

Intelligence Collection: Legal Issues



Dr. James F. Pastor, Ph.D., J.D.

LIABILITY LIMITATION

- This training session is intended to acquaint you with certain legal principles relating to Intelligence collection.
- You should consult the legal advisor for your agency or your employer before taking actions based on the materials provided and/or the opinions of law expressed in this unit of instruction.
- What is legally permissible varies on the particular circumstances of the situation. This training session is only designed to acquaint the attendee on broad legal/intelligence concepts and procedures.
- It is not intended to act as policy or procedure for you or your institution.

Learning Objective

Understand the legal, privacy and ethical issues relating to criminal intelligence.

Legal, Privacy and Ethical Issues Outline

1. Overview of legal and liability issues, intelligence audits/integrity and accountability.
2. 28 CFR Part 23
3. IC 5-2-4 (Indiana State Statute)
4. Standards for protecting information.
5. Overview of community trust and communication with citizens and media (briefing city and community leaders).

Remember the 60's?

- Much criticism still remains from the illegal spying by police & federal agents during the anti-war & civil rights era.
- Because of these abuses, many are “gun shy” about getting involved in intelligence collection.
- To address this concern, uniform procedures and standards on how intelligence is gathered, stored, accessed, and disseminated have been developed.
- This presentation highlights these procedures & standards!

Terrorist Screening Center

- **The Terrorist Screening Center's terrorism-screening database shows that U.S. authorities made more than 20,000 detentions as part of their terrorist-screening operations in 2006, but only a fraction of the people who were detained were actually arrested.**
- **Detentions by Customs and Border Protection agents accounted for more than half of that number, federal officials declined to say how many of the other 10,000 detainees were actually arrested, but the percentage was small, according to FBI officials.**
- **Critics of the database claim that the low arrest rate is proof that the government's screening efforts too often net innocent people, but federal officials say that the purpose of the database is to allow the government to keep track of suspicious persons, not necessarily to help authorities make arrests.**
- **For example, the database allowed U.S. officials to stop a suspicious Egyptian man from entering the country on multiple occasions; the man later carried out a suicide bombing in Qatar in 2005.**

Source: Washington Post (08/25/07) Page A1 by Ellen Nakashima

Success of TSC

- The U.S. terrorist watch list compiled by the Terrorist Screening Center now includes more than 755,000 names, which taking pseudonyms into account represent about 300,000 people "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of or related to terrorism."
- The list has been used about 53,000 times to identify individuals for potential arrest or to prevent them from entering the United States.
- Prior to 9/11, the list contained less than 20 entries, which grew to more than 150,000 within a few months after the attacks.

Source: "More Than 755,000 on US Terrorist Watch List"
Agence France Presse (10/24/07)

Typical Concerns relating to Intelligence Collection

- Maintenance of non-crime information
- Evidence of political, sexual and racial materials
- Freedom of association claims: religious, social, etc.
- Secrecy, spying and entrapment
- Failure to timely purge intelligence files

Homeland Security

Presidential Directive No. 6

- Integration and use of screening information to protect against terrorism.
 - develop, integrate, and maintain accurate information about individuals known or suspected of preparing for, or in aid of any terrorist acts on U.S. soil.
 - use that information for prosecution to the fullest extent of the law.
 - support Federal, State, County, Tribal, and local visa screening processes.

Homeland Security

Presidential Directives No. 11

- Comprehensive Terrorist Related Screening Procedures
 - detect, identify, track, and interdict foreign or domestic citizens that pose a threat to homeland security.
 - safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law.

Overview of Legal and Privacy Issues

Constitutional Issues

– First Amendment

- Right to assemble and petition
- Freedoms of religion, speech and the press

– Fourth Amendment

- Protection from unreasonable search and seizure

– Fourteenth Amendment

- Equal Protection
- Due Process

Overview of Legal and Privacy Issues

Statutory Framework

- Federal laws, including:
 - Privacy Act, 1974
 - Freedom of Information Act, 1966
 - Criminal Intelligence (28 CFR Part 23)
- State Statute (Indiana: IC 5-2-4)
- Agency policy

Federal Privacy Act

Govt. Data Collections & Disseminations Practices Act (GDCDPA)

- Allows individual to review almost all federal files (but does not specifically apply to state records) pertaining to him/herself;
- Places restrictions on the disclosure of personally identifiable information;
- Specifies no secret record systems on individuals; and
- Compels the government to reveal its information sources.

