epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

National Network to End Domestic Violence
Training of Trainers 2007
Saint Louis, MO
August 13-16
Where the Surveillance Society and People Collide?
Lillie Coney

The infrastructure of the new surveillance society is a composite of commercial and public sector interests. The objective is to optimize the collection, analysis, and sharing of information on individuals by public and private entities. To achieve this objective underlying communication infrastructure must support access to identity data networks. Some believe that the right mix of technologies will enable the authentication of identification documents, facilitate checkpoints to screen for persons on watch lists, control border entries and exits, track purchases, use of credit, better coordinate activities of private and government entities, or in advance applications for CCTV technology identify a face in a crowd using facial recognition. For example:

The REAL ID and Voter Photo ID Requirements

The United States is moving toward a uniform ubiquitous identity document that is issued by state and territorial authorities, but must meet federal requirements for uniformity. The law requires interoperability among identity document issuing authorities, law enforcement, and federal government agencies. In addition, proof of identity requirements includes documents establishing citizenship or legal residency status. Documents failing to meet these requirement must state "on its face that it may not be accepted by any Federal agency for federal identification or any other official purpose; and uses a unique design or color indicator to alert Federal agency and other law enforcement agencies."[1]

The REAL ID Act of 2005 creates a de facto national identification card. Ostensibly voluntary, it would become mandatory, as those without the card would face suspicion and increased scrutiny. It is a law imposing federal technological standards and verification procedures on state driver's licenses and identification cards, many of which are beyond the current capacity of the federal government, and mandating state compliance by May 2008. In fact, REAL ID turns state DMV workers into federal

[1] Government Printing Office, Public Law 109-13, Making Emergency Appropriations for Defense the War on Terror, and Tsunami Relief, and other purposes, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109

immigration officials, as they must verify the citizenship status of all those who want a REAL ID-approved state driver's license or identification cards.

REAL ID has taken on a public policy life of its on—in advance of the document being issued there are proposals that the document should be used to control access to voting in public elections.

Voter Photo Identification

According to the CalTech MIT study*, Voting: What Is, What Could Be*, between 4 and 6 million votes were lost in the 2000 election.[2] The study attributed the loss in part to problems with voter registration and polling place practices. In 2004, EPIC identified two general problem areas with voter registration during the elections: lack of transparency and voter privacy regarding the public administration of voter registration.[3] The solutions to voter registration and Election Day problems lie not in additional legal barriers between American voters and the ballot box but in increased training and funding for local election administration. There is no evidence that local election administrators face drastic challenges to the identification of voters. Registering to vote and the act of casting a ballot must, by law, cost nothing to the voter. Therefore, and for the reasons stated above, increased voter identification requirements are unnecessary, possibly unconstitutional, and disregard voters' privacy rights.

Identity (ID) cards are in use in one form or another in virtually all countries of the world. The type of card, its functions, and integrity vary enormously. While several countries have official, compulsory, national ID cards that are used for a variety of purposes, many countries do not. Nationwide ID systems are established for a variety of reasons. Race, politics and religion often drive the deployment of ID cards. The fear of insurgence, religious differences, immigration, or political extremism have been all too common motivators for the establishment of ID systems that aim to force undesirables in a State to register with the government, or make them vulnerable in the open without proper documents.

In recent years technology has rapidly evolved to enable electronic record creation and the construction of large commercial and state databases. A national identifier contained in an ID card enables disparate information about a person that is stored in different databases to be easily linked and analyzed through data mining techniques. ID cards are also becoming "smarter" – the technology to build microprocessors the size of postage stamps and put them on wallet-sized cards has become more affordable. This technology enables multiple applications such as a credit card, library card, health care card, driver's license and government benefit program information to be all stored on the same national ID along with a password or a biometric identifier.

---

[2] THE CALTECH/MIT VOTING TECHNOLOGY PROJECT, VOTING, WHAT IS, WHAT COULD BE (California Institute of Technology and The Massachusetts Institute of Technology Corporation) (2001) available at http://www.vote.caltech.edu/media/documents/july01/July01_VTP_Voting_Report_Entire.pdf.

[3] Ralph Vartabedian, LOS ANGELES TIMES, State Laws Unjustly Bar Voters, ACLU Says; Oct 19, 2004, at A16.

Governments in Finland, Malaysia, and Singapore have experimented with such "Smart" ID cards. In July 2002, the Labor government in the United Kingdom launched a six-month public consultation process on whether the United Kingdom should adopt an "entitlement card" with similar features. Critics contend that such cards, especially when combined with information contained in databases, enable intrusive profiling of individuals and create a misplaced reliance on a single document, which enables precisely the type of fraud the cards are meant to eliminate.

The Electronic Privacy Information Center (EPIC) opposes the use of the REAL ID as a voter authentication document. EPIC is on the record as being in opposition to Georgia's use of government-issued photo ID as the sole means of casting a ballot in a state or federal election. EPIC said that the Georgia voting photo identification law encroaches on privacy, would discourage voter turnout, and is inconsistent with the federal Help America Vote Act. Under the 1965 Voting Rights Act, Georgia is required to receive Justice Department approval before making any changes to its voting laws. The list of approved government photo identification documents does not include state and federal identification documents that would otherwise establish eligibility to vote. The State of Georgia does not intend to accept federal or state issued checks, employment identification documents, state college or university identification, utility bills, sworn affidavits, or public assistance identification. EPIC finds the Georgia voting ID law and the Carter-Baker Commission recommendation on REAL ID as the sole voting identification requirement objectionable, a barrier to the right to vote, and unnecessary in its encroachments on voters' privacy rights.

