CHAPTER TEN

Fusion centers and the expansion of domestic intelligence

I. The Problem

The Bush Administration's 2007 National Information Sharing Strategy established state and local fusion centers as the federal government's primary mechanism for collecting and disseminating domestic intelligence. The federal government has fueled the growth of these state and local intelligence centers, and has organized them into a national network that feeds information gathered at the local level into the Director of National Intelligence's Information Sharing Environment (ISE), where it becomes accessible to all participating law enforcement agencies as well as the larger intelligence community. While efficiently sharing legally gathered criminal intelligence information among law enforcement agencies is a laudable goal, the federal government has encouraged these entities to broaden their collection efforts "beyond criminal intelligence, to include federal intelligence as well as public and private sector data." This expansion of intelligence collection at the state and local level raises profound privacy and civil liberties concerns for all Americans, particularly because these fusion centers often incorporate non-law enforcement participants, including private sector companies and the U.S. military, in their intelligence operations.

The police power to investigate combined with the secrecy necessary to protect legitimate law enforcement operations provide ample opportunity for error and abuse. In May 2008, the *San Diego Union-Tribune* revealed a scandal involving the Los Angeles County Terrorism Early Warning Center (LACTEW). A group of military reservists and law enforcement officers led by the co-founder of the LACTEW engaged in a years-long conspiracy to steal highly classified intelligence files and secret surveillance reports. (*see* Rick Rogers, *Records Detail Security Failure in Base File Theft*, San Diego Union-Tribune, May 22, 2008)

Yet the federal government is rapidly moving forward to create what amounts to a national domestic intelligence system, without proper guidelines to regulate these activities and without appropriate congressional and public oversight. In January 2008 the Director of National Intelligence published "functional standards" for "suspicious activity reporting," to encourage state and local police to collect and report non-criminal "suspicious" behavior to the fusion centers and the ISE. In August 2008 the Departments of Justice and Homeland Security endorsed a Los Angeles Police Department suspicious activity reporting program that defines innocuous First Amendment protected activities like taking photographs or videos, taking notes, and espousing extreme beliefs as "suspicious" behavior that could indicate terrorist related activity. In July 2008, the Department of Justice proposed a rule to amend the primary federal regulation governing criminal intelligence databases (28 CFR Part 23) to expand both what information can be collected by law enforcement agencies, and with whom it may be shared. (*see* 73 Fed. Reg. 44673). This regulation (28 CFR Part 23) was part of a series of law enforcement

reforms initiated in the 1970s to curb widespread abuses of police investigative authorities for political purposes, particularly by police intelligence units. Encouraging the collection of information not reasonably linked to criminal activity while weakening the regulations governing intelligence systems will likely lead to similar abuses.

II. Proposed Solutions

A. Executive Action

1. The President should review the National Information Sharing Strategy to ensure that all federal information sharing programs are carefully bounded to protect the privacy and civil liberties of U.S. persons.

2. Federal regulations should be revised to ensure that no personally identifiable information can be collected in a criminal intelligence system without reasonable suspicion that the person is or may be involved in criminal activity. Previous regulatory restrictions on the dissemination of information from criminal intelligence systems contained in 28 CFR Part 23 should be reinstated.

3. The President should issue a new National Information Sharing Strategy that incorporates the following principles:
4. All information collected, analyzed, or shared must comply at a minimum with the Federal Privacy Act, and where stronger state statutes exist the additional privacy protection afforded must apply.

5. Information Fusion Centers must have a single operational definition for their mission and clearly defined scope for their operation.

   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.

6. Prohibit no-bid contracting, and require publication of contracts and listing of all private sector data sources used in fusion center data collection and analysis.

7. Require an annual report from the Secretary of Homeland Security to the Congress, on each fusion center, which includes the number of arrests, prosecutions, and convictions by category of offense directly related to fusion center operations.

8. Intelligence Fusion Centers should be subject to federal Privacy Impact Assessment rules.

9. The Department of Justice or Department of Homeland Security Inspector General should launch an investigation of information fusion centers 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 partnering organizations, businesses and government entities engaged in the effort.

10. The U.S. military should be strictly prohibited from participating in domestic intelligence activities.

B. Legislative Changes

1. Congress should conduct oversight hearings to examine the threat fusion centers pose to the privacy and civil liberties of U.S. persons.

2. Congress should codify restrictions on the collection of domestic intelligence information, to restrict the collection of personally-identifiable information that is not linked to illegal activity, using previous versions of 28 CFR Part 23 as a guide.

C. Legislative Appropriations (Solutions w/ Funding Requests)

1. Congress should withdraw funding from information sharing programs that do not incorporate effective privacy and civil liberties protections.