Federal Privacy Act

(GDCDPA)

- Assists individuals in obtaining information about *themselves*;
- Criminal records are generally exempt;
- Requires the information be:
 1. Accurate
 2. Complete
 3. Relevant
 4. Current

Freedom of Information Act

- Provides that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions of the records) are protected by a specific exemption.
- Must follow proper procedures.
- Must reasonably describe records being sought.
- Allow 10 days to respond to records request.
- Applies to records only, not tangible items or objects.
- Most states have laws patterned after FOIA.

Information Classifications

- Information is generally classified to safeguard active police and intelligence operations
- Information classifications include:
 - For Official Use Only (FOUO)
 - Sensitive but Classified (SBU)
 - Law Enforcement Sensitive (LES)
- Standard of *Need to Know/Right to Know* relates to access to the information

Legal Standards

- Reasonable Suspicion
- Criminal Predicate

Legal Standards

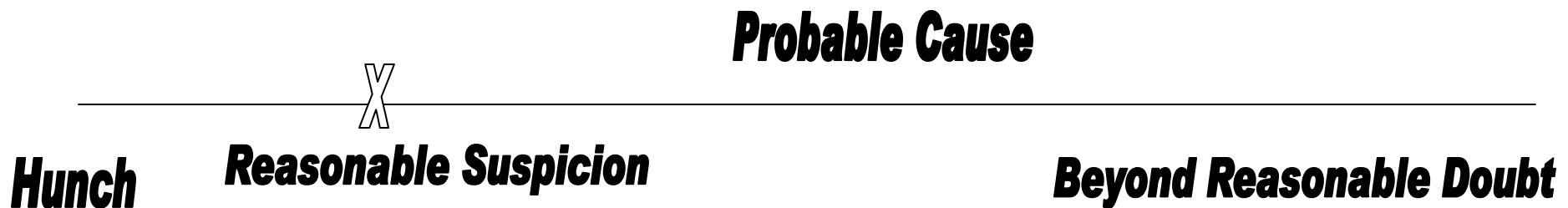
- Reasonable Suspicion or Criminal Predicate is established when:
 - information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity.

28 CFR Part 23

When an officer has reasonable suspicion that supports the belief that information relates to criminal activity, it may be collected, analyzed, stored, and shared.

Source: *Law Enforcement Prevention and Deterrence of Terrorist Acts*, Department of Homeland Security, Version 1.0, page 7/15.

Reasonable Suspicion Standard



Reasonable Suspicion Standard

- Subject has committed crime in the past,
- Subject is committing or conspiring to commit crime,
- Subject has intent (or motivation) to commit crime in the future (but be careful of entrapment!)

Reasonable Suspicion/ Criminal Predicate

Established when information exists which establishes sufficient facts to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

28 CFR Part 23.20 (c)

Patrol Example

- You observe an individual photographing a bridge.
- The individual notices your presence, and gets into his car and drives away.
- You notice a taillight out in the vehicle.
- You pull him over, notify him of the violation and engage him in discussion about his actions.
- If this stop leads to an arrest, courts (*Whren v. US*) will not assess your subjective motivation for making the stop (unless race was motivating factor).
- If this stop does not lead to an arrest, if you can articulate reasonable suspicion, the information gained by the encounter can be used to open an intelligence file.
- If you cannot articulate reasonable suspicion, you may be well advised to complete an information report.

Criminal Predicate & Potential Threat Element (PTE)

- Motivations are a key element when analyzing the potential for a group or individual to commit terrorist acts.
- Motivations include:
 1. Political
 2. Religious
 3. Racial
 4. Environmental
 5. Special Interest

Source: *Law Enforcement Prevention and Deterrence of Terrorist Acts*, Department of Homeland Security, Version 1.0, page 2/30.