The REAL ID will not be a definitive document on citizenship, but a test of one's ability to successfully navigate the course and receive a document based on the high bar established by the law. The law is lacking in that there is no requirement that local and state agencies receiving requests reply to the state DMVs attempting to verify source documents presented by applicants. Further the language of the law regarding an inability to verify documents will be ripe for abuse:

> (11) In any case in which the State issues a driver's license or identification card that does not satisfy the requirements of this section, ensure that such license or identification card--(A) clearly states on its face that it may not be accepted by any Federal agency for federal identification or any other official purpose; and (B) uses a unique design or color indicator to alert Federal agency and other law enforcement personnel that it may not be accepted for any such purpose.

Second, the requiring of a REAL ID as the sole means of authenticating voters makes the penalty for not having a REAL ID too costly for a popular democracy. Third, states can choose to opt-out of the REAL ID program, but the Act mandates that licenses from opt-out states cannot be used as identification for federal purposes. If Congress follows the Commission's recommendation that voters participating in federal elections can use only

the Real ID card as identification, then residents of states that reject the REAL ID program will not have acceptable voter identification.

As the deadline for compliance draws closer, more states are opting out of the controversial REAL ID national identification system. Arkansas, Colorado, Georgia, Hawaii, Idaho, Illinois, Maine, Missouri, Montana, Nebraska, Nevada, New Hampshire, North Dakota, South Carolina, and Washington have all passed anti-REAL ID legislation. The public resistance to REAL ID also is growing. In May, more than 60 organizations and 215 blogs joined a campaign to submit comments against REAL ID. There are bills in both the U.S. House and Senate to repeal the national identification scheme. EPIC and 24 experts in privacy and technology submitted detailed comments explaining the many privacy and security threats raised by the REAL ID Act.[4]

The Carter-Baker Commission erroneously assumes that if states make the REAL ID available to indigent voters then the issue of access will be addressed. The history of voting rights in this nation should not be ignored. The adoption of the 15th Amendment prohibits the denial of voting rights based on race.[5] The 19th Amendment prohibits the denial of the right to vote based on gender. [6] The 24th Amendment prohibits the poll tax for federal elections.[7] The 26th Amendment prohibits the denial of voting rights of those 18 and older base on age.[8] Each Amendment is a testament to the Federalists and Antifederalists struggle to define democracy in the United States.

The Carter-Baker Recommendations cite as the reason for a photo ID requirements the curbing of voter fraud is not substantiated by empirical evidence. We believe that the proposed recommendation if acted upon will prevent certain citizens from accessing the polls, will more likely reduce than enhance voting integrity. Although we recognize the Commission's interest in verifying voter identity, we believe that compelling qualified citizens to acquire and present state-issued picture identification cards at voting polls

---

[4] EPIC, Comments, Department of Homeland Security, REAL ID Regulations, June 8, 2007, available at http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf

[5] Amendment XV to the Constitution provides:

1. The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude.
2. The Congress shall have power to enforce this article by appropriate legislation.

[6] Amendment XIX to the Constitution provides:

1. The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.
2. Congress shall have power to enforce this article by appropriate legislation

[7] Amendment XXIV to the Constitution provides:

1. The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay any poll tax or other tax.
2. The Congress shall have power to enforce this article by appropriate legislation.

[8] Amendment XXVI to the Constitution provides:

1. The right of citizens of the United States, who are eighteen years of age or older, to vote shall not be denied or abridged by the United States or by any State on account of age.
2. The Congress shall have power to enforce this article by appropriate legislation.

represents an unjustified privacy infringement. We believe that the Georgia experience in not being able to present evidence of the type of election fraud intended to be addressed by the proposed state ID standard is indicative of the current debate on this issue. The Georgia state legislature has not cited evidence of actual effects of voter identity fraud on outcomes of Georgia elections. Indeed, Georgia's former Secretary of State Cathy Cox could not recall even "one documented case of voter fraud during [her] tenure as Secretary of State or Assistant Secretary of State that specifically related to the impersonation of a registered voter at voting polls."

Provisional Ballots

Congress has established recourse for local and state election officials for those instances when the authentication of a voter is in doubt--the Provisional Ballot. However, the rules for the use of this ballot and the inclusion of these ballots in the final results of election need clarification. The goal of preventing voters from participating in public elections when they should not, but allowing a process that includes legal voters in engaging the process is a good approach.

CCTV Surveillance

Anonymity exists even when a person is in a public place or engaged in public acts. Anonymity in public spaces means that an individual or group of individuals can still anticipate, and benefit from the freedom of not being identified or falling under scrutiny. Anonymity may seem counterintuitive—how could someone expect privacy yet be in a public place, such as walking along a sidewalk, sitting in a park, joining a demonstration, or attending an entertainment event? People in public places are aware that they can be seen, and they in turn can see others, but the key to understanding anonymity is the inability of human beings to recall in great detail their own past.[9]

How does anonymity exist? It exists because people are not engineered to remember, but are designed to forget. Research done to assist law enforcement in better understanding the contributions of eyewitnesses in criminal investigations produced by Mark Kebbell's and Gramham Wagstaff's titled *Face Value? Evaluating the Accuracy of Eyewitness Information*, states the following:[10]

> To illustrate the nature of memory, think back to your last journey to work. You will find it hard to recall details of every person or vehicle that you saw during your journey. This is because memory is not like a video camera system. A video camera captures all of the events that are viewed in the direction in which it is pointed, records them and can replay them; our memories cannot do this. Moreover, we do not passively take information and replay it; rather memory is

[9] Donald A. Norman, The Psychology of Everyday Things, Sneak Preview of Forthcoming Books, Los Angeles Times Magazine, P. 4A, March 6, 1988

