



**ELECTRONIC PRIVACY INFORMATION CENTER**

---

**Statement  
Department of Homeland Security  
Data Privacy and Integrity Advisory Committee  
September 19, 2007  
Lillie Coney**

I would like to thank the Data Privacy and Integrity Advisory Committee for inviting the Electronic Privacy Information Center (EPIC) to offer comments at today's meeting on fusion centers. EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC takes public positions only on matters of concern to consumers and as an advocate for civil liberty and privacy protection.

Our panel presentation today is about the emergence of an inter-networked communication infrastructure that could facilitate the creation of a modern surveillance society. The name given to the criminal justice/national security components of this endeavor are "information fusion centers." Fusion centers are an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals. 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, locate criminals and predict crime before it happens.

**Information Fusion Centers**

Fusion centers are being proposed as a means of bringing 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.

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.

#### *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)." 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 that could facilitate data sharing “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 [A Framework for Justice Information Sharing: Service Oriented Architecture] 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 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 systems. 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 fusion centers are designed to create the building blocks for “national-level interoperable information sharing and data exchange. It will integrate public safety and private sector data sources to the already established technology architecture for law enforcement information exchange.”<sup>1</sup>

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

---

<sup>1</sup> National Information Exchange Model, Learn More About NIEM, available at <http://www.niem.gov/whatIsNiem.php>

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.<sup>2</sup> The goal is to get local, state, federal law enforcement, federal government agencies, and private sector data warehouses into the fusion center project.

On 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—removing barriers between law enforcement, national security, and private sector data warehouses. 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 in preventing 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 Banking and Finance Chemical Industry & Hazardous Materials Criminal Justice Retail Real Estate	Education Emergency Services (Non-Law Enforcement) Energy Government Health and Public Health Social Services Transportation	Hospitality and Lodging Information and Telecommunications Military Facilities and Defense Industrial Base Postal and Shipping Private Security 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 a fusion center participant manages, while tactical information may provide data 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.

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.

<sup>2</sup> 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](http://www.iir.com/global/FusionCenter/critical_look_at_Centralized_and_Distributed_Strategies.pdf)

The range of data sought by fusion centers include: all sources of financial records; all contacts with the criminal justice system by criminals and non-criminals, all tribal, local, state, federal, private, and university law enforcement records including US Postal Inspectors, all forms of education (day cares, preschools, primary and secondary schools, colleges and universities, and technical schools); government issued licenses and permits, medical records (public health, ambulance, hospitals, mental health, clinics, and primary care physician medical files), hospitality and lodging, gaming industry, telecommunication service providers, military and defense industrial base; US Post Offices, 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.<sup>3</sup>

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

<b>Banking and Finance</b>	<b>Education/Health</b>	<b>Police, Jails, Prisons</b>	<b>Government Licensing</b>	<b>Hospitality and Lodging</b>
Banks, Investment Co. Credit companies Securities firms Financial services	Day care centers Preschools Colleges/universities Technical schools Mental Health Primary care doctors EMS/Ambulance Hospitals	Gang Info. Names of Associates Relatives Visitors	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 including 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.”<sup>4</sup> The process would involve fusing of 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 will be based on the needs of fusion center participants. The list of fusion center participants including all levels of law enforcement, national intelligence community, defense, and private sector entities could make the applications of the data-mining project limitless.

<sup>3</sup> 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](http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)

<sup>4</sup> 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](http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)

### *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.<sup>5</sup>

“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

...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 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 an 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. □<sup>6</sup>

### *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 fusion centers, it said this about the building of a

---

<sup>5</sup> 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>:

<sup>6</sup> 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](http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)

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."<sup>7</sup>

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.<sup>8</sup> It safeguards privacy through creating four procedural and substantive rights in personal data. First, it requires government agencies to show an individual any records 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. 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.

