3

Federalism, Privacy Rights, and Intergovernmental Management of Surveillance: Legal and Policy Issues

Michael W. Hail
Morehead State University,
United States of America

1. Introduction

The legal and policy issues involved with surveillance require recognition of the complexity of governance in United States intergovernmental system. With over 83,000 units of government, the U.S. intergovernmental system is complex and fragmented. And even within levels, much less across them, the United States system of federalism is one of limited government combined with an interdependent system of checks and balances. Rights are guaranteed by constitutions and court systems at two levels, operating concurrently. Additionally, the executive agencies across all levels are increasing engaged in collecting data on individuals. The myriad systems of data collection and management require a careful review for those developing, marketing, servicing, or using surveillance technologies.

2. Federalism and public policy

The legal rights of those operating surveillance systems are weighed against the civil rights of individuals being observed. This complex balance of rights exists in a multi-level grid of policymaking at the federal, state, and local levels of government in the United States (Hail, 2009). In addition to federalism distributing policy across levels of government, the U.S. constitutional system has always taken a sectoral approach to the regulation of privacy and a common law approach to privacy jurisprudence (Paruchuri et al., 2009).

In considering legal and regulatory issues in the United States, one must remember that to develop a comprehensive understanding of privacy not only must the federal judiciary be examined, but also the 50 states treatment of privacy issues related to technology and surveillance. This would include the dimensions of constitutional roles, bureaucratic organization, and policy authorities and the principal regulatory infrastructure for Third Party Federalism (Hail, 2004). The state government role is more significant for identification of individuals and the overall content of privacy concerns is more substantial at the sub-national level. As a recent article discussing state policy among state CIOs noted, "States' role in E-Authentication is greater than at the federal level" (Sternstein, 2005). These sub-national governments are primarily responsible for implementation of domestic

homeland security response and are the governments of "first responders". The use of technology by these governments involves intergovernmental finance instruments and the complex network of federalism policymakers.

Protection of privacy in video surveillance addresses privacy requirements for civil liberties protection at the multiple levels of government. It should be noted that over half of the States have an enumerated right to privacy protection in their constitutions or statutes that extends or exceeds the federal right to privacy. Additionally, legal concerns are thereby addressed for broad adoption of the privacy protecting technology and its effective use by government for homeland security and law enforcement.

This assessment of the public management issues for surveillance and data management for multi-jurisdictional environments provides important considerations for both public officials and scientists. The origins of political rights under constitutional government systems resulted in non-uniformity of political rights and legal and regulatory requirements (Hail and Lange, 2010). Surveillance technology requires a regulatory balance for the protection of individuals and the commercialization of technology. The research results indicate political culture for innovation and new technology development has a positive correlation with governance systems of federalism.

3. Recent survey research findings

Protection of privacy in video surveillance addresses constitutional and civil liberties protections across the institutions of federalism. In addition to the federally protected rights in the 1st, 4th, 5th, and 9th Amendments, it must be noted that over half of the States have an enumerated right to privacy protection in their constitutions or statutes that extends or exceeds the federal right to privacy. Additionally, legal concerns are thereby addressed for broad adoption of the privacy protecting technology and its effective use by government for homeland security and law enforcement. To assess these issues in the general population as well as among homeland security and law enforcement agencies, a surveys were conducted, as well as focus groups and interviews.

In the general population survey, citizens across demographic groups were comfortable with expansion of government video surveillance if it protected privacy rights. The survey research was conducted utilizing a modified list-assisted Waksberg-Mitofsky random-digit dialing procedure for sampling and the population surveyed was non-institutionalized Kentuckians eighteen years of age and older.[i] The margin of error is +/- 3.3 percent at the 95 percent confidence interval. SRC response rate was 31.1% and CASRO rate was 38.1%. Total N=3243 with 904 completes.