[10] Mark R. Kebbell, Graham F. Wagstaff, Police Research Series Paper 102, Face Value? Evaluating the Accuracy of Eyewitness Information, Research Development Statistics, March 1999, available at http://www.sosig.ac.uk/roads/cgi-bin/tempbyhand.pl?query=922267767-17783&database=sosigv3

> an active, creative process that can be inaccurate for a variety of reasons. For material to be remembered it must go through three main stages. It must be encoded in to memory, stored there and finally retrieved from memory. Problems can occur at each of these stages (for a more detailed introduction to the psychology of memory see Cohen, 1990).[11]

Significant events can become part of long-term memory,[12] but short-term memory[13] is a processing plant that functions with little regard for order and accuracy of events, places, people or things.[14] In our modern digital communication age, we are awash in information; we have the potential to take in more data with the assistance of technology than any generation of people to proceed us. Our minds exist in a hurricane of information, which reinforces the anonymity of privacy in public spaces as a real part of societal expectations of protection from unwanted intrusion or attention.

Under the condition of anonymity, individuals in public spaces find privacy because they become part of the "situational landscape."[15] Unless the person is of sufficient notoriety, a celebrity or public figure they experience the privacy provided by anonymity.[16] Therefore, people can and do expect privacy while in very public places as long as they are conducting themselves in a way that is not seen as extraordinary. The definition of extraordinary varies based on custom, culture, and social norms. For example, it would probably take a significant event, such as what occurred on September 11, 2001, to imprint long-term memories on the mind of the typical New Yorker walking along an uptown sidewalk.

Police, for example, rarely want to rely solely on a single person's account of a crime--although it may make for dramatic courtroom theater.[17] Good crime investigative techniques rely on sound forensic evidence along with eyewitness accounts that are notated based on well-developed rules for questioning witnesses to an event or crime.[18]

Deployment of close-circuit television (CCTV) surveillance to prevent crime has questionable results, but this has not stopped the use of CCTV in other settings. A low-income housing development in Washington, DC presents a cautionary tale about the potential for abuse of the technology. In this situation the housing development owners deployed a CCTV surveillance system with real time monitoring from a remote site. The CCTV system used one-way voice access allowing staff to give orders to residents using the threat of eviction to ensure compliance. The situation allowed the anonymous exercise of discretionary authority on the part of staff with no recourse for residents of the low-income housing development.

---

[11] id.
[12] Harvard Medical School's Consumer Health Information, Types of Memory, available at http://www.intelihealth.com/IH/ihtIH/WSIH000/31393/31397/347125.html?d=dmtContent
[13] id
[14] Norman, supra n. 3.
[15] Solove, Rotenberg, Schwartz, supra n. 1.
[16] Kebbell and Wagstaff. supra n. 4. P. 9
[17] Solove, Rotenberg, Schwartz, supra n. 1
[18] id

Since September 11th attacks, US policymakers and security and intelligence services are increasingly advocating the automation of policing functions within society. They are turning toward video surveillance technology as the answer to terrorist threats and the public's demand for security. However, important questions need to be addressed before uncritically accepting the routine surveillance of public spaces, including whether video surveillance is an effective tool for post-crime investigation; a remedy for crime prevention and deterrence. Finally, a proper remedy for protection and defense of privacy and civil liberties in a digital surveillance environment must be devised.

In his testimony provided by EPIC's Executive Director Marc Rotenberg to the District of Columbia City Council raised three critical points about the broad public adoption of CCTV technology for surveillance purposes.[19]

First, the use of surveillance cameras raises far-reaching Constitutional questions that implicate the rights of citizens, and most significantly people who engage in peaceful public activities while in public spaces.[20]

Second, the benefits of video surveillance systems as a means to reduce crime and deter terrorism have been significantly overstated. Studies from London, England and Sydney, Australia make clear that the value of cameras is overstated and that money is better spent on officers than cameras. Moreover, the particular effort to promote the use of face recognition technology may be one of the biggest corporate boondoggles in recent history, costing taxpayers hundreds of millions of dollars with little benefit in return.[21]

Third, these systems are being interposed in public settings without the benefit of uniform guidelines that equally balance privacy and security. Some efforts at rulemaking in this area disregard the important privacy protection of anonymity. These rules also may take too restrictive a view of the expectation of privacy and First Amendment protected activities. Many of these proposed systems of public surveillance lack adequate means of independent oversight. The reporting requirements are vague, the policy on usage and retention may be insufficient, the definitions may be too narrow, and the auditing limited.[22]

Constitutional Implications of CCTV Surveillance for Law Enforcement Purposes

Some have stated that the legal question concerning video cameras in public spaces is simply whether one has a reasonable expectation of privacy in a public place. I believe that this perspective fundamentally misstates the Constitutional interests at stake in this debate.

---

[19] Marc Rotenberg, Testimony before the District of Columbia City Council, Committee on the Judiciary, Public Works, and the Environment, June 13, 2002. http://www.epic.org/privacy/surveillance/testimony_061302.html

[20] id

[21] id

[22] id

There is no dispute that the police have a critical role in protecting public safety. This is particularly true when a large number of people are gathered for political protest. Protesters, as well as residents and tourists, have an interest in ensuring that public assemblies are peaceful and do not endanger persons or property. However, there are risks of misuse or abuse of the system. Studies have shown that there is a serious risk of race discrimination: black males are disproportionately scrutinized when such cameras systems are used.[23]

I want to be clear that this concern about surveillance of constitutionally protected activity is more than theoretical. Shortly after EPIC learned of the plan to install video cameras in public places, we submitted a series of Freedom of Information Act requests to several agencies in the District. A response that we received from the United States Park Police is particularly revealing.

The documents that we obtained contain individual logs of the aerial surveillance conducted by the District of Columbia Metropolitan Police (MPD). I would like to call your attention to the activities of surveillance by the MPD.