A Law Enforcement Assistance and Partnership Strategy report published by the minority staff of the 109<sup>th</sup> House Committee on Homeland Security, which included this effort at melding the role of law enforcement and private sector roles, "Chief Ellen Hanson of the City of Lenexa, Kansas Police Department recounts:

Local efforts to inform the public are an effective way to stay on top of information regarding possible terrorist activity. Here in Lenexa we have incorporated this element into our Crime Resistant Community Policing Program. We conduct regular trainings with the maintenance and rental staffs of apartment complexes, motels, and storage facilities. We show them how to spot and identify things like printed terrorist materials and propaganda and unique weapons of mass destruction like suicide bomb vests and briefcases. We build up a level of trust and familiarity that encourages them to pass on any suspicious information to our officers. They have confidence that the follow-up will be handled responsibly and they also understand that they have an opportunity to play an important part in local efforts to prevent acts of terrorism"<sup>9</sup>

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

---

<sup>7</sup> Advisory Committee on Automated Personal Data Systems, Report, Records, Computers and the Rights of Citizens, available at <http://www.epic.org/privacy/hew1973report/>

<sup>8</sup> EPIC, The Privacy Act of 1974, available at <http://www.epic.org/privacy/1974act/>

<sup>9</sup> 109<sup>th</sup> Minority House Committee on Homeland Security, available at <http://www.epic.org/privacy/fusion/leap.pdf>

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"<sup>10</sup> 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."<sup>11</sup>

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 fusion center Privacy Policy Development Guide and Implementation Templates written 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.

There are reasons to be troubled by the development of fusion centers without clear policy and oversight mechanisms in place. 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.<sup>12</sup> 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.<sup>13</sup>

There are no statutory definitions for terrorist or terrorist organization.<sup>14</sup>

"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."

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

---

<sup>10</sup> EPIC, pg. 355, Litigation Under the Federal Open Government Laws 2004

<sup>11</sup> EPIC, pg. 355, Litigation Under the Federal Open Government Laws 2004

<sup>12</sup> 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

<sup>13</sup> EPIC, Patriot Act Web Page, available at <http://www.epic.org/privacy/terrorism/usapatriot/>

<sup>14</sup> In Defense of Freedom, Letter to the 9-11 Commission on its final report, October 2004, available at



Program.<sup>15</sup> The White House opposed these along with other provisions of the bill in a statement on administration policy issued May 9, 2007.<sup>16</sup>

#### Conclusion:

According to news reports there are 43 current and planned fusion centers that we are aware of at this time. Investigations conducted by the Congressional Research Service, ACLU, EPIC, and others raise more questions than are answered about the real world implications of the Department of Homeland Security's role in the development of intelligence fusion centers. EPIC concluded that Intelligence fusion center development and implementation is unfocused and undirected. The appropriate supervision, guidance and oversight necessary to assure privacy, civil liberty, and civil rights protection are imperative. Information Fusion centers present grave threats to privacy and civil liberties.

There are too many unanswered questions regarding the creation, purpose, and use of fusion centers. 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 systems of surveillance to ensure that our freedoms and liberties are retained.

#### Recommendations:

- The Department of Homeland Security should fully disclose the location, jurisdiction served, and amount of federal funding provided to each intelligence fusion center operating within the United States
- Funding for Intelligence Fusion Centers should be suspended until a full federal privacy impact analysis is conducted.
- An IG investigation of information fusion centers should be launched to review their compliance with existing federal laws intended to protect due process; privacy, civil liberty, and civil rights.
- Federal reporting requirements should direct that each information fusion center make public the names of all federal, state, local, and private partners.
- Annual reports from each fusion center on the number of arrests, prosecutions, and convictions by category of offense, which are directly related to each information fusion center's operations.
- All information collected, analyzed, or shared must comply at a minimum with the Federal Privacy Act, and where stronger state statutes exist the additional protection afforded must apply.

---

<sup>15</sup> 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&>

<sup>16</sup> 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>

Lillie Coney  
Associate Director  
Epic.org  
1718 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20009  
202-483-1140 x 111  
EPIC Fusion Center Page: <http://www.epic.org/privacy/fusion/>  
EPIC Spotlight on Fusion Centers:  
<http://www.epic.org/privacy/surveillance/spotlight/0607/default.html>