The respondents were asked, "Do you have a video security system that is used routinely?" The results reflected that 55% of employed Kentuckians have an operative video surveillance system at their workplace. We then asked of those employed, "Would you be interested in a video surveillance system at work if you knew it could protect an individual's privacy?" The solid majority of 60% expressed that they were interested in privacy protecting video surveillance. There was clear recognition that video surveillance has become a regular feature of public and private workplace environments.

Urban residents, those in higher income levels, and those with advanced education attainment all were more disposed to privacy protecting video technology.

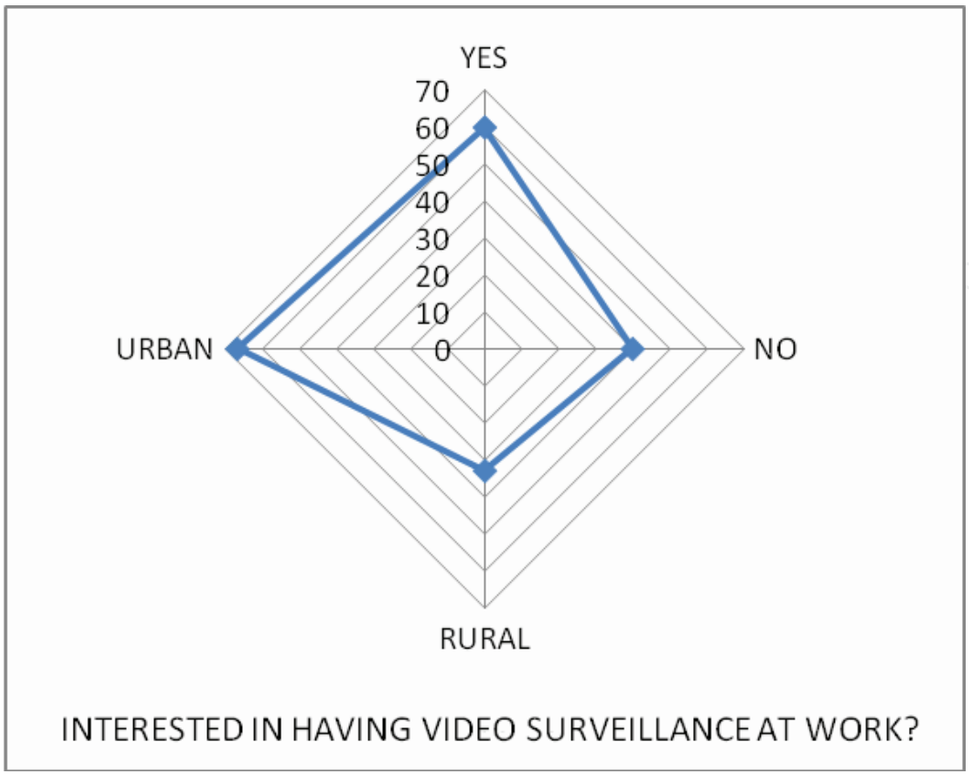


Fig. 1. Urban and Rural Views of Workplace Video Security

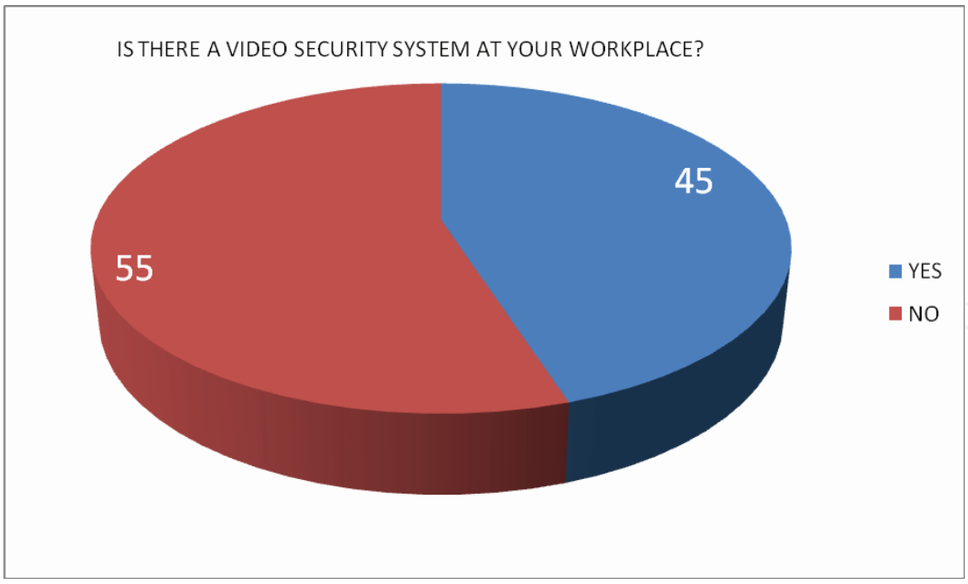


Fig. 2. Video Security at the Workplace

Additionally, focus groups of law enforcement, first responders, hospitals, and public infrastructure managers have reflected strong interest in privacy protecting video technology. Contact was made with 25 critical infrastructure officials from across Kentucky and site visits conducted with six critical infrastructure locations. Two focus groups were

held and nineteen participants from 8 local, state, and federal agencies attended. The focus groups were asked a series of questions to evaluate their knowledge of civil liberties with regard to privacy protection and the use of video evidence. They were also asked, "Would you be interested in a video surveillance system that could protect an individual's privacy?" 100% of the attendees responded favorably and several expressed interest in implementation of privacy protecting video surveillance at their infrastructure facilities.

4. Judicial policy and intergovernmental management