III. Allies*

American Library Association
Lynne E. Bradley, Director
lbradley@alawash.org
202-682-8410
The ALA Policy Manual: The Rights of Library Users and the USA Patriot Act (52.4.5) *available at* http://www.ala.org/ala/aboutala/governance/policymanual/policymanual.31_3.pdf

Bill of Rights Defense Committee (BORDC)
Chip Pitts, President
chip.pitts@att.net

Center for Democracy & Technology
Gregory T. Nojeim
gnojeim@cdt.org
202-637-9800 (ext 113)
The Internet in Transition, *available at* http://www.cdt.org/election2008/

Common Cause
Sarah Dufendach, Vice President for Legislative Affairs
www.commoncause.org
202-736-5709

The Constitution Project
Sharon Bradford Franklin
sfranklin@constitutionproject.org
202-580-6920

Council on American-Islamic Relations (CAIR)
Corey Saylor, National Legislative Director
csaylor@cair.com
202-384-8857 (c)
202-488-8787 (w)

Defending Dissent Foundation
Sue Udry, Director
Sue.udry@defendingdissent.org
202-549-4225
www.defendingdissent.org

Electronic Frontier Foundation (EFF)
Kevin S. Bankston
bankston@eff.org
415-436-9333 (ext.126)

Essential Information
John Richard or Robert Weissman
202-387-8034

Government Accountability Project
Jesselyn Radack, Homeland Security Director
JesselynR@whistleblower.org
202-408-0034 (ext. 107)

Liberty Coalition
Michael D. Ostrolenk, Co-Founder/National Director
www.libertycoalition.net
mostrolenk@libertycoalition.net
301-717-0599

OMB Watch
Sean Moulton, Director, Federal Information Policy
202-234-8494

Fax: 202- 234-8584

OpenTheGovernment.org
Patrice McDermott
pmcdermott@openthegovernment.org
202-332-6736

Muslim Advocates
Shahid Buttar
shahid@muslimadvocates.org
415-692-1512

South Asian Americans Leading Together
Priya Murthy
priya@saalt.org
301-270-1855

Stanford Law School - Mills International Human Rights Clinic
Barbara J. Olshansky, Leah Kaplan Visiting Professor and Clinic Director
Kathleen Kelly, Clinical Teaching Fellow
bj.olshansky@gmail.com
650-736-2312

U.S. Bill of Rights Foundation
Dane vonBreichenruchardt, President
usbor@aol.com
202-546-7079

* These groups and individuals support the general principles expressed and the general policy thrust and judgments in the policy proposals described above. The allies listed do not necessarily endorse the specific language in every proposed solution, but they do agree that the proposals reflect the general principles that should govern policy in this area. Please contact the individuals and organizations listed in this section for more information.

IV. Counter-Arguments and Rebuttal

A. *Fusion centers are needed to implement the Information Sharing Environment (ISE) as part of an effective counterterrorism strategy. Sharing of information among federal, state, and local officials, and broad investigative powers are necessary to combat the new threats posed in our post-9/11 world.*
The 9/11 Commission recommended that federal, state, and municipal governments enhance terrorism-related information sharing. DHS argues that: 1) state-based fusion centers implement this recommendation; and 2) the fusion centers cannot be effective if they are subject to 51 different sets of privacy and transparency laws. Federal intelligence entities argue that limits on state privacy

and transparency laws are necessary to harmonize the rules governing information sharing, and increase the amount of data shared by federal intelligence sources.

The 9/11 Commission Report also said information sharing programs must be accompanied by safeguards for "the privacy of individuals about whom information is shared," which the DHS has failed to establish. In the absence of a stronger federal standard, state privacy and transparency laws uphold the privacy and oversight requirements set out by the 9/11 Commission. Moreover, these laws strengthen federalism and reflect the commitment of the White House's National Strategy for Information Sharing to "comply with all applicable privacy laws." Finally, there is no evidence that state laws hinder anti-terrorism information sharing. Indeed, recent studies show that the the primary challenge is an insufficient amount of anti-terrorism work. The vast majority of fusion centers have abandoned the exclusively anti-terrorism mission and now focus on an "all crimes" approach, which underscores the need to leave state privacy and open government laws intact.

V. Recommended Documents for Further Information

a. ACLU Fusion Center Report and Update: www.aclu.org/fusion

b. EPIC Fusion Center webpage: http://epic.org/privacy/fusion/

c. EPIC website Virginia Fusion Center: http://epic.org/privacy/virginia_fusion/

d. Proposed changes to 28 CFR Part 23: http://frwebgate1.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=114340201613+18+1+0&WAISaction=retrieve

e. Comments to proposed changes to 28 CFR Part 23: http://www.regulations.gov/fdmspublic/component/main?main=DocketDetail&d=OJP-2008-0002

f. ACLU: http://www.aclu.org/images/asset_upload_file347_36595.pdf

g. Brennan Center: http://brennan.3cdn.net/fcaf421405afb56c3e_63m6y9nwb.pdf

APPENDIX: "Fusion Centers and the Expansion of Domestic Intelligence"
Recent Legislative and Judicial Activity

I. Jurisdiction

A. **Executive Branch**

Office of the Director of National Intelligence
Department of Justice
Department of Homeland Security

B. **Legislative Branch**

Senate Homeland Security and Government Reform Committee;
House Homeland Security Committee;
House Government Reform Committee;
Senate and House Judiciary and Intelligence Committees

II. Background/Status of Actions in Legislative, Executive, and Judicial Branches

On July 31, 2008, The Department of Justice and Department of Homeland Security issued proposed rules amending 28 CFR Part 23, the primary federal regulation governing criminal intelligence databases. During the comment period, which ended September 2, 2008, both law enforcement and privacy rights organizations submitted comments expressing concerns about the proposed regulatory changes. The proposed rule amending 28 CFR Part 23 has not been finalized as yet.