Criminal Predicate & Potential Threat Element (PTE)

PTE is defined as “any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of a Weapon of Mass Destruction, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of a specific motivation or goal, possibly political or social in nature.”

Source: *Law Enforcement Prevention and Deterrence of Terrorist Acts*, Department of Homeland Security, Version 1.0, page 2/14.

Criminal Predicate & Potential Threat Element (PTE)

Specific Elements

- Any group or individual
- Allegations or information
- Unlawful use of force or violence, specifically WMD
- Against persons or property
- Intimidate or coerce government or civilians
- Specific motivation or goal (political or social)

Source: *Law Enforcement Prevention and Deterrence of Terrorist Acts*, Department of Homeland Security, Version 1.0, page 2/13.

Bottom Line

If you can show PTE, then you have the necessary predicate to conduct an investigation!

28 CFR Part 23

Summary Requirements

- Required compliance for law enforcement agencies that operate multi-jurisdictional criminal intelligence systems using federal monies.
- Provides guidelines addressing:
 - Submission and entry of criminal intelligence information
 - Secure storage
 - Inquiry and search capability
 - Controlled dissemination, and
 - Periodic review, validate and purge process

28 CFR Part § 23.2

Legislative Purpose

- “The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. [carrot]
- However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for federally funded projects are required.” [stick]

Complying with 28 CFR Part 23.20

Key Operating Principles:

- Reasonable suspicion must exist that an individual is involved in criminal conduct/activity and the information collected is relevant to such activity [23.20 (a)]
- Cannot collect or maintain information on political, religious or social views, associations or activities of any individual or group unless reasonable suspicion exists involving the individual or group to criminal conduct or activity [23.20 (b)]

Collection Standards

A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance.

28 CFR Part 23.20 (d)

Collection Standards

Collection of information must be legal & ethical:

No political, racial, ethnic, social bias

No Trespass/No Invasion of Privacy

No Constitutional Violations-

(1st/4th/5th/8th/14th)

Dissemination Standards

A project or authorized recipient shall disseminate criminal intelligence information only where there is a **need to know** and a **right to know** the information in the performance of a law enforcement activity

28 CFR Part 23.20 (e)

Dissemination Standards

Criminal intelligence shall only be disseminated to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security and dissemination which are consistent with principles outlined in 28 CFR Part 23.

Dissemination Standards

- A project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles [23.20 (f) (1)]
- Dissemination of criminal intelligence information allowed to a government official or to any other individual, when necessary, to avoid imminent danger to life or property [23.20 (f) (2)]

Additional Requirements

- **A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage.**
- **A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept.**
- **Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials.**
- **Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies.**
- **The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.**

28 CFR Part 23.20 (g)

Additional Requirements

- All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance.
- Such procedures shall provide for the **periodic review** of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections.
- All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain.
- Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

28 CFR Part 23.20 (h)

Plain Language Requirements

- Audit trails required
- Records must provide who information is released to, why it is released and the date of dissemination
- Records relating to sensitivity & confidence levels, and the identities of submitting agencies and control officials
- Procedures to assure that all information has relevancy
- Procedures for the periodic review of information
- Information that is misleading, obsolete or unreliable shall be purged and destroyed

Maintenance of Record Requirements

- Physical Security Required
- Segregate “Classes” of Records
 1. Active Investigations
 2. Intelligence Files
 3. Temporary/Working Files
- Establish an official custodian of records
- Limit the information placed in each file (according to the type or reason for the file)

IC 5-2-4

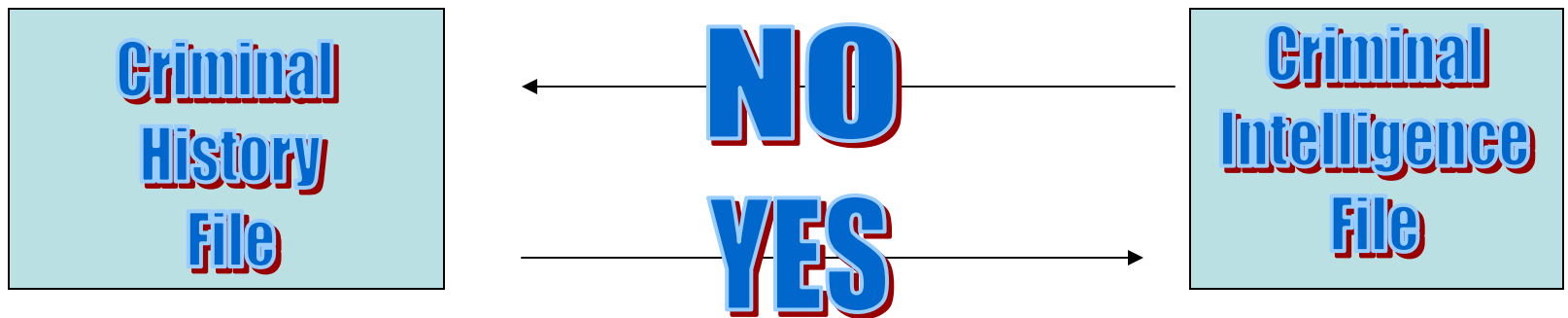
Maintenance of Records

- File restrictions (**IC 5-2-4-2**)
- Relevancy (**IC 5-2-4-3**)
- Retention and destruction of files (**IC 5-2-4-4**)
- Political, religious and social view restrictions (**IC 5-2-4-5**)
- Confidentiality (**IC 5-2-4-6**)
- Unlawful release of criminal intelligence (**IC 5-2-4-7**)

IC 5-2-4-2: Files Restricted

- Criminal intelligence information shall not be placed in a criminal history file, nor shall a criminal history file indicate or suggest that a criminal intelligence file exists on the individual to whom the information relates.
- Criminal history information may, however, be included in criminal intelligence files.

Illustration



IC 5-2-4-3: Criminal activity and relevancy restriction

Criminal intelligence information concerning a particular individual shall be collected and maintained by a state or local criminal justice agency only if grounds exist connecting the individual with known or suspected criminal activity and if the information is relevant to that activity.

IC 5-2-4-4: Retention and destruction

Criminal intelligence information shall be reviewed by the chief executive officer of the criminal justice agency at regular intervals to determine whether the grounds for retaining the information still exist and if not, it shall be destroyed

IC 5-2-4-5: Political, religious or social views, associations or activities restricted

- **No criminal justice agency shall collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, corporation, limited liability company, business, or partnership unless:**
 - 1. Such information directly relates to an investigation of past or threatened criminal acts or activities, and**
 - 2. There are reasonable grounds to suspect the subject of the information is or may be involved in criminal acts or activities.**

IC 5-2-4-6: Confidentiality

- Criminal intelligence information is hereby declared confidential and may be disseminated only in accordance with Section 7 of this chapter, and
- Only if the agency making the dissemination is satisfied that the need to know and intended uses of the information are reasonable, and
- That the confidentiality of the information will be maintained.

IC 5-2-4-7:

Unlawful release and offense

- Person who knowingly releases criminal intelligence information to an agency or person other than a criminal justice agency commits a Class A misdemeanor, unless:
- When necessary to avoid imminent danger to life or property, may disseminate **an assessment of criminal intelligence information** to:
 - (1) a government official; or
 - (2) another individual:
 - (A) whose life or property is in imminent danger;
 - (B) who is responsible for protecting the life or property of another person; or
 - (C) who may be in a position to reduce or mitigate the imminent danger to life or property.

Information Protection

Does your Agency subscribe to...?

- The Global Justice Information Sharing Initiative,
- National Criminal Intelligence Sharing Plan,
- IACP Code of Ethics,
- IACP Code of Conduct,
- LEIU Criminal Intelligence File Guidelines,
- 28 CFR Part 23 and
- IC 5-2-4

Summary

- Use common sense
- Review Legal Principles
- Remember “need to know” & “right to know”
- Maintain control and consistently assess your files
- Intelligence is an important tool, use it correctly but do not be afraid of it!

QUESTIONS



Dr. James F. Pastor, Ph.D., J.D.

312-423-6700

www.securelaw.info