There have been several important court rulings that establish the judicial policy framework for privacy and surveillance. In all cases, state courts must defer to the establishment of civil liberties by federal courts under the constitution's supremacy clause. As such, the analysis of judicial policy focuses upon federal policy parameters.

MAJOR FEDERAL PRIVACY RULINGS

Olmstead v. United States (1928)
Bartnicki v. Vopper (2001)
Brendlin v. California (2006)
Georgia v. Randolph (2006)
Hudson v. Michigan (2006)
Cutter v. Wilkinson (2005)
Davenpeck v. Alford (2004)
San Diego v. Roe (2004)
Boy Scouts of America v. Dale (2000)
Lawrence and Garner v. Texas (2003)
Bowers v. Hardwick (1986)
Waller v. Georgia (1984)
Katz v. United States (1967)
Stanley v. Georgia (1969)
Wilson v. Layne (1999)
Los Angeles County, California v. Max Rettele (2007)
Goodridge v. Department of Public Health (2003)
Troxel v. Granville (2000)
Planned Parenthood v. Casey (1992)

Table 1. Major Federal Judicial Rulings on Privacy

The American legal conceptualization of privacy is derivative of a tradition of privacy theory reaching from Plato and Aristotle through John Locke and John Stuart Mill. But the American legal jurisprudence for privacy rights has a central focus on the work of Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article (Warren and Brandeis, 1890). Warren and Brandeis developed a federal jurisprudence for privacy based upon the implied powers of the constitutions derivative of the Bill of Rights. They stated, "the right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel," and that "the law would

probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage," and they conclude that the right to privacy is to "protect the privacy of private life" (Warren and Brandeis, 1890). The right to privacy was in these terms understood as a tort where redress was a matter of civil concern rather than criminal. The rapid development of technology in the twentieth century created circumstances where the courts were challenged to apply this legal reasoning well after the technology had reached a broad application in society.