- On October 16, 2000, the United States Park Police of the National Mall of the Million Family March undertook aerial surveillance.
- On January 22, 2002, the Park Police of the pro-life demonstration to the Supreme Court conducted aerial surveillance.
- On that same day, the FBI conducted aerial surveillance of the pro-life demonstration.
- On January 20, 2001 the Metropolitan Police Department conducted aerial surveillance of the demonstration activity at 7th and Pennsylvania Avenue during the Presidential inaugural parade.
- On January 18, 2001 aerial surveillance was conducted by the MPD of "demonstration activity." The Park Police "provided downlink photos of coffins/demonstrators."

Although all of these incidents implicate Constitutional matters, the last example may be the most significant because it makes clear that video surveillance is specifically undertaken of individuals engaged in political protest. This clearly implicates constitutionally protected freedoms of freedom of assembly, and freedom of speech.

It is also clear that aerial surveillance is increasing. Many of the records we obtained concerned the protests in 2002.

- On April 20, 2002, the Metropolitan Police Department conducted a "downlink video of demonstration activity" at Connecticut and Florida.

[23] NACRO CCTV Study at 4; Clive Norris and Gary Armstrong, The unforgiving Eye: CCTV surveillance in public space, Centre for Criminology and Criminal Justice at Hull University (1997).

- On April 22, 2002, the United States Park Police conducted surveillance of demonstrators.
- On April 22, 2002 the Metropolitan Police Department provided a "downlink of MPD Command Center w/demonstrators."

The 2004 New York City case is an example of federal and state law enforcement officials increasingly using camera surveillance systems to track protesters, which can have a chilling effect on freedoms of speech, assembly, and association.[24]

There will be serious Constitutional questions that arise when images obtained by the police are used in trial against a criminal defendant. Particularly with a technology where it is so easy to manipulate digital images and so difficult to ensure the integrity of a digital file, very clear rules for retention, chain of custody, and use must be established.

The Benefits of CCTV are Overstated

What is the formula for calculating the value of CCTV in protecting public safety? There is little doubt that technologies and certain common sense practices reduce crime. Better lighting in public areas, community policing programs, and locking car doors are examples of techniques that have been proven to reduce the risk of car theft, robbery, and street crimes. In the realm of criminal investigation, fingerprint identification, proper processing of forensic evidence, and skilled investigators continue to play the deciding factors in post crime investigations.

It is worth noting Christopher Slobogin's assessments of why CCTV technology might not be that effective as a crime deterrent or crime interdiction tool in his paper *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*.[25]

> There are many reasons why cameras might not be effective at reducing crime in the areas on which they are trained. To understand why, consider the three ways cameras can, in theory, be useful: (1) they might help spot incipient crime that can be prevented, or at least solved, through immediate action; (2) they might create a record of crime that can be used in identifying and convicting perpetrators at some later point in time; and (3) they might deter crime. In each of these three areas, obstacles to smooth functioning exist.[26]

The inability of these surveillance systems to function as people do with the capacity to constantly evaluate their environment function as the main hurdles to CCTV being a sole means of crime detection and intervention. The remote real-time monitoring of CCTV information may not remedy the situation when one takes into account that cameras can be disabled or destroyed, and might not have the range to directly observe the scene of a

[24] See EPIC's Protestor Privacy and Free Expression Rights P. at http://www.epic.org/privacy/protest/
[25] Christopher Slobogin, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, Mississippi Law Journal, Vol. 77, Fall 2002, available at http://www.olemiss.edu/depts/law_school/ruleoflaw/pdf/LJournal02Slobog.pdf
[26] id.

crime. Further, those who are positioned to review the information provided by CCTV might find it difficult to determine if a crime is being committed.[27] The correct identification of a crime in progress may not result in an officer being dispatched to the area; especially if the calculation was made that fewer officers would be needed with the deployment of CCTV technology. The real possibility of false positives and false negatives should be considered. A false positive is when a crime is believed to be in progress and officers are dispatched only to find that no crime has occurred. A false negative is the assessment that no crime is occurring when in fact one has occurred. The failure of remote observers to determine the situation can lead to a waste of resources and personnel.

An additional complication for the deployment of CCTV for policing functions is that law enforcement officers may avoid responding to crime situations in areas where they are deployed out of concern that the images recorded might open them to investigation.[28] The investigations and trials that followed the disclosure of videos involving police actions, such as the one of Rodney King and Robert Davis make real their concerns.[29]

For CCTV to work as a possible crime deterrent the public must know that the technology is being used in the location. Notice may also result in criminals migrating to other areas to engage in unlawful acts.

However the role of CCTV in post-crime investigation following the London bombings in 2005 cannot be disputed. The post crime investigation by police identified the suspects, through old-fashioned police work, and from that information, CCTV surveillance tapes were reviewed. The role of CCTV to prevent crime is questionable, and should not be cited as a justification for investing in the technology.[30]

There is a Need for Uniform Standards

A GAO Report found that the justification for implementing the new surveillance system was "among other things, to facilitate crowd management during large demonstrations; officials also indicated that the system could also be used to combat terrorism."[31] Other justifications for the adoption and use of CCTV technology are crime prevention and post crime investigation.

