployment of technology to ensure that it does not invade private spaces (i.e., the CCTV camera that inadvertently or deliberately peers into a bedroom window, or the application of backscatter x-ray technology to show body features). However with developments in technology collection mechanisms can and should be shaped to minimize the likelihood of even accidental intrusion into private areas. For example, cameras in public areas can be equipped with technology to blank out views of private areas. Intrusive technologies like backscatter x-ray can be developed or operated in a binary format only indicating the presence of contraband items.

On one extreme is the approach offered by groups like the ACLU. Those groups seek to halt the introduction of the CCTV as a surveillance device, at least until the efficacy of such systems can be proven by empirical study. However, the time and resources required to conduct such studies would *defacto* result in discontinuation of CCTV projects. While the ACLU's call for more careful consideration of CCTV projects is not without some merit, the approach of creating barriers for technological developments in surveillance technology will only serve to deprive government of useful tools for accomplishing a range of legitimate and important activities.

On the other extreme are the proponents of employing surveillance technology, who cite fourth amendment case law and announce that there is no privacy concern with respect to surveillance in public areas. As noted in the analysis above, such a blunderbuss approach is not only inaccurate, it will likely lead to potentially crippling restrictions on surveillance programs imposed through legal actions and lack of public support. Privacy interests do pervade the public space and must be protected.

The middle ground between the extreme is reached through the development and employment of governance strategies outlined above. Those strategies can and should control operation and deployment of surveillance systems consistent with privacy values and drive development of technology to account for and address privacy concerns. It can provide government with a comfortable way to use technology consistent with privacy interests. Perhaps more importantly, rather than presenting the public with the specter of a government that spies and snoops on innocent activity, it offers the prospect of a government watchful of only those matters essential for protection. Successful governance should allow the use of CCTV and other developing technologies to be viewed not with dread, but, rather, like the guardian dreamed about in the Gershwin tune:

There's a somebody I'm longing to see
I hope that he turns out to be
Someone to watch over me[448]

448 George Gershwin and Ira Gershwin, "Someone to Watch Over Me."

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Secondary Sources

9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, D.C.: U. S. Government Printing Office, 2004. http://www.gpoaccess.gov/911/index.html (accessed May 11, 2007).

Adler, Michael. "Note: Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and Net-Wide Search," 105 *Yale L. J.* (1996): 1093.

American Bar Association. *Criminal Justice Section Standards for Technology-Assisted Physical Surveillance.* http://www.abanet.org/crimjust/standards/taps_blk.html (accessed February 2, 2008).

American Civil Liberties Union. *Data Mining Moves into the States.* http://www.aclu.org/FilesFDPs/matrix_20report.pdf (accessed May 9, 2007).

American Civil Liberties Union. *Data Mining Moves into the States.* http://www.aclu.org/privacy/spying/15694res20031030.html (accessed January 26, 2008).

American Civil Liberties Union. *MATRIX Myths and Realities.* http://www.aclu.org/privacy/spying/14999res20040210.html (accessed January 26, 2008).

American Civil Liberties Union. The Seven Problems With CAPPS II, http://www.aclu.org/privacy/spying/15258res20040406.html (accessed January 26, 2008).

Ball, Kristie and David Murakami Wood, eds. "A Report on the Surveillance Society: Summary Report," *Report for the Information Commissioner, by the Surveillance Studies Network*. London: U.K. Government, 2006. http://www.privacyconference2006.co.uk/files/report_eng.pdf (accessed September 16, 2007).

Barlas,Thomas. "Lawmakers Allow Municipalities to Implement Red Light Program," http://www.pressofatlanticcity.com/news/local/atlantic/v-page2/story/7526811p-7428234c.html (accessed January 13, 2008).

Betzel, Margaret. "2004 Year in Review Special Topic: Biometrics: Privacy Year in Review: Recent Changes in the Law of Biometrics," *I/S: A Journal of Law and Policy for the Information Society* 1 (2005): 517.

Blitz, Marc Jonathan. "Video surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity," *Texas Law Review* 82 (2004): 1349.

British Broadcasting Company, "Germany Plans Surveillance Boost," *News,* August 21, 2006, http://news.bbc.co.uk/2/hi/europe/5272638.stm (accessed September 17, 2007).

Buckley, Cara. "New York Plans Surveillance Veil for Downtown," *The New York Times*, July 9, 2007. http://www.nytimes.com/2007/07/09/nyregion/09ring.html?ex=1341633600&en=2644be97bd9577f9&ei=5088&partner=rssnyt&emc=rssp (accessed September 17, 2007).

Carrell, Nathan E. "Spying on the Mob: United States v. Scarfo—A Constitutional Analysis," *University of Illinois Journal of Law, Technology and Policy* 2002 (Spring 2002): 193.

Chicago Tribune Editorial Board. "Wave and Behave," *Chicago Tribune*, February 10, 2008. http://www.chicagotribune.com/news/opinion/chi-0210edit2feb10,0,1048507.story (accessed February 24, 2008).

Clayton, Mark. "US Plans Massive Data Sweep," *Christian Science Monitor*, February 9, 2006. http://www.csmonitor.com/2006/0209/p01s02-uspo.html (accessed January 27, 2008).

Cole, Mark. "Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK," *Surveillance and Society*, 2004, 2(2/2). http://www.surveillance-and-society.org/articles2(2)/signage.pdf (accessed September 23, 2007).

Constitution Project. *Guidelines for Public Video Surveillance*. Washington D.C.: The Constitution Project, 2007. http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf (accessed September 17, 2007).

Dalal, Reepal S. "Chipping Away at the Constitution: The Increasing use of RFID Chips Could Lead to an Erosion of Privacy Rights," *Boston University Law Review* 86 (2006): 485.

Delio, Michelle. "Privacy Activist Takes on Delta," *Wired*, March 5, 2003. www.wired.com/news/privacy/0,1848,57909,00.html (accessed January 26, 2008).

Dempsey, James X. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science and Technology* 8 (1997): 65.

Docknevich, Samuel K. "Technology Perspectives: CCTV Technology," *U. S. Department of Homeland Security, Privacy Office, Public Workshop CCTV: Developing Privacy Best Practices* (PowerPoint Presentation), December 17, 2007. http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Technology_Perspectives_Panel.pdf (accessed March 15, 2008)

Electronic Privacy Information Center. "Proposed 'Enhanced' Licenses are Costly to Security and Privacy," *EPIC Website-Spotlight on Surveillance*. September 2007. http://epic.org/privacy/surveillance/spotlight/0907/default.html (accessed January 26, 2008).

Electronic Privacy Information Center. "Spotlight on Surveillance: Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved," *EPIC Website*, August 2007. http://epic.org/privacy/surveillance/spotlight/0807/default.html (accessed January 26, 2008).

European Digital Rights. "France Adopts Anti-Terrorism Law," *EDRI-gram*, January 18, 2006. http://www.edri.org/edrigram/number4.1/frenchlaw (accessed September 28, 2007).

European Digital Rights. "French Adopts Anti-Terror Law Not Anti-Constitutional," *EDRI-gram.* February 2, 2006. http://www.edri.org/edrigram/number4.2/frenchlaw (accessed September 28, 2007).

European Digital Rights. "Public Debate on Draft Anti-Terror Act in Denmark," *EDRI-gram.* May 10, 2006. http://www.edri.org/edrigram/number4.9/denmark (accessed September 28, 2007).

Feder, Barnaby J. "Face Recognition Technology Improves," *The New York Times*, March 14, 2003. http://query.nytimes.com/gst/fullpage.html?res=9805E0D9103EF937A25750C0A9659C8B63 (accessed January 12, 2008).

Foucault, Michel. *Discipline and Punish, The Birth of the Prison*. New York: Vintage Books, 1995.

France, Elizabeth. *CCTV Code of Practice*. London: U.K. Government, 2000. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf (accessed September 23, 2007).

Frank, Thomas. "Security Devices Falter in Rail Tests," *USA Today*, 13 February 2007.

Gallagher, Caoilfhion. "CCTV and Human Rights: The Fish and the Bicycle? An Examination of *Peck v. United Kingdom* (2003) 36 E.H.R.R. 41," *Surveillance and Society* 2004, 2(2/3). http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf (accessed September 23, 2007).

Ganz, John S. "It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices," *Journal of Criminal Law and Criminology* 95 (2005): 1325.

Gershwin George and Ira Gershwin. "Someone to Watch Over Me." http://www.lyrics007.com/Gershwin%20George%20Lyrics/Someone%20To%20Watch%20Over%20Me%20Lyrics.html (accessed March 15, 2008).

Gill, Martin and Angela Spriggs. "Assessing the Impact of CCTV," *Home Office Research Study 29.* London: Home Office Research, Development and Statistics Directorate, February 2005. http://www.homeoffice.gov.uk/rds/surveys/hors292_survey.html (accessed September 25, 2007).

Gras, Marianne L. "The Legal Regulation of CCTV in Europe," *Surveillance and Society*, 2004, 2(2/2). www.surveillance-and-society.org/articles2(2)/regulation.pdf (accessed September 23, 2007).

Gross, Emanuel. "The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—the Proper Balance," *Cornell International Law Journal* 37 (2004): 27.

Gunnarsson, Helen W. "The Limited Lockstep Doctrine," *Illinois Bar Journal* 94, no. 7 (July 2006): 340.

Hampapur, Arun et. al. "Smart Video Surveillance: Exploring the Concept of Multiscale Spatiotemporal Tracking," *IEEE Signal Processing Magazine*. (March 2005). http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1406476 (accessed January 13, 2008).

Harris, David A. "Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology," *Temple Law Review* 69 (1996): 1.

Hempel, Leon, and Topfer, Eric. *CCTV in Europe, Final Report*. On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts, Working Paper No. 15. Berlin: Centre for Technology and Society, Technical University, 2004. http://www.urbaneye.net/results/ue_wp15.pdf (accessed May 11, 2007).

Herbert, William A. "No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?" *I/S: A Journal of Law and Policy for the Information Society* 2 (2006): 409.

IIT Research Institute. *Independent Technical Review of the Carnivore System*. Washington D.C.: U.S. Dept. of Justice, 2000. http://www.usdoj.gov/archive/jmd/carniv_final.pdf (accessed February 24, 2007).

Illinois Toll Highway Authority. *About I-Pass.* http://www.illinoistollway.com/portal/page?_dad=portal&_schema=PORTAL&_pageid=133,1471150 (accessed January 13, 2007).

Illinois Toll Highway Authority. *I-Pass, General Information, About I-Pass.* http://www.illinoistollway.com/portal/page?_dad=portal&_schema=PORTAL&_pageid=133,1471150 (accessed January 13, 2007).

Introna, Lucas D. and David Wood. "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems," *Surveillance and Society* 2, No. 2/3 (2004): 177. http://www.surveillance-and-society.org/cctv.htm (accessed January 12, 2008).

Kinzer, Steven. "Chicago Moving to 'Smart' Surveillance Camera," *The New York Times*, September 21, 2004. http://www.nytimes.com/2004/09/21/national/21cameras.html?ex=1190174400&en=8b9b4d48e88d756f&ei=5070 (accessed September 17, 2007).

Konkol, Mark J. "Do Cop Cameras Give Crooks the Blues: Jury is Still Out," *Chicago Sun Times*, March 5, 2006,

Kopel, David and Michael Krause. "Face the Facts Facial Recognitions Trouble Past and Troubling Future," *Reason Magazine*, 2002. http://www.reason.com/news/show/28539.html (accessed January 12, 2008).

Krouse,William J. "The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project," *CRS Report for Congress.* Washington D.C.: Congressional Research Service, 2004. http://www.fas.org/irp/crs/RL32536.pdf (accessed January 26, 2008).

Ku, Raymond Shih Ray. "Modern Studies in Privacy Law: Searching for the Meaning of Fourth Amendment Privacy After Kyllo v. United States: The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance," *Minnesota Law Review* 86 (2002): 1325.

LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 4th ed., 6 vols. St. Paul: Thomson/West, 2004.

Langland-Orban, Barbara, Etienne E. Pratch, and John T. Large. "Red Light Running Cameras: Would Crashes, Injuries and Automobile Insurance Rates Increase If They are Used in Florida" *Florida Public Health Review*, 2008: 5: 1. http://health.usf.edu/NR/rdonlyres/C1702850-8716-4C2D-8EEB-15A2A741061A/0/2008pp001008OrbanetalRedLightPaperMarch72008formatted.pdf (accessed March 18, 2008).

Lyon, David and Elia Zureik, eds. *Computers, Surveillance and Privacy.* Minneapolis, MN: University of Minnesota Press, 1996.

Marzouki, Meryem. "New French Anti-Terrorism Surveillance Plan," *EDRI-gram*, September 8, 2005. http://www.edri.org/edrigram/number3.18/France (accessed September 28, 2007);

McCahill, Michael and Clive Norris. *CCTV Systems in London, Their Structure and Practices*: *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts,* Working Paper No. 10 Hull, UK: Centre for Criminology and Criminal Justice, University of Hull, 2003. http://www.urbaneye.net/results/ue_wp10.pdf (accessed May 11, 2007).

McMahon, Patrick J. "Counterterrorism Technology and Privacy," *Cantigny Conference Series*. Chicago: McCormick Tribune Foundation, 2005.

Metropolitan Police Department, Washington D.C.. "MPDC's Closed Circuit Television (CCTV) System." http://mpdc.dc.gov/mpdc/cwp/view,a,1238,q,541201,mpdcNav_GID,1545,mpdcNav,%7C31748%7C.asp (accessed September 17, 2007).

National Law Enforcement and Corrections Technology Centers (NLECTC), "Innovations in Concealed Weapons Detection Technology," *TechBeat*, (Rockville, MD: National Institute of Justice, October 1997), http://www.nlectc.org/pdffiles/techbt.pdf (accessed December 4, 2007).

National Science and Technology Council, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics. *Biometrics Overview*. Available at http://www.biometrics.gov/docs/biooverview.pdf (accessed, February 24, 2007).

National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics. *Biometrics Frequently Asked Questions.* http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf (accessed January 26, 2008);

National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics. *Biometrics Overview*. http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Biometrics%20Overview.pdf (accessed January 26, 2008).

National Science and Technology Council; Committee on Technology; Committee on Homeland and National Security; Subcommittee on Biometrics. *Biometrics Frequently Asked Questions*. Available at http://www.biometrics.gov/docs/faq.pdf (accessed, February 24, 2007).

Ng, Rudy. "Catching Up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology," *Hastings Communications and Entertainment Law Journal* 28 (2006): 425.

Nieto, Marcus. *Public Video Surveillance: Is It an Effective Crime Prevention Tool?*. Sacramento: California Research Bureau. 1997. http://www.library.ca.gov/CRB/97/05 (accessed January 22, 2007).

Note, "In the Face of Danger: Facial Recognition and the Limits of Privacy Law," 120 *Harvard L. Rev.* (2007): 1871, 1876.

Nusimow, Avi. "Intelligent Video for Homeland Security Applications," *2007 IEEE Conference on Technologies for Homeland Security*. Institute of Electrical and Electrons Engineers, Inc.. New York. 2004. http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=4227766&arnumber=4227798&count=57&index=31 (accessed June 27, 2007).

O'Malley, Martin. "Mayor O'Malley Unveils New CitiWatch Control Center," *City of Baltimore Press Release*, May 12, 2005. http://www.ci.baltimore.md.us/news/press/050512.html (accessed September 17, 2007).

Otterberg, April A. "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment," *Boston College Law Review* 46 (2005): 661.

Phillips, David J. "Beyond Privacy: Confronting Locational Surveillance in Wireless Communication," *Communication Law and Policy* 8 (2003): 1.

Phillips, P. Jonathan et. al. "FRVT 2006 and ICE 2006 Large-Scale Results," *NISTIR 7408*. Gaithersburg, MD: National Institute of Standards and Technology, 2007. www.frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf (accessed January 12, 2008).

Posner, Richard. *Catastrophe*. New York: Oxford University Press, 2004.

Privacy International, *National Privacy Ranking 2006-European Union and Leading Surveillance Societies*, 2006. http://www.privacyinternational.org/survey/phr2005/phr2005spread.jpg (accessed March 14, 2008).

Reid, Angus. "French Want Increase in Surveillance Cameras," *Prison Planet.com*, September 6, 2007. http://www.prisonplanet.com/articles/september2007/060907Cameras.htm (accessed September 28, 2007).

Restatement (Second) of Torts. New York: West Publishing Company, 2006, § 652. http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm (accessed March 4, 2008).

Roberts, Chris. *Biometric Technologies: Palm and Hand*, 2006. www.ccip.govt.nz/newsroom/information-notes/2006/biometrics-technologies-palmhand.pdf (accessed January 21, 2008).

Rosen, Jeffery. "A Watchful State," *The New York Times Magazine*, October 7, 2001. http://query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63&sec=&spon=&pagewanted=1 (accessed January 13, 2008).

Schlosberg, Mark and Nicole A. Ozer. *Under the Watchful Eye: The Proliferation of Video Surveillance in California.* San Francisco: American Civil Liberties Union of Northern California, 2007. http://www.aclunc.org/issues/government_surveillance/aclu_issues_report_on_the_proliferation_of_video_surveillance_systems_in_california.shtml (accessed January 13, 2008).

Segura, Maricela. "Is Carnivore Devouring Your Privacy?" *Southern California Law Review* 75 (2001): 231.

Sessions, William S. and Michael German. "Cameras Alone Won't Stop Crime," *The Star Ledger*, August 19, 2007, http://www.nj.com/starledger/stories/index.ssf?/base/news-0/118750266928240.xml&coll=1#continue (accessed September 17, 2007).

Siegel, Loren; Perry, Robert A.; and Gram, Margret Hunt. *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight*. A Special Report by the New York Civil Liberties Union. New York: New York Civil Liberties Union, 2006, also available at http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf (accessed May 11, 2007).

Simmons, Ric. "The Powers and Pitfalls of Technology: Technology-Enhanced Surveillance by Law Enforcement Officials," *New York University Annual Survey of American Law* 60 (2005): 711.

———. "The Two Unanswered Questions of Illinois v. Caballes: How to Make the World Safe for Binary Searches," *Tulane Law Review* 80 (2005): 411.

Slobogin, Christopher. "Symposium: Public Privacy: Camera Surveillance and the Right to Anonymity," *Mississippi L. Rev.* 72 (Fall 2002): 213.

Smith, Glenn. "Cameras May Join City's Crime Fighting Arsenal," *The Post and Courier*, August 29, 2007. http://www.charleston.net/news/2007/aug/29/cameras_may_join_citys_crimefighting_ars14298/ (accessed September 17, 2007).

Smith, Pete. "Meth Detector Tested by Police May Fall into a Legal Grey Zone," *USA Today*, November 6 , 2007. http://www.usatoday.com/news/nation/2007-11-05-methgun_n.htm?loc=interstitialskip (accessed December 2, 2007).

Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," 44 *San Diego Law Review*, 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565#PaperDownload (accessed February 1, 2007).

St. Clair, Stacy. "Keeping up with Toms Who Peep Via High Tech," *Chicago Tribune*, December 26, 2007. http://pqasb.pqarchiver.com/chicagotribune/access/1403629641.html?FMT=FT&dids=1403629641:1403629641&FMTS=ABS:FT&type=current&date=Dec+26%2C+2007&author=Stacy+St+Clair&pub=Chicago+Tribune&desc=Keeping+up+with+Toms+who+peep+via+high+tech&pf=1 (accessed March 4, 2008).

Steinbock, Daniel J. "National Identity Cards: Fourth and Fifth Amendment Issues," *Florida Law Review* 56 (2006): 697.

Stewart, Ian. "Glasgow Attacks Seen Tied to London Bombs," *The Washington Post*, June 30, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/06/30/AR2007063000562.html (accessed September 17, 2007).

Taslitz, Andrew. "Enduring and Empowering: The Bill of Rights in the Third Millennium: The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions," *Law and Contemporary Problems* 65 (2002): 125.

Tien, Lee. "Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law," *DePaul University Law Review* 54 (2005): 873.

U. S. Department of Homeland Security, Transportation Security Administration. "Mitigating High Consequence Risk," *Mass Transit, Transportation Security Administration Official Website.* http://www.tsa.gov/what_we_do/tsnm/mass_transit/risks.shtm (accessed December 3, 2007).

———. "Secure Flight Program," *TSA Website-What We Do.* http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm (accessed January 26, 2008).

———. "Explosives Trace Detection," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/trace_portals.shtm (accessed December 3, 2007).

———. "Bottled Liquid Scanners," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/bls.shtm (accessed December 3, 2007).

———. "Mitigating High Consequence Risk," *What We Do, Transportation Security Administration Official Website.* http://www.tsa.gov/what_we_do/tsnm/mass_transit/risks.shtm (accessed December 3, 2007).

———. "Trace Portals," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/trace_portals.shtm (accessed December 3, 2007).

———. "Whole Body Imaging," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/body_imaging.shtm (accessed December 3, 2007).

———. "Millimeter Wave," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/mwave.shtm (accessed December 3, 2007).

———. "Backscatter," *Innovation & Technology, Transportation Security Administration Official Website.* http://www.tsa.gov/approach/tech/bscatter.shtm (accessed December 3, 2007).

———. *TSA Register Traveler: Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers, Version 3.1.* (January 2008), www.tsa.gov/assets/pdf/rt_standards_v3.1.pdf (accessed January 21, 2008).

———. *Transportation Worker Identification Credential (TWIC) Program: Frequently Asked Questions.* http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm#general (accessed January 21, 2008).

———. "TSA to Test New Passenger Pre-Screening," *TSA Website-Media Room.* August 26, 2004, http://www.tsa.gov/press/releases/2004/press_release_0496.shtm (accessed January 26, 2008).

———. *Notice of Proposed Rulemaking* [Docket No. TSA-2007-28572], August 8, 2007. http://www.tsa.gov/assets/pdf/secureflight_nprm.pdf (accessed January 26, 2008).

———. *US-VISIT Program.* http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed February 24, 2007).

———. *US-VISIT: How It Works.* http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm (accessed January 21, 2008).

———. *US-VISIT: Privacy Information.* http://www.dhs.gov/xtrvlsec/programs/editorial_0678.shtm (accessed January 21, 2008).

———. “REAL-ID Final Rule: Questions and Answers,” *DHS Website-Prevention and Protection.* http://www.dhs.gov/xprevprot/programs/gc_1172767635686.shtm (accessed January 27, 2008).

———. Office of the Inspector General. *ADVISE Could Support Intelligence Analysis More Effectively*, July 2, 2007. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-56_Jun07.pdf (accessed January 27, 2008).

———. Privacy Office. *Report to the Public Concerning the Multi-Sate Anti-Terrorism Exchange (MATRIX) Pilot Program.* Washington, D.C.: Government Printing Office, 2006. http://www.dhs.gov/xlibrary/assets/privacy/privacy-matrix-122006.pdf (accessed January 26, 2008).

————. “Fact Sheet: Enhanced Drivers Licenses,” *DHS Website-Press Room*, December 5, 2007. http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm (accessed January 27, 2008).

———. “Western Hemisphere Travel Initiative,” *DHS Website-Prevention and Protection.* http://www.dhs.gov/xprevprot/programs/gc_1200693579776.shtm (accessed January 27, 2008).

———. *Transportation Worker Identification Credential (TWIC) Program.* http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed February 24, 2007).

———. *Registered Traveler*. http://www.tsa.gov/what_we_do/layers/rt/index.shtm (accessed February 24, 2007).

U.S. Dept. of Homeland Security. “Minimum Standards for Drivers' Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes” *Final Rule*, Docket Number DHS-2006-0030 (6 CFR Part 37), January 10, 2008. http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part1_2008-01-11.pdf (Part 1); and http://www.dhs.gov/xlibrary/assets/real_id_final_rule_part2_2008-01-11.pdf (Part 2) (accessed January 28, 2008).

U. S. Federal Trade Commission, *Fair Information Practice Principle*, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (accessed February 2, 2008).

U. S. General Accounting Office. “Video Surveillance: Information on Law Enforcement’s Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington D.C.,” *Report to the Chairman, Committee on Government Reform, House of Representatives, 108th Cong., 2d sess.*, 2003. http://www.gao.gov/atext/d03748.txt (accessed January 22, 2007).

U. S. Government Accountability Office. “Aviation Security: Secure Flight Development and Testing Under Way, but Risk Should Be Managed as System Is Further Developed,” *Report to Congressional Committees*. Washington D.C.: U.S. Government Printing Office, 2005. http://www.gao.gov/new.items/d05356.pdf (accessed January 26, 2008).

U. S. Government Accountability Office. "Border Security: US VISIT Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry," *Report to Congressional Requestors.* Washington, D.C.: Government Printing Office, December 2006. http://www.gao.gov/new.items/d07248.pdf (accessed January 21, 2008).

U. S. Government Accountability Office. "Computer-Assisted Passenger Prescreening Faces Significant Implementation Challenges," *Report to Congressional Committees*, Washington, D.C.: Government Printing Office, February 2004. www.gao.gov/new.items/d04385.pdf (accessed January 24, 2008).

Vernick, Jon S.; Matthew W. Pierce; Daniel W. Webster; Sara B. Johnson and Shannon Frattaroli. "National Challenges in Population Health: Technologies to Detect Concealed Weapons: Fourth Amendment Limits on a New Public Health and Law Enforcement Tool," *Journal of Law, Medicine and Ethics* 31 (2003): 567.

Warren, Samuel D., and Louis D. Brandeis "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.

Washburn, Gary. "Another 100 Cameras Bound for Street," *Chicago Tribune*, October 4, 2006. http://pqasb.pqarchiver.com/chicagotribune/access/1139976581.html?dids=1139976581:1139976581&FMT=ABS&FMTS=ABS:FT&type=current&date=Oct+4%2C+2006&author=Gary+Washburn%2C+Tribune+staff+reporter&pub=Chicago+Tribune&edition=&startpage=2&desc=Another+100+cameras+bound+for+street+ (accessed September 17, 2007).

Webster, William R. "The Diffusion of Closed Circuit Television in the UK," *Surveillance and Society*, 2004, 2(2/3), http://www.surveillance-and-society.org/articles2(2)/diffusion.pdf (accessed September 20, 2007).

Welsh, Brandon C., and David P. Farrington. "Crime Prevention Effects of Closed Circuit Television: A Systematic Review," *Home Office Research Study 252* (London: Home Office Research Development and Statistics Directorate. August 2002. www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf (accessed January 13, 2008).

Williams, Robert F. "State Courts Adopting Federal Constitutional Doctrine: Case-by-Case Adoptionism or Prospective Lockstepping," *William and Mary Law Review* 46 (2005): 1499.

Wolfe, Jim. "Carnivore Gets a New Name," *Reuters*, February 14, 2001. http://www.metrostate.com/library/stories/01/feb/msnbc.htm (accessed January 26, 2008).

Woo, Christopher, and Miranda So. "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance," *Harvard Journal of Law and Technology* 15 (2002): 521.

Wood, David Murakami, ed. *A Report on the Surveillance Society: Full Report*, Report for the Information Commissioner by the Surveillance Studies Network. London: U.K Government, 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed September 25, 2007).

Xinhua. "France to Triple CCTV Surveillance Across the Country," *Peoples Daily Online*, July 27, 2007. http://english.peopledaily.com.cn/90001/90777/6225229.html (accessed March 14, 2008).

——— "French Parliament Approves Video Surveillance Powers," *Peoples Daily Online*, November 11, 2005. http://english.people.com.cn/200511/25/eng20051125_223757.html (accessed September 28, 2007).

Zimbardo, Philip. *The Lucifer Effect: Understanding How Good People Turn Evil*. New York: Random House, 2007.

Primary Sources

United States Supreme Court Decisions

Berger v. New York, 388 U.S. 41 (1967).

Bivens v. Six Unknown Federal Narcotics Agents, 403 U.S. 388 (1971).

California v. Ciraolo, 476 U.S. 207 (1986).

City of Dallas v. Stanglin, 490 U.S. 19 (1989).

City of Indianapolis v. Edmonds, 531 U.S. 32 (1990).

Coolidge v. New Hampshire, 403 U.S. 465 (1971).

Davis v. *Mississippi*, 394 U.S. 721, 727 (1969).

Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

Florida v. Riley, 488 U.S. 445 (1989).

Gerstein v. Pugh, 420 U.S. 103 (1975).

Griffin v. Wisconsin, 483 U.S. 868 (1987).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Hiibel v. Sixth Judicial Circuit Court, Humboldt County, 542 U.S. 177 (2004).

Illinois v. Caballes, 543 U.S. 405 (2005).

Katz v. United States, 389 U.S. 347 (1967).

Kyllo v. United States, 533 U.S. 27 (2001).

Michigan v. Sitz, 496 U.S. 444 (1990).

Miranda v. Arizona, 384 U.S. 436 (1966).

NAACP v. Alabama, 357 U.S. 449 (1957).

Oliver v. United States, 466 U.S. 170 (1984).

Olmstead v. United States, 277 U.S. 438 (1928).

Payton v. New York, 445 U.S. 573 (1980).

Roberts v. United States Jaycees, 468 U.S. 609 (1984).

Roe v. Wade, 410 U.S. 113 (1973).

Scott v. Harris, Slip Op. No. 05-1631, 550 U.S. ___ (April 30, 2007).

Silverman v. *United States*, 365 U. S. 505 (1961).

Smith v. Maryland, 442 U.S. 735, 743 (1979).

Terry v. Ohio, 392 U.S. 1 (1968).

United States v. Hester, 265 U.S. 57 (1924).

United States v. Jacobsen, 466 U.S. 109 (1984).

United States v. *Karo*, 468 U. S. 705 (1984).

United States v. Knotts, 460 U.S. 276 (1983).

United States v. Place, 462 U.S. 696 (1983).

Whelan v. Roe, 429 U.S. 589 (1977).

United States Circuit Court of Appeals Decisions

Alliance to End Repression v. City of Chicago, 237 F.3d 799, 801 (7th Cir. 2001)

Alliance to end Repression v. City of Chicago, 561 F. Supp. 537, 539 (N.D. Ill. 1982)

Barry v. Fowler, 902 F.2d 770 (9th Cir. 1990)

Bourgeois v. Peters, 387 F.3d 1303 (11th Cir. 2004).

Foster v. Metropolitan Airports Commission, 914 F.2d 1076 (8th Cir. 1990)

Johnston v. Tampa Sports Auth., 490 F.3d 820 (11th Cir. 2007).

United States v. Aukai, 497 F.3d 955 (9th Cir. 2007) (en banc).

United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

State Court Decisions

Oregon v. Campbell, 759 P.2d 1040 (Or. 1988).

State v. Jackson, 76 P.2d 217 (Wash. 2003) (*en banc*).

Foreign Court Decision

Peck v. United Kingdom, 36 E.H.R.R. 41 (2003).

Federal Statutes

The Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (2000).

The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701-2710 (2000).

42 U.S.C. § 1983

42 U.S.C. § 1988

Public Law 109-13, 119 Stat. 231,302 (May 11, 2005), 49 U.S.C. § 30301.

State Statutes

Illinois Freedom of Information Act, 5 ILCS 140 *et seq.*(2006).

Illinois Local Records Retention Act, 50 ILCS 205/1 *et seq.*(2006).

Public Act 093-0851, codified at 720 ILCS 5-26/4 (2008). http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=093-0851 (accessed March 2, 2008).

Foreign Statutes

European Parliament, Draft European Parliament Resolution on the First Report on the Implementation of the Data Protection Directive (95/46/EC), February 24, 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ep_report_cappato_04_en.pdf (accessed January 26, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California