The state courts, like state governments across all areas of public policy, have generally been more advanced in dealing with judicial policy than their federal counterparts. In 1905, in *Pavesich v. New England Life Insurance Co.*, the Georgia Supreme Court created a common law right of privacy when the New England Life used the Pavesich 's name and picture, without consent, to advertise insurance services. The Georgia Court followed Warren and Brandeis, interpreted "the right to be let alone" in their ruling. This was followed in 1928 by U.S. Supreme Court case of *Olmstead v. United States.*, which established the first major federal court ruling. In *Olmstead*, federal law enforcement agents installed wiretaps in the basement of Olmstead's building as well as the streets near his home without obtaining a warrant and the evidence resulted in Olmstead being convicted. The Court held that neither the Fourth nor Fifth Amendment rights of the recorded parties were violated. The use of wiretapped conversations as incriminating evidence did not violate their Fifth Amendment protection against self incrimination because they were not forcibly or illegally made to conduct those conversations. Instead, the conversations were voluntarily made between the parties and their associates. The Fourth Amendment rights were not infringed because mere wiretapping does not constitute a search and seizure under the meaning of the Fourth Amendment. These terms refer to an actual physical examination of one's person, papers, tangible material effects, or home but not their conversations. *Olmstead* was overturned in 1967 by *Katz v. United States*. In *Katz v. United States*, the Supreme Court redefined a search. Recognizing that the Fourth Amendment protects "people, not places," the Court said that a search occurs whenever the government intrudes into a person's reasonable expectation of privacy. This is a complete change from the *Olmstead* Court which in essence said that there was no expectation of privacy in conversations.

The Fourth Amendment to the U.S. Constitution has become a fertile ground for privacy litigation. The Fourth Amendment prohibits unreasonable searches and seizures by the government. This is combined with the protections not enumerated in the Ninth Amendment where the residual rights not addressed in the constitution are reserved to the people. The Fourth Amendment does not prohibit all searches, only ones considered unreasonable. The Supreme Court has made this inquiry simple. Any search made without a warrant is per se unreasonable, unless it can be justified by one of several narrowly defined exceptions to the warrant requirement.

The case law has been supplemented by several Congressional Acts over the last 50 years. Some of the major acts include the Federal Wiretap Act in 1968 (FWA), Electronic Communications Privacy Act of 1986 (ECPA), The Foreign Intelligence Surveillance Act of 1978 (FISA), and the Patriot Act of 2002 (PAT).

In order for surveillance data to be admitted in a judicial trial, the technology behind the video must stand up to judicial scrutiny as well. The history of scientific evidence admitted in court starts in 1923 with the case of *Frye v. United States.* This was a case from the Court of Appeals of the District of Columbia which held that evidence could be admitted in court only if "the thing from which the deduction is made" is "sufficiently established to have

MAJOR FEDERAL VIDEO & WIRED RECORDING RULINGS
Bartnicki v. Vopper, 121 S. Ct. 1753 (2001)
Baugh v. CBS, 828 F. Supp. 745 (N.D. Cal. June 22, 1993)
Boehner v. McDermott, 22 Fed. Appx. 16 (D.C. Cir. 2001)
Copeland v. Hubbard Broadcasting, Inc., 526 N.W.2d 402 (Minn. Ct. App. Jan. 24, 1995)
Desnick v. ABC, 44 F.3d 1345 (7th Cir. 1995)
Food Lion Inc. v. Capital Cities/ABC Inc., 194 F.3d 505 (4th Cir. 1999)
Hornberger v. American Broadcasting Company, Inc., 799 A.2d 566 (N.J. App. 2002)
Krauss v. Globe International, No. 18008-92 (N.Y. Sup. Ct. Sept. 11, 1995)
Medical Laboratory Management Consultants v. American Broadcasting Company, Inc., 306 F.2d 806 (9th Cir. 2002)
Oregon v. Knobel, 777 P.2d 985 (Or. 1989), acquitted on retrial, No. 86-545 (Ore. Dist. Ct. Josephine Cty. Jan. 9, 1991)
Pennsylvania v. Duncan, CR78-92 (Pa. 11th Jud. Dist., charges dismissed, March 26, 1992)
PETA v. Bobby Berosini, Ltd., 895 P.2d 1269 (Nev. 1995)
Sussman v. American Broadcasting Cos., Inc., 186 F.3d 1200 (9th Cir. 1999)
In the matter of Entercom New Orleans License, LLC, FCC File No. EB-01-IH-0099 (2002)
In the Matter of Use of Recording Devices in Connection with Telephone Service, 2 FCC Rcd 502 (1987)
Broadcast of Telephone Conversations, 47 C.F.R. §73.1206 (1989)
P.L. 99-508 (The Electronic Communications Privacy Act of 1986), amending 18 U.S.C. §§ 2510 et seq.