The public concern over the use of video recording technology's use to unknowingly record individuals was so great that the 108th Congress addressed the issue in the Video

---

[27] id
[28] id
[29] Associated Press, New Orleans Man Beaten By Police Revisits Scene of Struggle, October 11, 2005, available at http://www.officer.com/article/article.jsp?id=26385&siteSection=5,
[30] Fran Spielman and Frank Main, City plans camera surveillance web, Chicago Sun-Times, Sept. 10, 2004; see generally Privacy International, Overview: CCTV and Beyond, available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65433.
[31] Government Accounting Office, Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, DC, GAO-03-748, June 2003

Voyeurism Prevention Act of 2004, which became public law 108-495.[32] The law amended the federal criminal code to prohibit knowingly videotaping, photographing, filming, recording by any means, or broadcasting an image of a private area of an individual, without that individual's consent, under circumstances in which that individual has a reasonable expectation of privacy. Congress defined "a reasonable expectation of privacy" to mean both private settings and public situations.[33] The law created an exemption for lawful law enforcement, correctional, or intelligence activity, but it did not require that they create guidelines for CCTV surveillance. These guidelines, which should include audits of the information gathered, and routine-reporting requirements would go a long way in allaying concerns about misuse or abuse of recorded images obtained in the course of an investigation.

In one incident, four security officers in Merseyside, Great Britain, were charged with voyeurism they were accused of using street surveillance cameras to peer into a private home to spy on a woman.[34] A D.C. Council investigation found wrongdoing by police during demonstrations in 2002 and that D.C. Police Chief Charles H. Ramsey and other police officials conspired to cover up evidence of such wrongdoing.[35] The Council's Judiciary Committee submitted a March 2004 report detailing numerous transgressions by D.C. police:

- Metropolitan Police Department use of undercover officers to infiltrate political organizations in the absence of criminal activity and in the absence of policy guidance meant to protect the constitutional rights of those individuals being monitored.
- A pattern and practice of misrepresentation and evasion on the part of leaders of the Metropolitan Police Department with regard to actions by the Department.
- Repeated instances of what appear to be preemptive actions taken against demonstrators including preemptive arrests.
- Failure of the Metropolitan Police Department to effectively police its own members for misconduct associated with demonstrations.
- Failure of the Metropolitan Police Department to acknowledge and to protect the rights of individuals to privacy, and to free speech and assembly.

---

[32] Library of Congress, Thomas, see: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.01301:

[33] Senate Bill 1301, Enrolled and Passed by Both the House and the Senate, http://thomas.loc.gov/cgi-bin/query/D?c108:17:./temp/~c108hpa03g::, "`(5) the term `under circumstances in which that individual has a reasonable expectation of privacy' means--

`(A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or

`(B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place."

[34] Emma Gunby, Council Workers Bailed In 'Peeping Tom' Case, Press Association, Aug. 23, 2005.

[35] District of Columbia Council, Judiciary Committee, Report on Investigation of the Metropolitan Police Department's Policy and Practice in Handling Demonstrations in the District of Columbia at 1 (Mar. 24, 2004), available at http://www.dccouncil.washington.dc.us/patterson/kathypatterson.org/p.s/prinfo/MPDReportFinal5304.doc and http://www.epic.org/privacy/surveillance/spotlight/1205/mpdrep5304.pdf.

- Repeated instances of violating the Department's own guidelines for handling demonstrations contained in the Standard Operating Procedures for Mass Demonstrations, Response to Civil Disturbances, and Prisoner Processing including guidelines on use of force in defensive situations, de-escalation in crowd control, and predicates required for mass arrests.

It is also important for policy and decision makers to be mindful of the march of technology. New CCTV systems are capable of recording images that allow easy archiving, recovery, and sharing of information. Enhanced features include night vision, computer assisted operations, thermal imaging, and motion detection facilities that help improve the operator's attention to the images being relayed. The clarity of the images recorded is of high resolution and many systems can allow the reading of newspaper print at a hundred meters.[36] The advances that will be made in CCTV technology with the perfecting of other applications, such as facial recognition and the scanning of intimate areas between the skin and clothing are also reasons to develop guidance to regulate their use.[37]

The federal government is spending an increasing amount of money on surveillance technology and programs at the expense of other projects.[38] In fiscal year 2006, the federal government planned to add facial recognition checks to all visa applications, which already include fingerprint biometrics.[39] Although the technology has not proven itself useful in deployment in airports and city streets, the push continues to forge a path to everyday urban and suburban life.

Tampa is one of the U.S. cities that has used facial recognition technology in concert with camera surveillance systems to surreptitiously scan the public.[40] In August 2003, Tampa stopped using the system, supplied by Identix, because of its failures. "It's just proven not to have any benefit to us," said a police department spokesman.[41] The Tampa system is also an example of the privacy risks created by such facial recognition systems. What began as a system to catch criminals became a system to find people who might have information sought by police. That is a poor reason to invade the privacy of the general public. With such systems, a person can be scanned without her knowledge or consent. A person's "suspect activity" may be no more than walking around a popular nightlife area.[42]

Information Fusion Centers

[36] Privacy and Human Rights, supra n. 12
[37] id
[38] EPIC, Spotlight on Surveillance, Facial Recognition Systems Have an Ugly Effect on Personal Privacy, available at http://www.epic.org/privacy/surveillance/spotlight/1105/default.html
[39] id
[40] id
[41] id
[42] id

Fusion centers are a means of brining together information from distributed sources for the purpose of collection, retention, analysis, and dissemination. The term fusion center was first coined by the Department of Defense (DOD) and refers to the fusing of information for analysis purposes. On November 9, 2002, the New York Times disclosed a massive DOD fusion center project managed by the Defense Advanced Research Project Agency (DARPA) known as Total Information Awareness (TIA). DARPA was developing a tracking system intended to detect terrorists through analyzing troves of information.

The project called for the development of "revolutionary technology for ultra-large all-source information repositories," which would contain information from multiple sources to create a "virtual, centralized, grand database." This database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information. Also fed into the database would be intelligence data.

A further crucial component was the development of biometric technology to enable the identification and tracking of individuals. DARPA had already funded its "Human ID at a Distance" program, which aimed to positively identify people from a distance through technologies such as face recognition or gait recognition. A nationwide identification system would have been of great assistance to such a project by providing an easy means to track individuals across multiple information sources.

In September 2003, Congress eliminated funding for the controversial project and closed the Pentagon's Information Awareness Office, which had developed TIA. It was not believed to signal the end of other government data-mining initiatives that are similar to TIA. Projects such as the Novel Intelligence from Massive Data within the Intelligence Community Advanced Research and Development Activity (ARDA) moved forward. It was also known that the FBI and the Transportation Security Administration were also working on data-mining projects that fused commercial databases, public databases, and intelligence data and had meetings with TIA developers.

Another fusion center initiative was the Multi-state Anti-Terrorism Information Exchange (MATRIX) program. MATRIX was a prototype database system run by the State of Florida and Seisint, a private company. Built by a consortium of state law enforcement agencies, MATRIX proposed to combine public records and private record data from multiple databases with data analysis tools. MATRIX was established with the assistance of the Institute for Intergovernmental Research’s Global Justice Information Sharing Initiative. The program collapsed when it was disclosed to the public, and states were pressured by residents to withdraw from the program.

In March 2004 the MATRIX project was on its last gasp, when the states of New York and Wisconsin withdraw their participation in the project. In April 2004, it was reported to the 9-11 Commission that the CIA and the FBI still could not search each other’s terrorist databases. The barriers were a lack of interoperability among databases used by the two agencies.

Latest Government Information Fusion Center Initiative

In December 2004, the push for a national Fusion Center initiative received a boost when the Department of Justice sponsored Global Infrastructure/Standards Working Group published A Framework for Justice Information Sharing: Service Oriented Architecture (SOA). States using local, state, and federal funds created information fusion centers. In August 2005, the Global Justice Information Sharing Initiative of the Department of Justice published the Fusion Center Guidelines

> "The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorist information and intelligence and other information (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal/terrorist activity. This criminal information and intelligence should be both strategic (i.e., designed to provide general guidance of patterns and trends) and tactical (i.e., focused on a specific criminal event)."

The Department of Homeland Security set out an objective to create by 2008 a network of fusions centers as unique law enforcement and threat information resource that could facilitate "across jurisdictions and functions" supported by "multidisciplinary teams" dispersed throughout a national network of information hives.

Turning Fusion Centers into Hardware and Software

> *The purpose of this* [SOA] *report is to describe the recommendation of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) for the operational requirements of justice agencies and the requirements for a national community.*

The guidelines stated the software of the choice as being Extensible Markup Language (XML), which facilitates efficient and near real time sharing of information resident on geographically dispersed databases. The initiative promotes the data sharing among multiple-geographically dispersed users though the application of a common platform that can be used on existing hardware. The goal is to achieve a low cost method of removing barriers to data sharing among beat officers, court records, state records, jails and prisons, that is efficient and effective.

The Fusion Center Guidelines endorses the use of the new database sharing capability created by the open source XML standards. This open standards programming language provides users with a data sharing capability that would not require the replacement or redesign of existing system. This programming language allows the identification of fields of information through the use of a translation feature that accomplishes its task between the system being asked for information, and the end requester. In this process the

source of the data and the recipient do not need to change their computer networks to participate in the information exchange network.

The interesting aspects of the proposal are the promotion of a national collection and analysis of information. The "National Information Exchange Model" proposed for the fusion centers is designed to create the building blocks for "national-level interoperable information sharing and data exchange that will integrate the public safety and private sector entities to the already established law enforcement exchange."[43]

Exchanging information is only the beginning of the process; the goal is "institutionalizing the relationships between the fusion center and the public safety and private sector partners." The Global recommendations make the case for distributed and centralized data management systems. According to advice on the topic a distributed systems will allow the data controller to be in charge of access, while the centralized process would allow the fusion center to manage the data. A white paper examining strategies for enhancing the sharing of information pointed out that successful distributed and centralized information-sharing systems are in operation today.[44] The goal is to get local, state, federal law enforcement, federal government agencies, and private sector data warehouses into the same project.

In September 14, 2006 the Department of Homeland Security reported that 38 state and local Information Fusion Centers supported by $380 million in federal dollars were operational. The investment in time, energy, and resources are focused on one objective maximizing access to the greatest amount of information as possible. Part of the stated motivation for the development of this information resource began with post-September 11, 2001 acknowledgement that a lack of information sharing may have contributed to the failures of federal intelligence and law enforcement to prevent the tragedy.

Fusion Center Data Sources

Appendix C of the Guidelines outlines a detailed list of entities that should be included in the local and state fusion center matrix.

Agriculture, Food, Water, and the Environment	Education	Hospitality and Lodging
Banking and Finance	Emergency Services (Non-Law Enforcement)	Information and Telecommunications
Chemical Industry and Hazardous Materials	Energy	Military Facilities and Defense
Criminal Justice	Government	Industrial Base
	Health and Public Health Services	Postal and Shipping
		Private Security

[43] National Information Exchange Model, Learn More About NIEM, available at http://www.niem.gov/whatIsNiem.php

[44] Alan Harbitter, A Critical Look at Centralized and Distributed Strategies for Large-Scale Justice Information Sharing Applications, available at http://www.iir.com/global/FusionCenter/critical_look_at_Centralized_and_Distributed_Strategies.pdf

Retail Real Estate	Social Services Transportation	Public Works

(Source Fusion Center Guidelines: Appendix C)

The proposal directs that information categories could fall into one of two types: strategic and tactical information. Strategic information may provide data on individuals not under criminal investigation or operations that an entity manages and tactical information may provide data be in support of ongoing criminal investigations. It would be very difficult to imagine someone living within the United States who would not have one or multiple points of information confluence in the proposed system.