Table 2. Major Federal Judicial Rulings on Recording Technologies

gained general acceptance in the particular field in which it belongs. "*Frye* dealt with a systolic blood pressure deception test, which was the forerunner of the polygraph test. In 1923, this blood pressure test was not widely accepted among scientists, and so the *Frye* court ruled it could not be used in court.

However, in 1993, the United States Supreme Court changed the long-standing law of admissibility of scientific expert evidence by rejecting the Frye test as inconsistent with the Federal Rules of Evidence in the case of *Daubert v. Merrell Dow Pharmaceuticals*. The Court held that the Federal Rules of Evidence and not *Frye* were the standard for determining admissibility of expert scientific testimony. *Frye's* "general acceptance" test was superseded by the Federal Rules' adoption. Rule 702 is the appropriate standard to assess the admissibility of scientific evidence. The Court derived a reliability test from Rule 702.

Under *Daubert*, the admissibility of expert testimony is to be more rigorously scrutinized by the trial judge to determine whether it meets the requirements of Fed. R. Evid. 702, which

provides "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as a expert by knowledge, skill, experience, training or education, may testify thereto in the form of an opinion or otherwise." In order to qualify as scientific knowledge, an inference or assertion must be derived by the scientific method and any proffered testimony must be supported by appropriate validation. In short, the requirement that an expert's testimony pertaining to scientific knowledge establish a standard of evidentiary reliability is the requirement for admissibility. The Supreme Court later clarified the expert testimony could not be highly focussed or developed for the case in question, but performed research independent of the litigation. Now, any expert must provide verifiable evidence that the expert's testimony is based on scientifically valid principles with possible objective sources of such verification include learned treatises, the policy statement of a professional association, and published articles in reputable scientific journals.

These complex judicial policies for the use of surveillance technology and its admissability make the work of executive branch agencies and bureaucratic managers ever more challenging. Not only the bargaining of juridictional issues and inter-agency politics, but the legal requirements for compliance make these use of surveillance technology ever more specialized and politically complex.

5. The interdependence of devolution of policy in American federalism and intergovernmental management of technology and data

In the U.S., federalism distributes sovereignty between the national government and those of the States. The intergovernmental system of policy making ensures cooperation and conflict within and between levels of government. Against this complex political system, one must understand the constitutional parameters placed upon these governments by the constitution. The implementation of any major surveillance technology requires regulation of the use of that technology by multiple governments protecting the rights of commerce in the market for that technology and the civil liberties of those it might be used upon.

The Bill of Rights remains central to the federal jurisprudence for privacy rights. The Founding Fathers were divided as to whether there should be a "bill of rights." In fact, the Philadelphia Convention of 1787 completed its work without including any such explication of rights, though they had considered and subsequently rejected enumeration of rights. "George Mason almost as an afterthought in the last days of the convention brought the issue up, …[and subsequently] it was defeated by every state"(Wood, 1969). Even as the ratification debates produced a compromise between leading federalists and anti-federalists that included such prominent founders as James Madison, other federalists such as Roger Sherman, the author of the Connecticut Compromise that created modern American federalism, remained opposed to a "bill of rights" as unnecessary. Even after the Constitution is ratified and the first ten amendments added, it should be remembered that it was a natural rights understanding of "rights" that informed the Founding Fathers view of the Constitution. As James Burnham phrased it, "these rights, in short, are limits, not powers" (Burnham, 1959). Thus, the constitutional theory of the Founding Fathers was premised upon limitations to the national powers as reflected in the amendments in the Bill of Rights. These limitations on government are unevenly applied to other entities and individuals in society, and the exponential growth of technology has made this moreso.