What the guidance said about the "Fusion Center Functions"

> The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorist information and intelligence and other information (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal/terrorist activity. This criminal information and intelligence should be both strategic (i.e., designed to provide general guidance of patterns and trends) and tactical (i.e., focused on a specific criminal event).[45]

The Fusion Center Guidelines repeatedly stress the importance of "collaboration and corporation," to the success of the center. The focus of the work of fusion centers will not be limited to terrorism or terrorist activity, but will extend investigation of welfare fraud, illicit drugs, traffic accidents, and aviation accident analysis.

The range of information to be collected by service providers who participate in the fusion center effort could include: all sources of financial records kept by banking institutions; all contacts with the criminal justice system by criminals and non-criminals, all forms of education (day cares, preschools, primary and secondary schools, colleges and universities, and technical schools); government issues licenses and permits, access to medical records held by hospitals, public health, and primary care physicians, hospitality and lodging, information and telecommunication service providers, military facilities and defense industrial base; postal and shipping services, private security (alarm companies, armored car companies, investigative firms, corporate security offices, private security companies); public works; social services; and transportation.[46]

Some of the categories and data targets of the fusion center program follow:

Banking and	**Education/Health**	**Police, Jails,**	**Government**	**Hospitality and**

[45] Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines, pg. 13August 2005, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

[46] Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines, August 2005, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Finance		Prisons	Licensing	Lodging
Banks Investment Co. Credit card Co. Credit report Co. Securities firms Financial services	Day care centers Preschools Colleges/universities Technical schools Mental Health Primary Care Physicians EMS Hospitals Veterinary	Gang Info. Names of Associates Relatives Visitors Biographical Info.	Game & Fish DMV Lics. Vehicle Reg. Boat Reg.	Gaming Industry Sports Authority Sporting facilities Amusement parks Cruise lines Hotels, motels, and resorts Convention Centers

Along with a host of local, state and federal law enforcement agencies, private companies also participated in the Public Safety Fusion Group included Walt Disney World Company, Fidelity Investments, Microsoft Corporation, and Archer Daniels Midland. The goal is to within the fusion center environment integrate "nontraditional customers of information and intelligence."[47] As well as, fusing information based on an identified threat, criminal predicate, or public safety by the seamless collection, collating, blending, analyzing, disseminating, and use of information intelligence. The intelligence and analysis of information is proposed to be base on the needs of users, with the list of users including all levels and types of law enforcement, intelligence community, DOD, Defense Industry, private sector entities it appears the official uses could be limitless.

Expanding the Customer Base for Domestic Fusion Centers

The definition of "national intelligence" was changed by the enactment of the Intelligence Reform and Prevention Act of 2004, bill to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government.[48]

> "The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States…"

The new law also defines the "information sharing environment," (ISE) as

> The President shall...ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the

[47] Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines, August 2005, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

[48] Senate Bill 2845, the Intelligence Reform and Terrorism Prevention Act of 2004, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02845:

> ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that…connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector…ensures direct and continuous online electronic access to information…facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations…builds upon existing systems capabilities currently in use across the Government;

The focus of fusion centers is on information collection as a means of determining crime trends with and eye toward predicting crime before it occurs. The "four major desired outcomes" for fusion centers are: the reduction of the incident of crime; suppression of criminal activity; the regulation of noncriminal conduct; the provision of services. [49]

In September 14, 2006 the Department of Homeland Security reported that 38 state and local Information Fusion Centers supported by $380 million in federal dollars were operational.[50] The investment in time, energy, and resources are focused on one objective maximizing access to the greatest amount of information as possible. Part of the motivation for the development of this information resource began with post-September 11, 2001 acknowledgement that a lack of information sharing may have contributed to the failures of federal intelligence and law enforcement mechanism.

Privacy and Civil Liberties and Fusion Centers

There are questions about the focus on privacy and civil liberties considerations within the development of the Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines. The guidelines were published in the summer of 2005, but the Global Privacy and Information Quality Working Group issued its final report a Privacy Policy Development Guide and Implementation Templates in October 2006. While the report lauded the importance of privacy protections from conception through implementation of a information sharing initiative it said this about building of a project team, "The project team should have access to subject-matter experts in areas of privacy law and technical systems design and operations, as well as skilled writers, but these individuals do not necessarily have to be team members."[51]

The Privacy Act of 1974, Public Law 93-579, was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. [52]It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records

---

[49] Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines, August 2005, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

[50] Department of Homeland Security, Fusion Center Guidelines, available at

[51] Advisory Committee on Automated Personal Data Systems, Report, Records, Computers and the Rights of Citizens, available at http://www.epic.org/privacy/hew1973report/

[52] EPIC, The Privacy Act of 1974, available at http://www.epic.org/privacy/1974act/

kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it lets individuals sue the government for violating its provisions.

There are, however, several exceptions to the Privacy Act. For one thing, government agencies that are engaged in law enforcement can excuse themselves from the Act's rules. Agencies have also circumvented information sharing rules by exploiting a "routine use" exemption. It is unclear how the merging of law enforcement purposes with non-law enforcement purposes would play out, but what is clear is that legal challenges would create new areas for local, state, and federal courts to review the fusion center process.

Privacy and Civil Liberty advocates are well aware of the provisions of the Federal Privacy Act intended to protect against government abuses that can be associated with computer databases. The law is intended to avoid the types of problems that can be created by digital communication technology under the control of the government. Congress found that, ”[t]he privacy of an individual is directly affected by the collection, maintenance, use and dissemination of personal information by Federal agencies”[53] The law was also informed by the determination that the “opportunities for an individual to secure employment, insurance, and credit, and his [or her] right to due process, and other legal protections are endangered by the misuse of certain information systems.”[54]

The foundations of the Privacy Act are the elements of the Code of Fair Information Practices that are codified by that law. The Code of Fair Information Practices is cited three times in the Privacy Policy Development Guide and Implementation Templates drafted by the Global Privacy and Information Quality Working Group of the DOJ’s Global Justice Sharing Initiative. None of the citation enumerated what the Code of Fair Information Practices are—nor its history.

The Code of Fair Information Practices and a Brief History

The Code for Fair Information Practices is the central contribution of the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems.[55] The Advisory Committee was established in 1972, and the report released in July. The citation for the report is as follows:

U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).The Code of Fair Information Practices is based on five principles:

[53] EPIC, pg. 355, Litigation Under the Federal Open Government Laws 2004
[54] EPIC, pg. 355, Litigation Under the Federal Open Government Laws 2004
[55] US Department of Health Education and Welfare, Fair Information Principles, 1973 available at http://www.epic.org/privacy/consumer/code_fair_info.html

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

FIPs matured over the decades and was adopted by many nations in the West and found legal breath in the OECD

Some things to Think About

"No one is administrative pure"[56]
Michael German

Michael German is a former FBI agent who was writing about the conditions within the agency as they related to staff being able to steer clear of breaking administrative rules. If employees of the agency are not kept informed of new rules as they are promulgated then the likelihood that someone—somewhere in the agency is in violation has a high probability. He was writing specifically about the issue of FBI whistleblowers, those who would seek to bring fraud, waste or abuse to the attention of elected officials, or the public.

In the context of fusion centers, no one knows the rules that will bring someone under scrutiny, and what the consequences of that scrutiny might be.

- December 2006, an article on the Salt Lake City Police Department's fusion center efforts described it as "a way of tracking information that comes in from community groups like community councils and neighborhood watch, as well as the mayor's office.[57]

[56] Michael German, FBI Insiders Guide, available at http://www.globalsecurity.org/security/library/report/2005/guide-iii.htm
[57] Doug Smeath, Deseret Morning News, Police idle Community Action Team, December 19, 2006

- January 2007, an article cites the Sacramento-based intelligence fusion center for indictments filed against California Healthcare Collective for illegal marijuana farming.[58]
- March of 2007, the Governor of California supported the creation of a "Baca countywide Gang Assessment Center," he referred to as a fusion center.[59]

The Washington Post reported on June 14, 2007 that the FBI conducted a self-audit of 10 percent of its records on National Security Letter use and found over 1,000 violations.[60] The majority of the violations were associated with the obtaining of telephone records from telecommunication service providers. The FBI acted in the wake of criticism that resulted from an earlier Department of Justice Inspector General report, which determined that the FBI abused their National Security Letter authority established by the Patriot Act.[61]

There are no statutory definitions for terrorist or terrorist organization.[62]

> "Clarification—There must be a clear statutory definition of the words "terrorism," and "terrorist," as well as the phrase "terrorist organization." Without clear definitions, these designations could be misused, such as in the past when the word "subversive" was used to justify actions taken against some civil rights activists, civil liberty groups and others who were engaged in lawful pursuits."

The Fusion Center development process and the Guidelines did not address the communication problems that the 9-11 Commission identified as contributing factors to the national intelligence and federal law enforcement failures of September 11, 2001. Further, the Guidelines do not limit its focus to terrorist or terrorist activity, but extend to an "enhanced coordination effort strengthened partnerships, and improve, crime-fighting" capability "for all types of crime…"[63]

In 2007, the House Committee on Homeland Security sought to address potential problems associated with fusion centers by mandating a training program on privacy, civil liberties, and civil rights protection for fusion center employees participating in the

---

[58] Michael Doyle, Fresno Bee, Valley drug-fighters honored, January 18, 2007
[59] Kaelyn Forde Eckenrode, Whittier Daily News, Governor pledges help in battle against gangs, March 5, 2007
[60] John Solomon, FBI Found it Frequently Overstepped in the Collection of Data, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453.html June 14, 2007
[61] EPIC, Patriot Act Web Page, available at http://www.epic.org/privacy/terrorism/usapatriot/
[62] In Defense of Freedom, Letter to the 9-11 Commission on its final report, October 2004, available at
[63] Global Justice Information Sharing Initiative and Department of Homeland Security, Fusion Center Guidelines, August 2005, available at http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Program.[64] The White House opposed these along with other provisions of the bill in a statement on administration policy issued May 9, 2007.[65]

Conclusion:

Increased demands for proof of citizenship or legal status, close-circuit television surveillance, and the spread of information fusion centers are a disturbing trend within the United States. There are individuals living within societies who provide early indications of potential harms that can come from universal changes in surveillance and identification policies—-they are the "canaries in the coalmine." This panel discussion presents an excellent forum for examining social justice issues on how the deployment of surveillance technology and new identification systems are affecting the civil liberties of religious, ethnic, tribal, and unique populations.

There are too many unanswered questions regarding the creation, purpose, and consequences of surveillance, national identification systems, and federally support data retention programs connecting public and private actors. Advocates working in the public's interests, academic researchers, legal scholars, attorneys, the courts, and journalists all can play a vital role in checking the application of these systems of surveillance to ensure that our freedoms and liberties are retained.

Lillie Coney
Associate Director
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
202-483-1140 x 111

[64] Library of Congress, Thomas, House Resolution 1684, Department of Homeland Security Authorization Act of 2007, available at http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR01684:@@@D&summ2=m&
[65] Executive Office of the President, Statement of Administration Policy H.R. 1684 the Department of Homeland Security Authorization Act, available at http://www.whitehouse.gov/omb/legislative/sap/110-1/hr1684sap-h.pdf