As Elazar and other federalism scholars have noted, the States serve as a laboratory for policy experimentation and for addressing the often unique, heterogeneous needs resulting from local and regional diversity (Elazar, 1987). Even after a century of nationalizing policy authority, the States play a significant, meaningful, and constitutionally guaranteed role in the intergovernmental policy process that both affirms and extends the rights and limitations that serve as guarantees of liberty in the Bill of Rights and the constitution. The enduring challenge of public administration and policy makers is how to preserve this constitutional framework in the face of accelerated technology applications that challenge civil liberties. The management of growing volumes of data by government agencies and regulation of surveillance technologies in an integrated legal challenge for constitutional governments and at the center of both remains the right of privacy.

6. References

Burnham, James (1959). Congress and the American Tradition. Regnery Publishing. Washington, DC:

Elazar, Daniel J. (1987). Exploring Federalism. University of Alabama Press. Tuscaloosa.

Hail, Michael W. (2009). "Bush's New Nationalism: The Life and Death of New Federalism." Perspectives on the Legacy of George W. Bush. Michael Orlov Grossman and Ronald Eric Matthews Jr., Editors. Cambridge Scholars Publishing. Newcastle upon Tyne.

Hail, Michael W. (2004). "Measuring Devolution Through Third Party Federalism." Proceedings of the 2004 meeting of the Mid-West Political Science Association.

Hail, Michael., and Lange, Stephen. (2010). Federalism and Representation in the Theory of the Founding Fathers: A Comparative Study of U.S. and Canadian Constitutional Thought. *Publius: The Journal of Federalism*, Special Issue (February 25), 1-24.

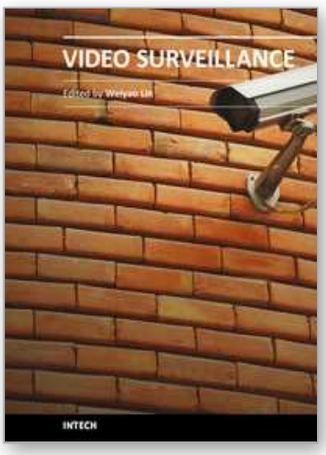
Paruchuri, Jithendra K., Sen-ching S. Cheung, and Michael W. Hail. (2009). "Video Data Hiding for Managing Privacy Information in Surveillance Systems." *EURASIP Journal on Information Security*. Volume 2009 (2009), Article ID 236139, 18 pages.

Sternstein, Aliya. (2005). "NASCIO faces authentication." Jan. 7, 2005. http://fcw.com/geb/articles/2005/0103/web-privacy-01-07-05.asp.

Warren, Samuel D. and Louis D. Brandeis (1890). "The Right of Privacy", 4 Harvard Law Review. 193. Boston, Massachusetts.

Wood, Gordon. (1969). The Creation of the American Republic 1776-1787. W.W. Norton & Co. New York.

[i] The survey was a cooperative effort through the University of Kentucky annual Kentucky Survey and the research was sponsored by a grant from the US Department of Homeland Security through the National Institute for Hometown Security.



Video Surveillance
Edited by Prof. Weiyao Lin

ISBN 978-953-307-436-8
Hard cover, 486 pages
Publisher InTech
Published online 03, February, 2011
Published in print edition February, 2011

This book presents the latest achievements and developments in the field of video surveillance. The chapters selected for this book comprise a cross-section of topics that reflect a variety of perspectives and disciplinary backgrounds. Besides the introduction of new achievements in video surveillance, this book also presents some good overviews of the state-of-the-art technologies as well as some interesting advanced topics related to video surveillance. Summing up the wide range of issues presented in the book, it can be addressed to a quite broad audience, including both academic researchers and practitioners in halls of industries interested in scheduling theory and its applications. I believe this book can provide a clear picture of the current research status in the area of video surveillance and can also encourage the development of new achievements in this field.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen