ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
CRIMINAL JUSTICE DIVISION

MEMORANDUM

DATE: November 25, 2015

FROM: Darin E Tweedt, Chief Counsel
Criminal Justice Division

SUBJECT: Criminal Justice Division Overview

This memorandum is to assist outside counsel with the HR investigation into the use of the "Digital Stakeout" computer program by Special Agent (SA) [redacted] The memorandum provides an overview of the Criminal Justice Division's responsibilities and organization.

Overview of Responsibilities

The Criminal Justice Division provides investigative, trial and training support to Oregon's District Attorney's and law enforcement agencies. The Division also acts as a safety net for District Attorneys' Offices in crisis. The Division's prosecutors are often called upon to act as the District Attorney and perform all local prosecution functions in times of need. Finally, the Division leads or participates in several important criminal and anti-terrorism related information sharing and analysis programs.

The Criminal Justice Division conducts specialized criminal investigations and prosecutions and provides highly trained and experienced special agents, prosecutors and analysts to fight crime across Oregon. The Division also provides outreach and training to communities, victim service providers, and members of the law enforcement community to help ensure that Oregonians receive the highest level of service from the criminal justice system.

Program Description

The Division is divided into three sections: The Special Investigations and Prosecutions Section, the Organized Crime Section and the Criminal Intelligence Unit. Members of these units perform a variety of investigation, prosecution and analytical roles, some of which are detailed below.

Special Investigations and Prosecution Section

The Special Investigations and Prosecution Section is composed of three specialty units: the District Attorney/Law Enforcement Assist Unit, the Child Exploitation Unit and the Cooperative Disability Investigations Unit.

EXHIBIT A

2250 McGilchrist St SE, Suite 100, Salem, OR 97302-1147
Telephone: (503) 378-6347 Fax: (503) 373-1936 TTY: (800) 735-2900 www.doj.state.or.us

- District Attorney/Law Enforcement Assistance Unit: The District Attorney/Law Enforcement Assistance Unit supports law enforcement agencies and District Attorneys by investigating and prosecuting highly complex criminal cases, cases requiring specialty expertise, and cases in which the investigating agency or District Attorney has a conflict. This unit has experts in the investigation and prosecution of homicide, child exploitation, Driving Under the Influence of Intoxicants, and domestic violence. In addition, this unit is primarily responsible for providing important training to law enforcement officers and prosecutors throughout Oregon at low or no cost. The unit is composed of five attorneys, one Special Agent and one Operations and Policy Analyst assigned as Program Coordinator to the Oregon District Attorneys Association.

- Child Exploitation Unit: The Child Exploitation Unit focuses on identifying, investigating, prosecuting and preventing crimes relating to the sexual exploitation of children. The Child Exploitation unit is comprised of an anti-human trafficking initiative and the Oregon Internet Crimes Against Children Task Force (ICAC). The human trafficking initiative focuses on the commercial sexual exploitation of children outside of the Portland metropolitan area. The Internet Crimes Against Children Task Force focuses on investigating, prosecuting and preventing the sexual exploitation of children on the internet. In addition to case work, members of the Child Exploitation Unit conduct statewide trainings for law enforcement officers, prosecutors, schools and parents. The unit is composed of an attorney, five Special Agents and a Research Analyst.

- Cooperative Disability Investigations Unit: This unit is part of a multi-agency task force that investigates suspicious social security disability claims. The unit's mission is to obtain evidence that can resolve questions of fraud before benefits are ever paid. The Criminal Justice Division component is three Special Agents and an Administrative Specialist.

Organized Crime Section

The Criminal Justice Division is charged by statute with investigating and prosecuting organized crime and allegations of public officials involved in corruption or malfeasance. ORS 180.610. The Organized Crime Section has criminal investigators, prosecutors, and analysts who specialize in identifying and combating such crimes. It is composed of three attorneys and five Special Agents. Section members often team with analysts from the Criminal Intelligence unit.

In addition, the Division has specialized equipment and trained personnel to conduct wiretap investigations against organized crime groups. These investigations are highly effective at disrupting and dismantling criminal organizations.

Criminal Intelligence Unit

The ability to gather and analyze information about criminals and their organizations is invaluable to law enforcement agencies.[1] The Criminal Intelligence Unit, aka Criminal Intelligence Center, facilitates the gathering, analysis and sharing of criminal information with local, state and national law enforcement agencies. The Unit is composed of the Oregon TITAN Fusion Center, the Oregon HIDTA Investigation Support Center, and the Oregon HIDTA Watch Center.

- Oregon TITAN Fusion Center: The Fusion Center is Oregon's focal point for receiving, analyzing, gathering, and sharing threat-related information in order to better detect, prevent, investigate, and respond to criminal and terrorist activity.

The Fusion Center is composed primarily of staff from the Criminal Justice Division.[2] This staff works in conjunction with federal, state and local law enforcement agencies. The Fusion Center produces threat assessments[3], officer safety bulletins, general crime bulletins and terrorism related bulletins. In addition, the Fusion Center is an essential component of the state's critical infrastructure review process. The Fusion Center also provides criminal analysts to assist federal, state and local law enforcement agencies with criminal investigations. Finally, the Center provides important training to law enforcement agencies, businesses and first responders about active shooters and the latest terrorist trends, techniques and procedures.

- High Intensity Drug Trafficking Area (HIDTA) Investigation Support Center: The Investigation Support Center is a co-located multi-agency program. Its mission is to promote, facilitate, and coordinate the exchange of criminal intelligence information, and provide

---

[1] The benefits of gathering and analyzing criminal information was recognized by the Oregon legislature in 1977 when it directed the Department of Justice to:

> "(2) Establish a coordinated system of collecting, storing and disseminating information relating to organized crime.
> (3) Develop and maintain a liaison between local, state and federal law enforcement agencies in Oregon, assisting them in the investigation and suppression of organized criminal activity and encouraging cooperation among those agencies.
> (4) Conduct comprehensive factual studies of organized criminal activity in Oregon, outlining existing state and local policies and procedures with respect to organized crime, and formulating and proposing such changes in those policies and procedures as the department may deem appropriate." ORS 180.610 (2), (3) and (4).

[2] The Criminal Justice Division component is one attorney, one Special Agent, five Research Analysts and an IS Specialist.

[3] A threat assessment is the "[p]rocess of identifying or evaluating entities or events for indications of potential harm to life, property, operations or information. These assessments involve investigative research which results in a written product identifying possible threats to a specific person or incident. Examples include Pendleton Round-up, Hillsboro Air Show or Governor's Inauguration. Threat assessments may be conducted by an individual or team of analysts based on the complexity of the assessment." Oregon TITAN Fusion Center Procedure, Threat Assessments/Risk & Vulnerability Assessments, September 18, 2015.

Oregon TITAN Fusion Center

PRIVACY POLICY

1.0 Purpose

The Oregon TITAN Fusion Center (the Center) was initiated in response to the increased need for timely information sharing and exchange of terrorism and crime-related information among members of the Oregon law enforcement community. The purpose of the Center is to protect the citizens of the State of Oregon from terrorism activity by providing an all-crimes information clearinghouse for federal, state, local and tribal law enforcement agencies.

The Center is a collaborative effort of state and federal law enforcement agencies to provide resources, expertise, and information to the law enforcement community with the goal of maximizing the ability to detect, disrupt, prevent, and respond to terrorism, organized crime, and gang-related criminal activity.

One component of the Oregon TITAN Fusion Center focuses on the development and exchange of information, including criminal intelligence. This component focuses on the process where information is collected, integrated, evaluated, analyzed and disseminated. The Oregon law enforcement community recognizes that combining intelligence resources will allow greater dissemination of intelligence products and will greatly enhance the ability to predict, prevent, and respond to terrorist threats and related criminal activity within the state. Law enforcement agencies also recognize the role of intelligence sharing in avoiding conflicting operational activities that may endanger officers and civilians.

The information received and maintained by the Oregon TITAN Fusion Center is provided on a voluntary basis by "participating agencies," or is information obtained by the Center from other sources such as other law enforcement agencies, "open" media sources, commercial databases, public records and unclassified government material. The Oregon TITAN Fusion Center will keep a record of the source of all information sought and collected by the Center. "Participating agencies" are those which have assigned personnel to work at the Center and have entered into a Memorandum of Understanding. The Oregon TITAN Fusion Center's products and services will be made available to local, state, and federal law enforcement agencies operating in Oregon and to other entities as permitted by this Privacy Policy (Policy).

The purpose of this privacy, civil rights, and civil liberties protection policy is to promote Oregon TITAN and user conduct that complies with applicable federal, state, local, and tribal law (see Appendix A, Terms and Definitions, of this policy)] and assists the Center and its users in:

1. Increasing public safety and improving national security.
2. Minimizing the threat and risk of injury to specific individuals.
3. Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.

4. Minimizing the threat and risk of damage to real or personal property.
5. Protecting individual privacy, civil rights, civil liberties, and other protected interests.
6. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
7. Minimizing reluctance of individuals or groups to use or cooperate with the justice system.

2.0 Compliance with Laws Regarding Privacy, Civil Rights, and Civil Liberties

All participating agency personnel, personnel providing information technology services to the Oregon TITAN Fusion Center, private contractors, and users (including Information Sharing Environment [ISE] participating centers and agencies) will comply with the provisions contained in this Policy and with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information as stated below and herein.

The internal operating policies governing the operation of the Oregon TITAN Fusion Center comply with 28 CFR Part 23, ORS 181.575, the Oregon Department of Justice Administrative Rules 137-090- 0000-0225, ORS Chapter 192 relating to public records, the U.S. and Oregon constitutions, and state and federal law pertaining to confidential records and records containing personally identifiable information.

The Center's Executive Advisory Committee has approved this Policy and oversees its implementation in various ways including: liaising with the community to ensure that privacy and civil rights are protected as provided in this policy and by the Center's information-gathering and collection, retention, and dissemination processes and procedures; and conducting an annual review and recommendation for updates to the policy, with the assistance of the Privacy Officer, in response to changes in law and implementation experience, including the results of audits and inspections. The Director for the Center is responsible for insuring that all participating agency personnel, personnel providing information technology services to the Oregon TITAN Fusion Center, private contractors, and users will comply with the terms of this Policy. Section 9 of this Policy contains specific provisions relating to the review, implementation and enforcement of this Policy.

The Privacy Officer, who is the attorney for the Center and who is appointed by the Chief Counsel of the Oregon Department of Justice Criminal Division, receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us.

The Director of the Oregon TITAN Fusion Center ensures that enforcement procedures and sanctions outlined in Section 9.3 are adequate and enforced.

3.0 Definitions

Appendix A provides definitions for words or phrases regularly used in this Policy to explain their meaning in the context of this Policy.

4.0 Seeking, Collecting, and Retaining Information and Criminal Intelligence

Each participating agency will determine which database(s) it will provide, and access to such database(s) will be governed by the laws that govern the particular agency respecting such data, as well as by applicable federal laws.

Because the laws governing information that can be sought, collected or released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information will abide by the collection limitations applicable to it by reason of law. Information contributed to the Oregon TITAN Fusion Center should be that which has been collected in conformance with those limitations.

The following provisions set out the policies that will guide the operation of the Oregon TITAN Fusion Center in four areas: 1) the types of information that may be sought and the types of information that may be collected or retained; 2) information that may not be sought, collected, or retained; 3) permissible methods of seeking information, including the receipt of information from third parties in the form of unsolicited tips; and 4) assessing information with respect to its validity, reliability, and access or disclosure.

4.1 Information That May Be Sought or Retained

1. The Oregon TITAN Fusion Center will seek or retain information only under the following circumstances:
    a. The source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
    b. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate, and
    c. The information is based on a possible threat to public safety or the enforcement of the criminal law; or
    d. Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation, and the information is relevant to the criminal (including terrorist) conduct or activity; or
    e. The information is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
    f. The information is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches).

2. Collection, retention and storage of criminal intelligence will comply with applicable state and federal law. The Center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.

3. The Oregon TITAN Fusion Center will not seek or retain information about an individual or organization solely on the basis of their religious, political, racial, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

4. The Oregon TITAN Fusion Center shall apply labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
    a. The information is "protected information" to include "personal data" on any individual (see Definitions), and, to the extent expressly provided in this policy, includes organizational entities.

5. The information is subject to ORS 181.575, ORS 192.410-192.505, OAR 137-090-0000, et seq., 28 CFR Part 23, the United States Constitution and the Oregon Constitution restricting access, use or disclosure.

6. The Oregon TITAN Fusion Center personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
    a. Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
    b. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
    c. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
    d. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

7. The Oregon TITAN Fusion Center will keep a record of the source of all retained information.

8. Tips and Leads Information or Data – The Oregon TITAN Fusion Center may seek or retain information of uncorroborated information or reports generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads may include suspicious Incidents Reports (SIR) information, suspicious activity report (SAR) information, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

   A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information raises some suspicion but may be based on a level of suspicion that is less than "reasonable suspicion" and, without further inquiry or analysis; it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning. Center personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

   a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the eligibility of the information have been unsuccessful. The Center will use a standard reporting format and standard collection codes for SAR information.
   b. Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
   c. Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
   d. Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

e. Retain information for one hundred and eighty (180) days in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label. An additional one hundred and eighty (180) day retention may be authorized by the Director of the Center, after consultation with Privacy Officer, if after the first one hundred and eighty (180) days, it appears likely that based upon investigation during the first one hundred and eighty (180) days the unvalidated tip, lead, or SAR information may be credible.

f. Adhere to and follow the Center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

9. The Oregon TITAN Fusion Center incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

10. The Oregon TITAN Fusion Center will identify and review protected information that may be accessed from or disseminated by the Center prior to sharing that information through the Information Sharing Environment. Further, the Center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

11. The Oregon TITAN Fusion Center requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    a. The name of the originating Center, department or agency, component, and subcomponent.
    b. The name of the Center's justice information system from which the information is disseminated.
    c. The date the information was collected and, where feasible, the date its accuracy was last verified.
    d. The title and contact information for the person to whom questions regarding the information should be directed.

12. The Oregon TITAN Fusion Center will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

4.2 Methods of Seeking or Receiving Information

1. Information gathering and investigative techniques used by the Oregon TITAN Fusion Center will comply with all applicable laws, including but not limited to ORS 181.575, OAR 137-090-0000, et seq., 28 CFR Part 23, the United States Constitution and the Oregon Constitution.

2. The Oregon TITAN Fusion Center's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The Oregon TITAN Fusion Center's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities or associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. The Oregon TITAN Fusion Center will not directly or indirectly seek, receive or retain information from:
    a. An individual or nongovernmental information provider, who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or Oregon TITAN Fusion Center policy.
    b. An individual or information provider who is legally prohibited from obtaining the specific information sought or disclosing it to the Center.
    c. An individual or information provider who used methods for collecting the information that the Center itself could not legally use, except where:
        i. The information was provided through an anonymous tip, in which case the Center may use the information as a basis to investigate further, but shall not retain the information unless it meets the requirements set out in Section 4.1; or
        ii. The information was provided by a cooperating defendant or criminal informant and the person was not acting at the direction or under the control of the Center; and
        iii. The commercial database entities provide a written assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

d. The Center could not itself legally collect the specific information sought from the individual or information provider, except that the Center may receive aggregated information where:
    i. The individual or information provider has lawfully obtained such information; and
    ii. The Center could lawfully collect the specific pieces of information that comprise the aggregate.

e. The Center has not taken the steps necessary, such as obtaining a search warrant or subpoena, to be authorized to seek and receive the information.

5. Information gathering and investigative techniques used by the Oregon TITAN Fusion Center will be no more intrusive than is necessary in the particular circumstance to gather information it is authorized to seek or retain under applicable statues and rules.

6. External agencies that access the Oregon TITAN Fusion Center's information or share information with the Center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

4.3 Classification Regarding Validity and Reliability of Information

1. At the time of retention in a system maintained by the Oregon TITAN Fusion Center, the information will be categorized regarding its:
    a. Content validity;
    b. Nature of the source (anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source); and
    c. Source reliability.

4.4 Classification of Information according to limits on access and disclosure

1. At the time a decision is made to retain information, it will be classified pursuant to the applicable limitations on access and sensitivity of disclosure in order to:
    a. Protect an individual's right of privacy and civil rights;
    b. Protect confidential sources and police undercover techniques and methods;
    c. Not interfere with or compromise pending criminal investigations; and
    d. Provide legally required protection based on the status of an individual (such as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter, a domestic violence crime victim or as a witness).

2. At the time a decision is made to retain, or store, criminal intelligence, it will be classified pursuant to the applicable limitations on access and disclosure contained in OAR 137-090-0100. Criminal intelligence information is classified according to the following system: Sensitive, Confidential and Restricted.
See, http://arcweb.sos.state.or.us/rules/OARS_100/OAR_137/137_090.html

3. The classification of stored information will be reevaluated whenever:
    a. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
    b. There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

4. Classifications regarding access will be used to control:
    a. The information to which a particular group or class of users can have access based on the group or class;
    b. What information a class of users may add, change, delete or print; and
    c. To whom the information may be disclosed and under what circumstances.

5. Credentialed, role-based access criteria will be used by the Center, as appropriate, to control:
    a. The information to which a particular group or class of users can have access based on the group or class.
    b. The information a class of users can add, change, delete, or print.
    c. To whom, individually, the information can be disclosed and under what circumstances.

6. Access to or disclosure of records retained by the Center will be provided only *to persons within the center or in other governmental agencies* who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the Center and the nature of the information accessed will be kept by the Center.

7. The labeling of retained information will be reevaluated by the Center or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

5.0 Information Quality

The agencies participating in the Oregon TITAN Fusion Center remain the owners of the data they contribute.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Oregon TITAN Fusion Center, any agency that obtains information through the Center must independently verify the information with the agency that originally provided it before taking any official action (e.g., warrant or arrest) based on the information.

User agencies and individual users are responsible for complying with applicable laws governing the use, further dissemination, purging, and updating of information obtained from the Center.

5.1 The Oregon TITAN Fusion Center will make every reasonable effort to ensure that information sought or retained is:

1. Derived from reliable and trustworthy sources of information;

2. Accurate, current; and

3. Complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

5.2 The Oregon TITAN Fusion Center will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information from criminal intelligence storage systems.

5.3 The Oregon TITAN Fusion Center will make every reasonable effort to ensure that information will be deleted from criminal intelligence storage systems when the Center learns that:

1. The information is invalid, inaccurate, unverifiable, no longer useful, no longer relevant, or otherwise unreliable;

2. The information does not support a reasonable suspicion of criminal activity;

3. The source of the information did not have authority to gather the information or to provide the information to the Center; or

4. The source of the information used prohibited means to gather the information, except where:
   a. The information was provided through an anonymous tip, in which case the Center may use the information as a basis to investigate further, but shall not retain the information unless it meets the requirements set out in Section 4.1; or
   b. The information was provided by a cooperating defendant or criminal informant and the person was not acting at the direction or under the control of the Center.

5.4 The Oregon TITAN Fusion Center will investigate, in a timely manner, alleged errors and deficiencies (or refer them to the originating agency) and correct, delete, or refrain from using protected information found to be erroneous or deficient.

5.5 The Center will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the Center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the Center did not have authority to gather the information or to provide the information to another agency; or the Center used prohibited means to gather the information (except when the Center's information source did not act as the agent of the Center in gathering the information).

5.6 Originating agencies external to the Center are responsible for reviewing the quality and accuracy of the data provided to the Center. The Center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

5.7 At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

5.8 The labeling of retained information will be reevaluated by the Oregon TITAN Fusion Center or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

5.9 The Oregon TITAN Fusion Center will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the Center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

6.0 Collation and Analysis of Information

6.1 Collation and Analysis

Information sought or received by the Oregon TITAN Fusion Center or from other sources will only be analyzed:

1. By qualified individuals approved and employed by the Oregon Department of Justice, or by a participating agency, who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved and trained accordingly; and

2. To provide tactical and/or strategic criminal intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities generally, including terrorism; or

3. To further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the Center.

Information sought or received by the agency or from other sources will not be analyzed or combined in a manner or for a purpose that violates Section 4.1.4.

6.2 Oregon TITAN Fusion Center requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the Center. Analytical products may be reviewed and approved for dissemination or sharing by the Director of the TITAN Fusion Center, the Oregon Department of Justice - Criminal Justice Division's Special Agent in Charge, Deputy Chief Counsel or the Chief Counsel when:

1. Immediate dissemination or sharing is reasonably necessary to protect life or prevent physical injury where the risk of injury or death is imminent, and

2. The Privacy Officer cannot be contacted or contact with the Privacy Officer would delay dissemination or sharing and delay would reasonably increase the risk of injury or death of a person.

6.3 Information subject to collation and analysis is information as defined and identified in Section 4.1 1. of this policy.

6.4 Records about an individual or organization from two or more sources will not be merged by the Oregon TITAN Fusion Center unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

6.5 If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the Oregon TITAN Fusion Center if accompanied by a clear statement that it has not been adequately established that the information relate s to the same individual or organization.

7.0 Sharing and disclosure of Information/Criminal Intelligence

This section addresses to whom and under what circumstances the Oregon TITAN Fusion Center may disclose information/criminal intelligence. Disclosure may be passive, by allowing authorized law enforcement personnel access to databases via direct queries, or active, as when the Center disseminates or publishes information in bulletins, notices, or reports.

Information obtained from or through the Oregon TITAN Fusion Center will not be used or disclosed for purposes other than those specified in the Memorandum of Understanding signed by each participating agency. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Agencies external to the Oregon TITAN Fusion Center may not disseminate information accessed or disseminated from the Center without approval from the Center or other originator of the information.

The Oregon TITAN Fusion Center adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

7.1 Sharing Information within the Oregon TITAN Fusion Center and with Other Law Enforcement Agencies

1. Access to information retained by the Oregon TITAN Fusion Center will only be provided to personnel assigned to the Center or in other governmental agencies who are authorized by law to have access; who will use it only for legitimate law enforcement, public protection, public prosecution, or public health purposes ("right to know"); and who will use it only in the performance of their official duties ("need to know").

2. The Center will maintain an audit trail to document access by or dissemination of information to such persons.

7.2 Sharing Criminal Intelligence within the Oregon TITAN Fusion Center and with Criminal Law Enforcement Agencies

Criminal intelligence can only be used for lawful purposes. A lawful purpose means that the request for information is directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

1. Access to criminal intelligence will be provided according to OAR 137-090-0000 et.seq. and other applicable laws.

2. The Center shall not confirm the existence or nonexistence of criminal intelligence to any person or agency that would not be eligible to receive the information itself.

7.3 Sharing Information with those Responsible for Public Protection, Safety, or Public Health

1. Information retained by the Oregon TITAN Fusion Center may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes ("right to know") and only in the performance of official duties in accordance with applicable laws and procedures ("need to know").

2. An audit trail will be kept of the access by or dissemination of information to such persons.

3. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

4. The Center shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

7.4 Sharing Information for Specific Purposes

1. Information gathered and retained by the Oregon TITAN Fusion Center may be disseminated for specific purposes upon request by persons authorized by law to have such access ("right to know") and only for those uses or purposes specified in the law ("need to know").

2. The Center shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

3. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the Center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of 20 years by the Center.

7.5 Disclosing Information to the Public

1. Information gathered and retained by the Oregon TITAN Fusion Center may be disclosed to a member of the public only if the information is a public record as defined in ORS 192.410-192.505 and is not exempt from disclosure.

2. The Center may collect a fee from those requesting information, as authorized in ORS 192.440, for costs associated with providing the information.

3. The Oregon TITAN Fusion Center will follow OAR 137-090-0040 in responding to requests for stored criminal intelligence.

4. The Center shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

5. The Center will maintain an audit trail of all requests and of the information disclosed.

7.6 Disclosing Information to the Individual about Whom Information has been Gathered

1. Upon satisfactory verification of his or her identity and subject to the conditions specified in Section 7.6.3, an individual is entitled to know the existence of and to review the information about himself or herself that has been gathered and retained by the Center. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The Center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual.

2. Upon receiving such a request, the Center will direct the individual to contact the agency that originally submitted the information. The submitting agency will determine what information may be released under the laws governing that agency.

3. The existence, content, and source of the information will not be made available to an individual when:
    a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (ORS 192.501(3));
    b. Disclosure would endanger the health or safety of an individual, organization, or community (ORS 192.501(18) and (23), ORS 192.502(2), (4) and (8));
    c. The information is stored in a criminal intelligence system, such as the Oregon State Intelligence Network (28 CFR Part 23 and ORS 137-090-0150– 137-090-0170); or
    d. Disclosure is otherwise limited or prohibited by law.

4. If the information does not originate with the Center, the request will be referred to the originating agency, if appropriate or required, or the Center will notify the source agency of the request and its determination that disclosure by the Center or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

5. If an individual challenges the accuracy or completeness of information retained at and the Center and for which the Center is the original source, the Center will inform the individual of the procedure for requesting a review of any challenges and for making corrections.
    a. If a request for correction is denied, the Center will advise the individual of the reason(s) for the denial.
    b. The Center will also inform the individual of the procedure for appeal when the Center has declined to correct challenged information to the degree requested by the individual.
    c. A record will be kept of all requests for corrections and the resulting action, if any.

6. The agency may collect a fee from those requesting information, as authorized in ORS 192.440, for costs associated with providing the information.

7. The Center will maintain a record of all requests and of the information disclosed to an individual.

8. Information gathered or collected and records retained by the Center will not be:
    a. Sold, published, exchanged, or disclosed for commercial purposes.
    b. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
    c. Disseminated to persons not authorized to access or use the information.

9. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:
    a. Is exempt from disclosure,
    b. Has been or may be shared through the ISE,
        i. Is held by the Oregon TITAN Fusion Center and
        ii. Allegedly has resulted in demonstrable harm to the complainant.

10. The Center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the Center's Privacy Officer at the following address: 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the Center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the Center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the Center will not share the information until such time as the complaint has been resolved. A record will be kept by the Center of all complaints and the resulting action taken in response to the complaint.

11. To delineate protected information shared through the ISE from other data, the Oregon TITAN Fusion Center maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

7.7 Records that will ordinarily not be provided to the public

1. Records required to be kept confidential by law are exempted from disclosure requirements under ORS 192.410-192.505.

2. Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

3. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under ORS 192.410-192.505.

4. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements ORS 192.410-192.505. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

5. Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under 28 CFR Part 23 or OAR 137-090-0150 – 137-090-0170 be shared without permission.

6. A violation of an authorized nondisclosure agreement entered into between participating agencies as authorized by Oregon Public Records laws.

8.0 Retention, Review, Purge, and Destruction of Information/Stored Criminal Intelligence

8.1 Retention and Review of Information

1. When information retained at the Center has no further value or meets the criteria for removal under ORS Chapter 192, OAR 137-090-0000 to 137-090-0225, i28 CFR Part 23, and Center policy, it will be returned to the submitting agency or purged and destroyed according to the above stated law or Center policy.

2. The Director of the ODOJ Criminal Justice Division's Criminal Intelligence Unit or a designee will review information prior to its removal from a record or information storage system.

8.2 Destruction of Records Containing Information

1. Records containing information will be destroyed, or returned to the submitting (originating) agency, according to the requirements of OAR 166-300-0015.

2. The Center will provide notification of proposed destruction or return of records to the submitting agency.

3. The Center will maintain a record of the information that has been purged or returned.

8.3 Review, Purge, and Destruction of Stored Criminal Intelligence

The Center will follow 28 CFR Part 23 and OAR 137-090-0150 – 137-090-0170 in reviewing, purging, and destroying stored criminal intelligence. The maximum retention period is five (5) years, and a criminal intelligence file must be purged after five years unless the information in that criminal intelligence file has been updated consistent with these Standards and Procedures.

The procedure contained in 28 CFR Part 23 Section D will be followed by Oregon TITAN Fusion Center for notification of appropriate parties, including the originating agency, before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

1. The Center will maintain a record that information has been purged and destroyed, which will contain at a minimum the date of the purge or return and if returned the name and address of the agency to which it was returned; and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

9.0 Accountability and Enforcement

9.1 Information System Transparency

1. A link to the Oregon TITAN Fusion Center Privacy Policy will be included on the publicly accessible Oregon Department of Justice website, http://www.doj.state.or.us/. The link will be located under "Request for Public Records" and the sub-category "OTFC Privacy Policy."

2. The Oregon TITAN Fusion Center will designate a person who shall be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system. The Privacy Officer may be contacted at 610 Hawthorne Ave, SE, Suite 210, Salem, Oregon, 97301, oregonfusioncenter@doj.state.or.us .

9.2 Accountability for Activities

1. ODOJ will appoint a Director for the Center (Center Coordinator) who will have primary responsibility for the day-to-day operation of the Oregon TITAN Fusion Center, including operations, its justice systems; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this Privacy Policy.

2. Use of the Center's information systems is limited to personnel who have been selected, approved, and trained accordingly. Each individual user must complete an Individual User Agreement and is required to abide by this Privacy Policy in the use of information obtained by and through the Center. Individual users remain responsible for their legal and appropriate use of the information

contained therein.

3. The Oregon TITAN Fusion Center's Security Officer is designated and trained to serve as the Center's security officer.

4. The Oregon TITAN Fusion Center will operate in a secure facility protected from external intrusion. Remote access to databases located at the Center's headquarters will be provided over secure network lines.

5. The Center will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The methods and techniques used shall be consistent with security practices that are generally accepted within the law enforcement community.

6. The Oregon TITAN Fusion Center will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

7. The Oregon TITAN Fusion Center will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized by law or agency policy to take such actions.

8. Access to Oregon TITAN Fusion Center information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

9. Queries made to the Oregon TITAN Fusion Center's data applications will be logged into the data system identifying the user initiating the query.

10. The Oregon TITAN Fusion Center will utilize watch logs to maintain audit trails of requested and disseminated information.

11. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

12. The Oregon TITAN Fusion Center will adopt and follow procedures and practices to ensure and evaluate the compliance of its users and the system itself with the provisions of this Privacy Policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer or Center Director the Center.

13. The Oregon TITAN Fusion Center will require any individuals authorized to use any system located at the Center's headquarters to provide a written acknowledgement of receipt of this policy and to agree in writing to comply with the provisions of this Privacy Policy. Such authorized individuals include personnel assigned to the Center and participating users.

14. The Oregon TITAN Fusion Center Executive Advisory Committee internally will annually conduct or coordinate audits and inspections of the information contained in information systems located at the Center's headquarters. The committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the Center. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the agency's information.

15. The Executive Advisory Committee will also be responsible for overseeing the investigation into any allegation of unauthorized or illegal use of the Center's data or information, including alleged violations of this Policy.

16. The Oregon TITAN Fusion Center Privacy Officer will annually review and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations. This review will be performed with the Center's legal counsel and such other persons as may be designated by the Chief Counsel of ODOJ's Criminal Division.

17. Any changes made to this Policy will be presented to the Oregon TITAN Fusion Center Executive Advisory Committee for approval.

18. The Oregon TITAN Fusion Center will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person, where such action threatens physical, reputational, or financial harm to the person.

19. The notice will be made promptly and without unreasonable delay following discovery or notification of the unauthorized access, consistent with the legitimate needs of law enforcement to investigate the circumstances surrounding the access or any measures necessary to determine the scope of such access and to reasonably restore the integrity of the information system. Notice need not be given if doing so meets the criteria specified in Section 7.6.3.

20. The audit log of queries made to the Oregon TITAN Fusion Center will identify the user initiating the query.

21. The Oregon TITAN Fusion Center will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 20 years (pursuant to Oregon Department of Justice Records Retention Schedule and OAR 166-300-0015) of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

22. The Oregon TITAN Fusion Center's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the Center's Privacy Officer.

9.3 Enforcement

If a user is suspected of or found to have violated the provisions of this Policy regarding the collection, classification, retention, sharing, use, disclosure, or destruction of information, the Director of the Oregon TITAN Fusion Center will:

1. Suspend or discontinue the user's access to information;

2. Take disciplinary action against the person as permitted by applicable personnel policies;

3. Apply other sanctions or administrative actions as provided in the Center's personnel policies;

4. Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or take other action authorized by the employer's personnel policy; or

5. Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of this Policy as stated in Section 1. The Oregon TITAN Fusion Center reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's privacy policy.

10.0 Training

10.1 The Oregon TITAN Fusion Center will require the following individuals to participate in training regarding the implementation of and adherence to this Policy:

1. Personnel assigned to the Center;

2. Personnel providing information technology services to the Center;

3. Staff in other public agencies or private contractors providing services to the Center; and

4. Users who are not employed by the Center or a contractor.

10.2 The Oregon TITAN Fusion Center will provide special training regarding the Center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

10.3 The Training will cover:

1. The purpose of the Policy;

2. The substance and intent of the provisions of the Policy relating to the collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the Center;

3. The consequences of improper handling or use of information accessible within or through the Center; and

4. Penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

5. Originating and participating agency responsibilities and obligations under applicable law and policy.

6. How to implement the policy in the day-to-day work of the user, whether a paper or systems user.

7. The impact of improper activities associated with infractions within or through the agency.

8. Mechanisms for reporting violations of Center privacy protection policies and procedures.

10.4 Copies of the Policy will be made available in electronic and paper form to all individuals listed in section 10.1 above.

2555321-v1

APPENDIX A
Terms and Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The Oregon TITAN Fusion Center and all agencies that access, contribute, and share information in the Oregon TITAN's justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Refers to the Oregon TITAN Fusion Center and all participating state agencies of the Oregon TITAN Fusion Center.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality—Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information—Consists of information on the activities and associations of:

1. Individuals who:
    a. Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or
    b. Based upon reasonable suspicion, are suspected of being or having been involved in criminal activities with known or suspected crime figures.

2. Organizations, businesses, and groups which:
    a. Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or
    b. Based upon reasonable suspicion are suspected of being or having been illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.
    c. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.
Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information. Such data may comprise personally identifiable information.

Information Quality—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agency—Refers to any criminal law enforcement agency that enters into a Memorandum of Understanding with the Oregon TITAN Fusion Center and assigns personnel to work at the Center.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information or Data—Personal information refers to any information that relates to an identifiable individual (or data subject). Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information—One or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:
Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).
Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the Center will adhere to those legal requirements and Center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the Center, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Oregon constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to organizations by fusion Center policy or other state, local, or tribal agency policy or regulation.

Public ----- includes:

1. Any person and any for-profit or nonprofit entity, organization, or association;
2. Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
3. Media organizations; and
4. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.
    a. Public does not include:
5. Employees of the Oregon TITAN Fusion Center and participating agencies;
6. People or entities, private or governmental, who assist the Center and participating agencies; and
7. Public agencies whose authority to access information gathered and retained by the Center is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the Center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Repudiation—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland—by both the originator of the information and any recipient of the information.

Suspicious Activity—Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

User—An individual representing a participating agency who is authorized to access or receive and use a Center's information and intelligence databases and resources for lawful purposes.

Policy 3-101.5 Social Media Non-Covert Investigation Policy

Effective Date: *July 31, 2015*
Applicability: *All regular, temporary and volunteer employees*
References: *ORPC 4.2 and 4.3*

1. Non-Covert Investigative Use

Social media can be a valuable source of information for use in Department of Justice (DOJ) work. Such information can be used to, among other things, identify witnesses, locate witnesses, locate a party, gather information about a party's employment or assets, obtain admissions for use in litigation, gather information about expert witnesses, and discover evidence of a violation of a law.

This policy governs the acquisition and use of **public** information from social media websites through passive means for any DOJ-related purpose.

This policy does not address the acquisition of **non-public** information from social media sites. Although it may be legally and ethically permissible to obtain non-public information, such activities should be approached with caution and may only be undertaken with the prior approval of a Division Administrator or designee.

Further, this policy does not address the use, covert or otherwise, of social media for purposes of criminal investigations by the Criminal Justice Division.

This policy also does not address the use of social media sites to disseminate agency-related information to the public.

2. Public vs. Non-Public Information; Passive vs. Active Use

Personal pages on social media sites can be opened for viewing by the public or can have access restrictions. This will depend on the privacy settings chosen by each individual social media site user. Information that can be viewed on a social media site by every other user of that site is considered publicly available. Viewing such information does not require interaction with a user and is considered passive conduct.

In contrast, information on social media sites that can only be viewed with the permission of a user is considered private, or non-public, information. Accessing non-public information is considered active conduct and implicates a number of ethical and legal considerations. Such use is not permitted under this policy.

3. Passive Viewing of Information on Social Media Sites

Passive viewing of information on social media sites is permissible for DOJ employees. Authorization requires prior written approval of a supervisor (See paragraph 5 below). This includes social media sites that require logging into the site as a user in order to view other users' information. This policy does not authorize interacting with social media site users for

investigative purposes through the use of "tweets," "friending," or any other method except as described below in section 4.

4. Messaging

If it is not possible or practical to contact a site user in another way, it is permissible to send a message on a social media site asking the site user to contact an individual or office with DOJ with contact information. Every message sent to a site must clearly explain the reason the DOJ employee is trying to contact the user.

However, such contact raises potential ethical considerations. ORPC 4.2 prohibits a lawyer from contacting a social media site user who is represented by counsel. ORPC 4.3 provides that when contacting an unrepresented party a lawyer may not state or imply that the lawyer is disinterested. In addition, if a lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. Lastly, ORPC 5.3 provides that a lawyer having direct supervisory authority over a non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer. Consequently, these ethical concerns apply to non-lawyers contacting represented parties as well (e.g., Division of Child Support employees). Therefore, any message to a site user requesting contact information should include a statement making it clear that, if the site user is represented in the matter, the site user should request the site user/party's attorney to contact the DOJ.

5. Related Policy

This policy should be read in conjunction with DOJ Policy 3-101, which authorizes internet access if it is necessary to perform an assignment or if it is related to an activity that has been approved by DOJ. DOJ Policy 3-101(4)(i)(4) provides that work-related use of social media sites such as Myspace or Facebook requires prior written approval from a supervisor and the Administrative Services' Information Services Section (IS). Each Division shall establish a process for identifying the employees who will be authorized to access social media sites for DOJ work and enabling those employees to obtain written authorization using the DOJ *Authorization for Investigative Use of Social Media* form. See Appendix 3-101.5. **Social media site use authorized by this policy assumes an employee has obtained prior written approval.**

6. DOJ Computer Network Security

Accessing social media sites while logged onto the DOJ computer network may compromise network security. DOJ employees who are authorized to access social media sites must do so only from authorized DOJ devices (computers, laptops, smartphones, tablets, etc.) or through remote access into the DOJ network. Accessing DOJ-maintained social media sites accounts or accessing social media sites for DOJ purposes on personal devices without accessing the DOJ network is prohibited.

7. Personal Safety and Confidentiality

Social media sites should only be accessed using DOJ-created social media accounts. DOJ employees should not log into social media sites using personal accounts. Use of personal

accounts could compromise an employee's safety because of the potential to reveal personal identifying information. In addition, much of the work of the department involves confidential and sensitive matters. Conducting investigative work using personal accounts creates a substantial risk that such information may be improperly disclosed.

8. Use of Information from a User's Social Media Site Provided by a Party or Third Party

It is permissible for attorneys and non-attorney staff to use information obtained independently by third parties from a social media site provided it was legally obtained. The value and admissibility of such information may be questionable if the method of acquisition cannot be verified. The best practice would be to require the party or third party to demonstrate, using a computer, how the information was obtained.

This page intentionally left blank

Ellen F. Rosenblum
Attorney General

FUSION CENTER PROCEDURE
Threat Assessments / Risk & Vulnerability Assessments
September 18, 2015

DEFINITIONS:

1. Threat Assessment: Process of identifying or evaluating entities or events for indications of potential harm to life, property, operations or information. These assessments involve investigative research which results in a written product identifying possible threats to a specific person or incident. Examples include Pendleton Round-up, Hillsboro Air Show or Governor's Inauguration. Threat assessments may be conducted by an individual analyst or team of analysts based on the complexity of the assessment.

2. Risk & Vulnerability Assessment: Physical appraisal or process which collects information and assigns values to risks facing an entity, asset, system, network or geographic area. These assessments involve a physical inspection and investigative research for the purpose of evaluating an assets ability to react and recover from a man-made or natural attack or event. Risk and Vulnerability assessments will be conducted using a team approach and not by a single analyst.

3. ASAC: Refers to the Assistant Special Agent-in-Charge, assigned by the Oregon Department of Justice, Criminal Justice Division, to manage the Oregon TITAN Fusion Center.

4. RA-3: Refers to a Research Analyst 3 employed by the Oregon Department of Justice, Criminal Division assigned to the Oregon TITAN Fusion Center.

5. OPA: Refers to an Operations and Policy Analyst employed by the Oregon Department of Justice, Criminal Division assigned to the Oregon TITAN Fusion Center.

6. OTFC: Refers to the Oregon TITAN Fusion Center.

7. DHS: United States Department of Homeland Security.

8. PCII: Protected Critical Infrastructure Information.

PROCEDURES:

- The ASAC will be given any request for a Threat or Risk & Vulnerability Assessment received by the OTFC. The request should include the name and phone number of the requester, and any other pertinent information for review.
- Once reviewed, the assessment will be entered in the "Assessment Log" by the ASAC and a tracking number will be issued.
- For a Threat Assessment, the ASAC will assign an OPA/RA-3 and, based on the event, a timeline for completion will be assigned. It will be the responsibility of the OPA/RA-3 to reach out to the requester to assist in completing the threat assessment. Once the Threat Assessment is completed it will be given to the ASAC for review. Once approved, the product can go out to the requester.
    - The Threat assessment will be written as an unclassified FOUO document unless specified otherwise.
    - The document will include the following sections:
        - Historical Information (date, time, location etc.)
        - Key Judgements
        - Potential Threats
        - Summary
        - Recommendations
        - Other sections as deemed appropriate (See appendix A for "go by.")
- For a Risk & Vulnerability Assessment, the ASAC will assign an OPA/RA-3 as the team leader for this event. The team leader will contact the asset manager and determine a date/time for the physical assessment. The team leader will evaluate the number of personnel needed and these personnel will be assigned by the ASAC. The written product will be the responsibility of the team leader and will be approved by the ASAC prior to distribution. Once the date/time for the physical assessment has been established, a timeline for completion will be given. This timeline will include date for a draft of the written assessment to be completed, date for completion of the project and date for the product to be presented to the asset manager.
    - Risk & Vulnerabilities products will be maintained in a locking cabinet in the CIKR area. Any assessment deemed to be PCII will fall under DHS established directives.
    - The format for the Risk & Vulnerability assessment will include an executive summary and the Risk and Vulnerability worksheet (See appendix B).

Oregon TITAN/ Fusion Center Policy Regarding First Amendment Protected Events

I. Purpose of policy

As articulated in the United States Constitution, one of the freedoms guaranteed by the First Amendment is the right of persons and groups to peaceably assemble. Persons and groups engaging in First Amendment related activities have the right to:

1. Organize and participate in peaceful assemblies, including demonstrations, rallies, parades, marches, picket lines, or other similar gatherings.
2. Conduct assemblies/gatherings in public places.
3. Express their political, social, or religious views in a peaceful assembly.
4. Freely associate with other persons and collectively express, pursue, promote, and defend common interests.

Furthermore, Oregon law provides that no law enforcement agency may collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

Law enforcement officers, in turn, must ensure the safety of the general public while protecting the privacy and rights of persons practicing their First Amendment right to assemble peacefully. To support officers as they fulfill these responsibilities, the Oregon TITAN/Fusion Center and the Oregon Department of Justice Criminal Intelligence Unit (the Center) provide assessment and situational awareness review of First Amendment protected events.

The purpose of this policy is to provide guidelines for the Center so that situational assessment and review of First Amendment protected events are in accordance with federal and Oregon law.

II. Information Screening and Review

A. The Center may review event information in order to assess the potential impact of the event on public safety. Such information will not be collected or maintained unless in compliance with ORS 181.575.

The Center shall only review event information from the following sources:

1. Event permit requests filed with a government body.
2. The media.

3. Information published in any publicly accessible forum by event organizers or participants.
4. Direct statements made by event organizers or participants to any law enforcement officers or the CIU.
5. Investigations **if** the subject of the investigation satisfies ORS 181.575.

B. A review of information from the above listed sources does not constitute information "collection" under ORS 181.575. No criminal intelligence file shall be created with such information and no storage or maintenance of the information reviewed shall occur unless in compliance with ORS 181.575, the Center's Privacy Policy, and all other applicable Oregon and federal law.
C. Information reviewed for this purpose must first satisfy the Information Input requirements of OAR 137-090-0090 and the Oregon TITAN/Fusion Center Privacy Policy 4.1 (1) which requires the CIU to first determine if the information to be reviewed is relevant, reliable and valid and relates to a possible threat to public safety or the enforcement of the criminal law.
D. Information reviewed shall be purged from all Center systems within 30 days unless the information warrants being maintained pursuant to ORS 181.575.

III. Obtaining Information

Permissible Means of obtaining information

1. The Center may communicate openly and directly with any person involved in a public gathering regarding the number of persons expected to participate and similar information regarding the time, place, route, and manner of a public gathering and review documents submitted for such purpose, such as parade permit applications.
2. The Center may review publicly accessible information posted or published by the event organizers, sponsor organizations, or self-admitted participants.
3. The Center may review publically accessible media articles about the event, event organizers or participants.
4. The Center may collect any information, including from investigations, about a person or group who have indicated an intention to attend **and** who are known to be or reasonably suspected of engaging in violence or other unlawful acts in order to determine whether they are inciting or planning violence or other unlawful activities at this event. Information collected for this purpose must be accompanied by a statement which specifically articulates the unlawful activity related to the person or group and the specific basis of suspicion of violence or criminal activity.

IV. Prohibited Conduct Relating to First Amendment Protected Events

1. Investigating and collecting, maintaining, using, or sharing information regarding persons or groups **solely because they are involved in constitutionally protected activity**.
2. Investigating and collecting, maintaining, using, or sharing information regarding persons or groups **solely because of the content of their speech**.
3. Investigating and collecting, maintaining, using, or sharing information regarding persons or groups' exercise of their First Amendment rights **for a purpose unrelated to the event**.
4. Instructing the debriefing of or questioning witnesses, event participants, or arrestees regarding their social, political, or religious views unless specifically related to criminal conduct and then only as necessary to achieve the clearly stated objective of protecting the public or law enforcement personnel.

V. Sharing Information

A. Information reviewed under this section may be shared as situational awareness for law enforcement to aid them in their public safety duties as set forth in this policy. No criminal intelligence information may be shared unless such information otherwise meets the requirements of The Center's Privacy Policy for information sharing (Section7), as well as all applicable Oregon and Federal law.

B. All Center Bulletins and Situational Awareness publications shall not be disseminated until reviewed and approved by one of the following: the Center's legal advisor; DOJ CJD Chief Counsel; or DOJ CJD Deputy Chief Counsel.

C. Once a review of the relevant information is complete, The Center shall determine whether it should provide its findings to agencies outside The Center. This determination should be based on a criminal predicate (pursuant to ORS 181.575) or other law enforcement purpose to justify sharing of information, including:
   1. The size of the event (is it multijurisdictional).
   2. Reasonable law enforcement purpose related to persons or groups associated with the event planning to engage in criminal activity in connection with the event or who have engaged in criminal activity during past events.
   3. Whether the event will also take place in another jurisdiction.
   4. Public safety impact on roads, hospitals or law enforcement resources.
   5. A reasonable likelihood of violence between event participants and law enforcement, other citizens or other groups likely to be present near the event.

VI. Required Warnings and Reminders – Bulletin Contents

Situational Awareness bulletins shall also contain the following reminders to law enforcement:

1. That the purpose of the Situational Awareness bulletin is the aid law enforcement in the protecting of life and property.

2. That Officers responding to First Amendment Protected events should ensure that all privacy, civil rights, and civil liberties protections are upheld in the performance of their duties.
3. That officers responding to First Amendment Protected events should practice fair and impartial enforcement of laws, statutes, and ordinances.

VII. Information Collection and Maintenance

Information shall not be collected, maintained, stored or entered into a criminal intelligence file unless it meets all the requirements of ORS 181.575, the Center's Privacy Policy and all applicable Oregon and federal law.

ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
CRIMINAL JUSTICE DIVISION

10/01/2015

Memorandum To: Dave Kirby, SAC

Memorandum From: [redacted] Special Agent

Reference: Possible threats towards law enforcement by DOJ employee

Sir,

On September 30, 2015, at approximately 7:00 a.m., I was utilizing a demo program entitled, "Digital Stakeout" during a product test period. This program takes user inputted keywords and searches multiple open source social media sites.

Due to increased threats towards law enforcement, I used a hashtag search for, "fuckthepolice," and "blacklivesmatter," which are keywords and hashtags known for posting threats towards law enforcement. I narrowed the search by using "Salem, Oregon" as a location. I have also used search terms such as, "Volksfront," "White power," "OMG," and, "Hells Angels" during my initial use of the program. I received numerous returns, and clicked on a feature entitled, "Collage" which shows pictures posted to social media based on my search terms.

Scrolling through the returns, I observed numerous anti police posts and pictures posted by the same user on Twitter. Following the link for the user, I was taken to an unprotected Twitter account. An unprotected Twitter account allows all postings to be viewed by any person with internet access. The account name was "Erious J., Jr," with a Twitter handle of "@EriousEsq." I believe, based upon my observation of the account, the owner and poster of Tweets to this account is an attorney within the Oregon Department of Justice.

The attached is a printed copy of the contents on the open Twitter account. They are for your review, and they can also be viewed on the Twitter website. Feel free to contact me with any further questions you may have.

[redacted]
Criminal Investigator
Oregon Department of Justice

TWEETS 590 | FOLLOWING 58 | FOLLOWERS 58 | FAVORITES 2

Follow

Erious J., Jr.
@ErIousEsq

Strictly an Observer

Salem, OR

Joined June 2012

New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

You may also like · Refresh

Nkenge
@TrueNkenge

Rukaiyah
@RukaiyahAdams

Driving While Black
@DWB_TheApp

SuzB24
@SuzB24

Mariann Hyland
@HylandMariann

Trends

#TravelForGood
Promoted by Travelocity
#PodcastDay
Kim Davis
#RuinAnAnimatedMovie
#TheList
#WakeUpTris
Music To Watch Boys
#ALDUB11thWeeksary
Tony Stewart
iOS 9.0.2
Astana

Home About

Search Twitter

Have an account? Log in

Tweets Tweets & replies Photos & videos

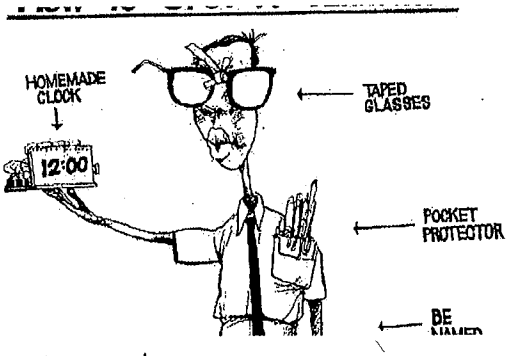
Erious J., Jr. @EriousEsq · Sep 26
It takes a nation of millions...#BMAInitiative @ulpdx #blacklivesmatter

1 3

Erious J., Jr. @EriousEsq · Sep 26
The Leaders of tomorrow!! The Black Male Achievement initiative's Summer Youth Experience..#BMAInitiative #pdx @ulpdx

4 2

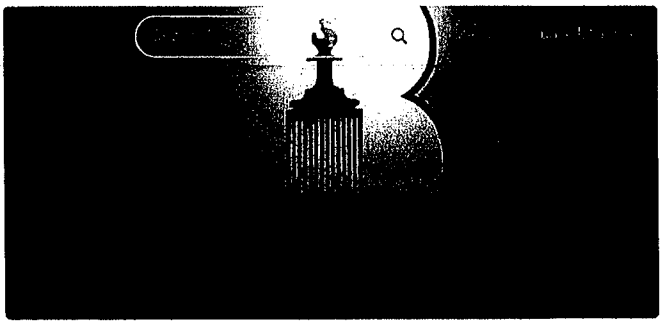
Erious J., Jr. @EriousEsq · Sep 17
If I was old, they'd probably be a friend to me. But since I'm young, they consider me the enemy: #IStandWithAhmed



1 1

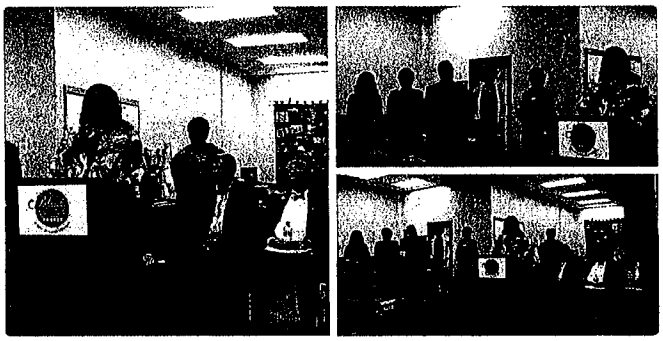
Erious J., Jr. @EriousEsq · Aug 25
WOULDN'T YOU KNOW...NOT ONE BLACK PERSON EITHER WORKING OR PATRONIZING THE PLACE. #culturalappropriation #pdx

Home About



Erlous J., Jr. @EriousEsq · Aug 24
Nice artwork @theknowbar #Portland Three cheers for gentrification...

Erlous J., Jr. @EriousEsq · Aug 11
My boo, President & CEO, doing her thing!! #ulpdx @ulpdx @truenekenge #mealsonwheels #portland



1

Erlous J., Jr. @EriousEsq · Aug 1
Fight the power #travonmartin #saveourcities #blacklivesmatter #alivewhileblack

Home About

1

Erious J., Jr. @EriousEsq · Jul 31

#SaveOurCities at the 2015 @NatUrbanLeague Annual Conference!

2

Erious J., Jr. @EriousEsq · Jul 29

A Queen on yet another throne..@TrueNkenge #SaveOurCities

1

Erious J., Jr. @EriousEsq · Jul 29

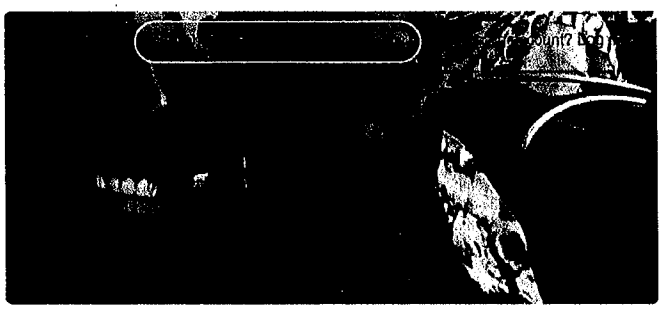
My Boo...CEO & Pres. of the @ULPDX in da HOUSE!! #SaveOurCities

1

Erious J., Jr. @EriousEsq · Jul 29

At the Leadership Luncheon #SaveOurCities @TrueNkenge

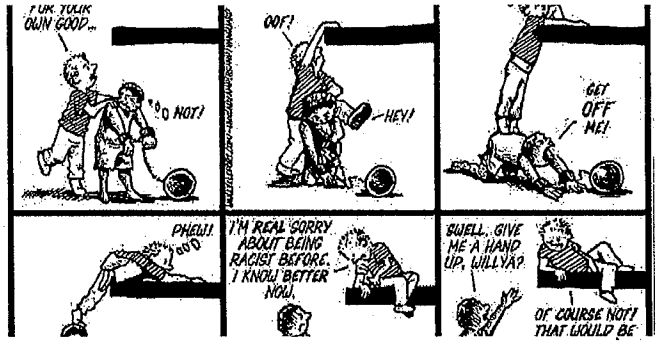
Home About



1 2

Erious J., Jr. @EriousEsq · Jul 23

In a nutshell #blacklivesmatter #alivewhileblack #growingupblack



18 13

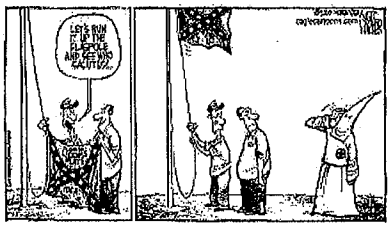
Erious J., Jr. @EriousEsq · Jun 24

AMERICA...#blacklivesmatter #alivewhileblack

1 3

Erious J., Jr. @EriousEsq · Jun 24

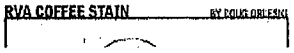
BLESS...#blacklivesmatter #ALIVEWHILEBLACK



1 2

Erious J., Jr. @EriousEsq · Jun 24

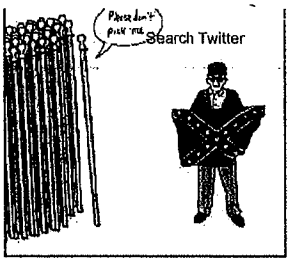
GOD...#blacklivesmatter #alivewhileblack



Home About

Search Twitter

Have an account? Log in



1

Erious J., Jr. @EriousEsq · Jun 24

Dont mind company...just call first..#germanshepherd #watchdog

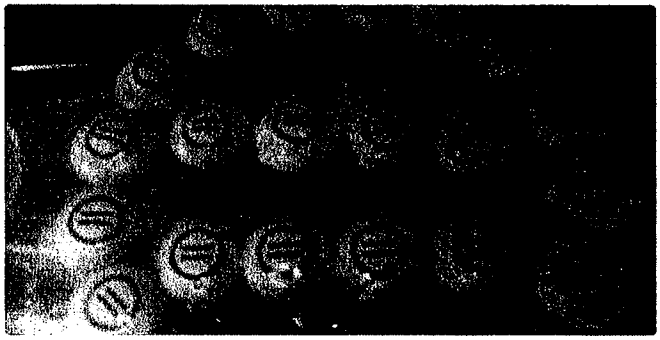
Erious J., Jr. @EriousEsq · Jun 24

Save the world or not, yard work still gotta get done @ULPDX #DIY

1

Erious J., Jr. @EriousEsq · Jun 24

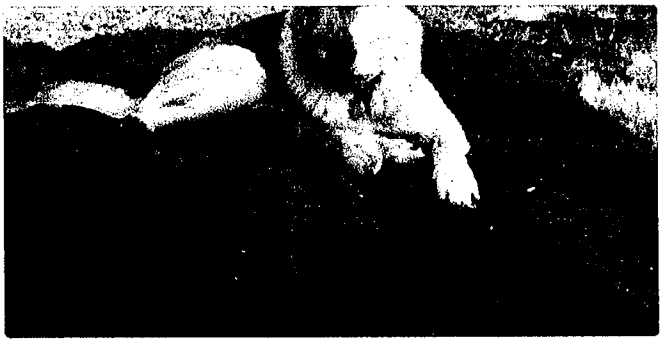
Urban League SWEET! @ULPDX



Home About

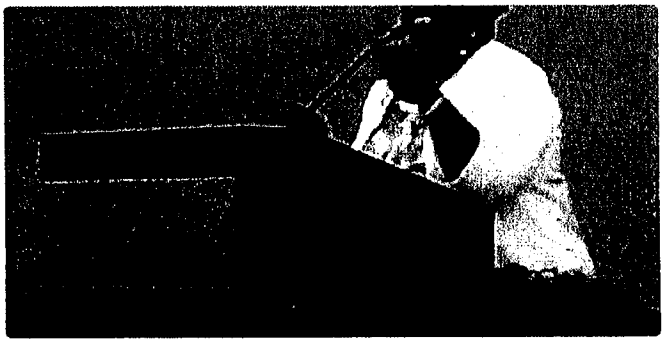
1 2 Search Twitter Have an account? Log in

Erious J., Jr. @EriousEsq · Jun 24
My Zenobia...Princess of the mountain #germanshepherd



Erious J., Jr. @EriousEsq · Jun 22
Gangster by association. ..American that is. Won my trial later that day...@sonnench

Erious J., Jr. @EriousEsq · Apr 16
Sharon Gary Smith Inspiring the masses at REAP's Legacy Luncheon. #spreadlegacy



1 1

Erious J., Jr. @EriousEsq · Apr 14
A proud Blackman and the proud Blackman that raised him. #blackfathers #Blackman #blackfatherhood

Home About

3 1

Erious J., Jr. @EriousEsq · Apr 12
#alivewhileblack #blacklivesmatter #ferguson #policebrutality #walterscott

Erious J., Jr. @EriousEsq · Apr 3
#blacklivesmatter #alivewhileblack #dwb @chrisrock

Erious J., Jr. @EriousEsq · Apr 3
@Chrisrock #blacklivesmatter #alivewhileblack

Erious J., Jr. @EriousEsq · Mar 27

Home About

Search Twitter

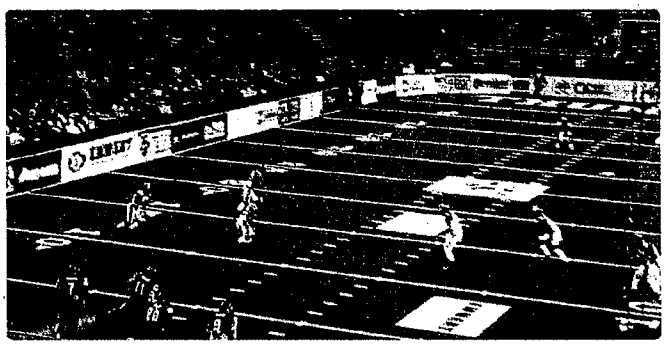
Have an account? Log in

I am here...i am here...@PDXTHUNDER #AARONROCKS sec. 207, row E, seats 7 & 8. come see me.

1

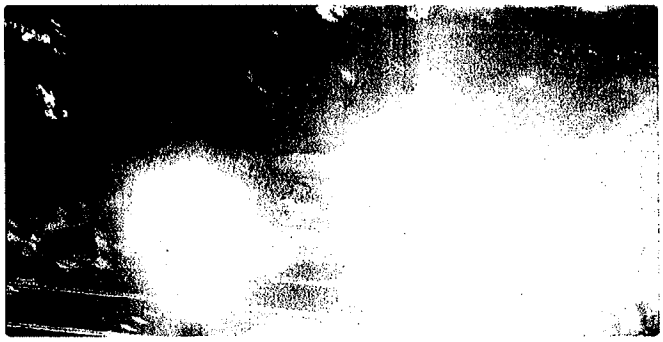
Erious J., Jr. @EriousEsq · Mar 27

BOOM ! Love sending the D out first!!



Erious J., Jr. @EriousEsq · Mar 27

Cant have a BOOM without Fire!! @PDXTHUNDER



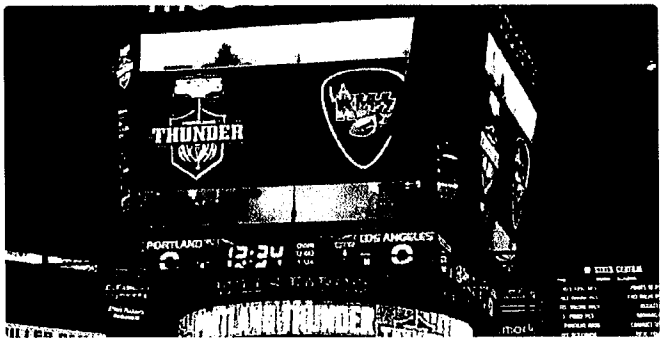
1 2

Erious J., Jr. @EriousEsq · Mar 27

Now that was a SICK intro!!! @PDXTHUNDER

Home About

Erious J., Jr. @EriousEsq · Mar 27
Wanted a team to root for...might as well be the @PDXTHUNDER



Erious J., Jr. @EriousEsq · Mar 21
Im waiting....#DIY #SalemOr #homestead

Erious J., Jr. @EriousEsq · Mar 21
But can your wife do this? #DIY #SalemOr #homestead

Erious J., Jr. @EriousEsq · Mar 15
Look at my Brownie DIY'n it! #did #salemor

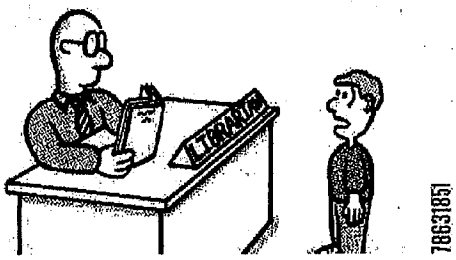
Home About

Erious J., Jr. @EriousEsq · Mar 11
Why be Green. Its hard enough being Black. #HBCUVPWI #alivewhileblack #SAE

Erious J., Jr. @EriousEsq · Mar 11
Mrs. Harmon Johnson rocking her FAMUnique stylie...or is it styzzle? @TrueNkenge #FAM #HBCUpride

★ 2

Erious J., Jr. @EriousEsq · Feb 7
Get it!? #blackhistorymonth #blacklivesmatter #alivewhileblack



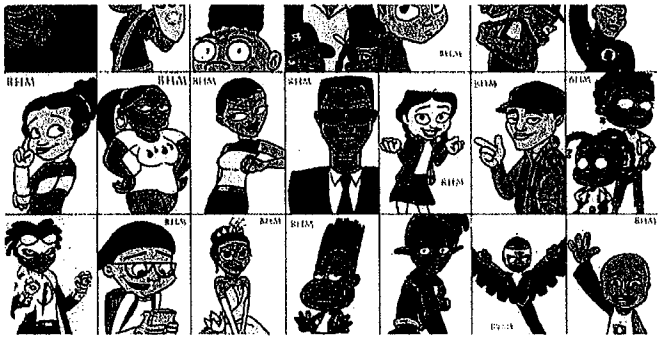
78631851

Erious J., Jr. @EriousEsq · Feb 7
#blackhistorymonth #blacklivesmatter #alivewhileblack

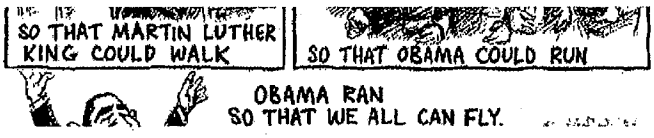
10 8

Erious J., Jr. @EriousEsq · Feb 7
#blacklivesmatter #alivewhileblack #blackhistorymonth

Erious J., Jr. @EriousEsq · Feb 7
#blacklivesmatter #alivewhileblack #blackhistorymonth

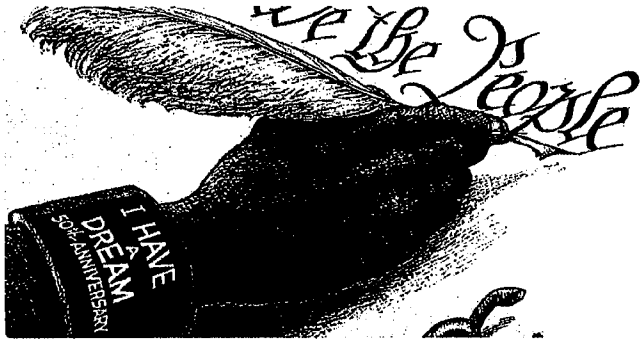


Erious J., Jr. @EriousEsq · Feb 7
#blackhistorymonth #blacklivesmatter #alivewhileblack

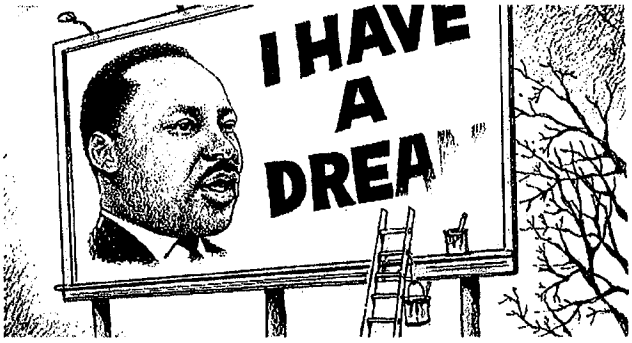


Home About

Erlous J., Jr. @ErlousEsq · Jan 19
In order to form a more perfect UNION...#MartinLutherKingDay #alivewhileblack #BlackLivesMatter



Erlous J., Jr. @ErlousEsq · Jan 19
History belongs to the victors...#blacklivesmatter #MartinLutherKingDay #alivewhileblack

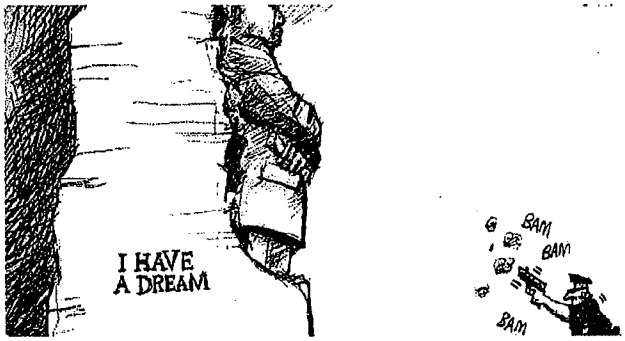


Erlous J., Jr. @ErlousEsq · Jan 19
All in 2gether now..#MartinLutherKingDay #alivewhileblack #BlackLivesMatter

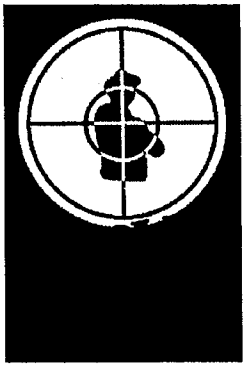
Home About

Search Twitter Have an account? Log in

Erious J., Jr. @EriousEsq · Jan 19
Some things will never change..#blacklivesmatter #MartinLutherKingDay #alivewhileblack



Erious J., Jr. @EriousEsq · Jan 19
Consider yourselves...WARNED!!!



4:18 PM - 19 Jan 2015 · Details

Erious J., Jr. @EriousEsq · Jan 1
Heres to change, hope and evolution. HAPPY NEW YEAR!! #blacklivesmatter #ALIVEWHILEBLACK #racisminamerica

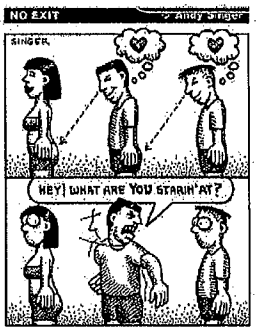
Erious J., Jr. @EriousEsq · Dec 26

Home About

Search Twitter

Have an account? Log in

If its good for the gander...#equality #womenslivesmatter

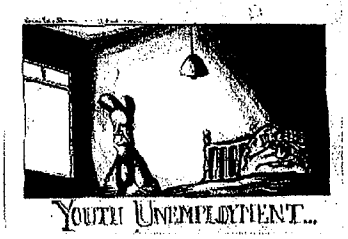


Erious J., Jr. @EriousEsq · Dec 25

Merry Christmas y'all. #MerryChristmas

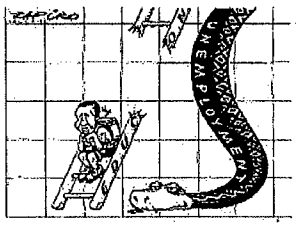
Erious J., Jr. @EriousEsq · Dec 23

#education #employment4all #blacklivesmatter #blackness



Erious J., Jr. @EriousEsq · Dec 23

#blacklivesmatter #alivewhileblack #education #equality4all



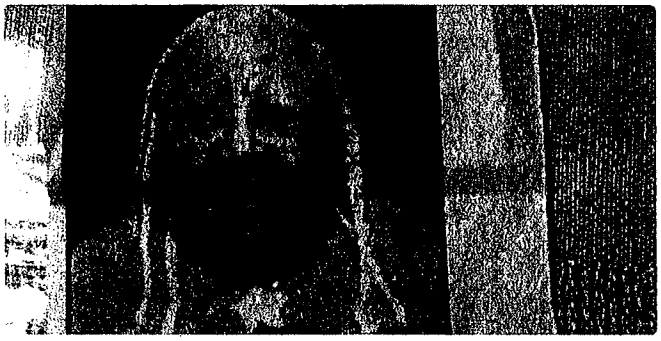
1

Erious J., Jr. @EriousEsq · Dec 23

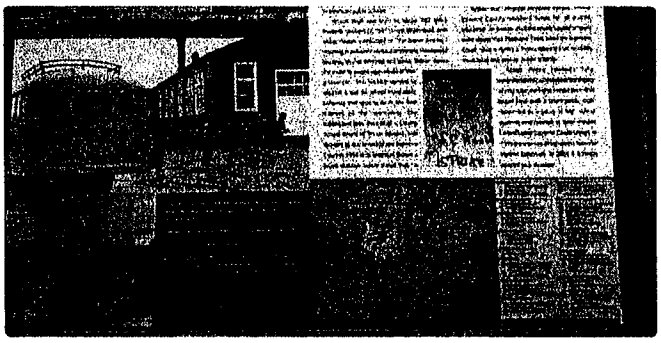
Who says E aint bout the holidays?

Home About

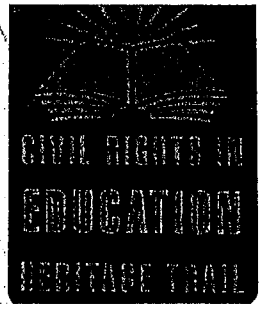
Erious J., Jr. @EriousEsq · Dec 23
My grandma. Hope it runs in the family.



Erious J., Jr. @EriousEsq · Dec 23
A brief history of education and civil rights in Farmville, Va.
#civilrights #alivewhileblack #Equality4All



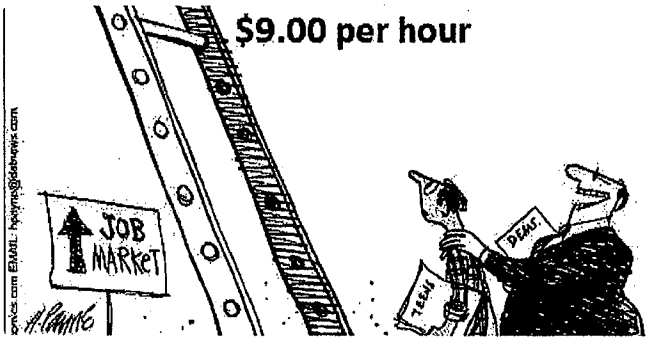
Erious J., Jr. @EriousEsq · Dec 23
First stop, Farmville, Va. #civilrights



Home About

Search Twitter Have an account? Log in

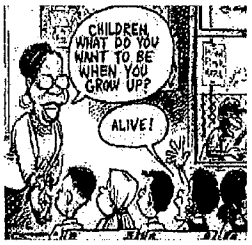
Erious J., Jr. @EriousEsq · Dec 23
No words for this one..



Erious J., Jr. @EriousEsq · Dec 23
Give us free..

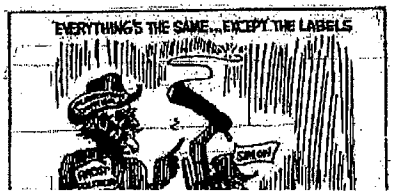
1

Erious J., Jr. @EriousEsq · Dec 23
Never thought I'd see 21. Look I'm grown now....



1

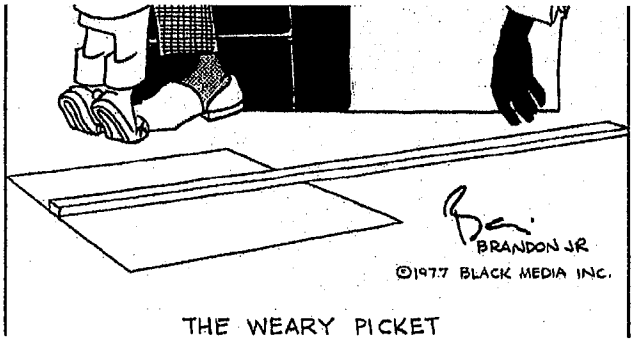
Erious J., Jr. @EriousEsq · Dec 22
You gotta read the label..if you dont, you might get poisoned.
#blacklivesmatter #alivewhileblack #blackness



Home About

Have an account? Log in

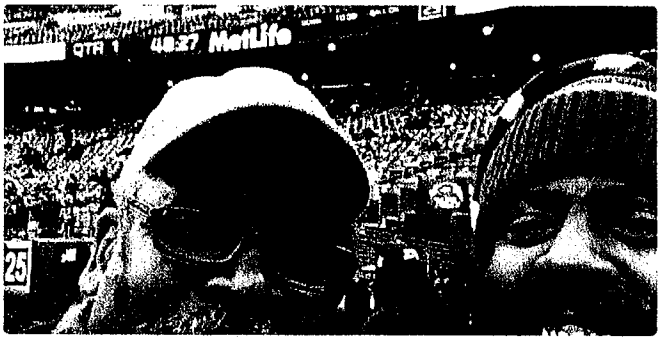
Erious J., Jr. @EriousEsq · Dec 22
Well...did we?! #blacklivesmatter #alivewhileblack #blackness #civilrights



★ 2

Erious J., Jr. @EriousEsq · Dec 21
He's flawed but he's OURS!! #NYJvsNE #nyjets

Erious J., Jr. @EriousEsq · Dec 21
Me and my Pops..J! E! T! S! JETS! JETS! JETS! #nyjets #NYJvsNE



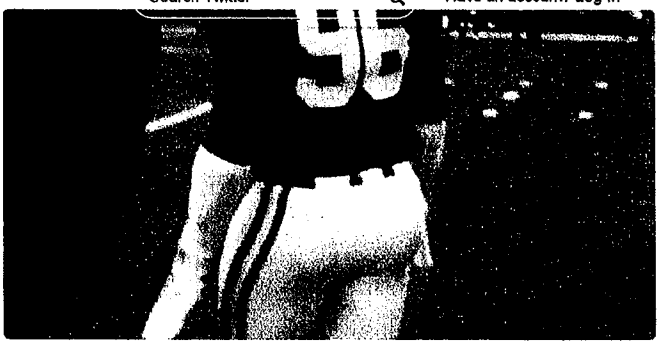
★ 1

Erious J., Jr. @EriousEsq · Dec 21

Home About

Search Twitter Have an account? Log in

The only Jet worth tweeting! #nyjets

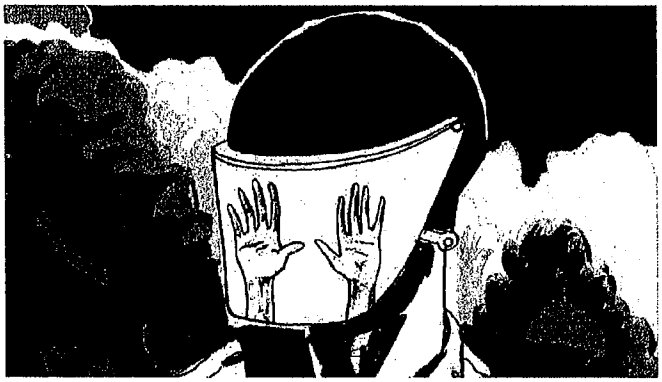


Erious J., Jr. @EriousEsq · Dec 21

On the MetLife field with my POPS! #nyjets

Erious J., Jr. @EriousEsq · Dec 18

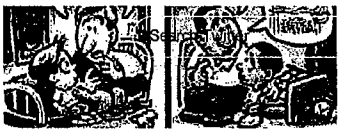
#alivewhileblack #blacklivesmatter #ferguson #michaelbrown



5:37 PM - 18 Dec 2014 · Details

Erious J., Jr. @EriousEsq · Dec 18

#blacklivesmatter #alivewhileblack



2 1

Erious J., Jr. @EriousEsq · Dec 18
#alivewhileblack #blacklivesmatter #alwaysremember #neverforget

Erious J., Jr. @EriousEsq · Dec 14
Mountaintops anyone? #AffirmativeAction #AliveWhileBlack #BlackLivesMatter #blackness

1:55 PM - 14 Dec 2014 · Details

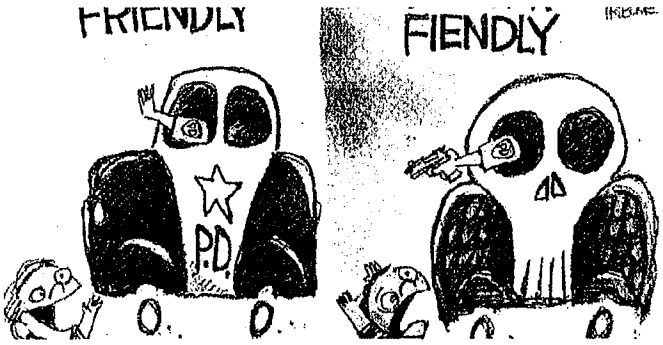
Erious J., Jr. @EriousEsq · Dec 14
Never looked at it this way. #AffirmativeAction #blackness #AliveWhileBlack #AliveWhileBlack

Home About

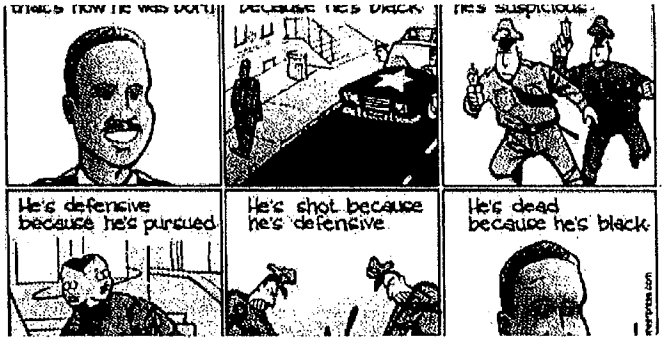
Erious J., Jr. @EriousEsq · Dec 14
This one is for nostalgia's sake. #BlackLivesMatter #racism #lynching #AliveWhileBlack

2 5

Erious J., Jr. @EriousEsq · Dec 14
Fiends....How may of us have them ...#AliveWhileBlack #racism #BlackLivesMatter #PoliceBrutality



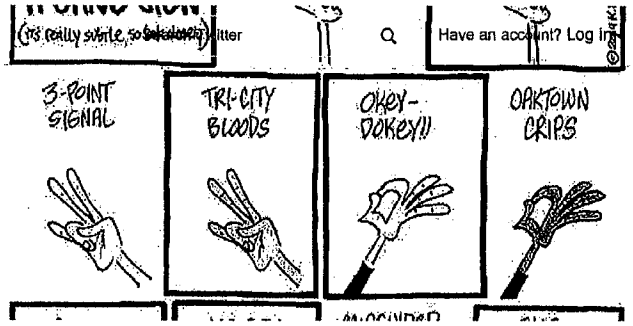
Erious J., Jr. @EriousEsq · Dec 14
If A equals B. And B equals C. A MUST equal C. #BlackLivesMatter #AliveWhileBlack #noindictment #PoliceBrutality



2 3

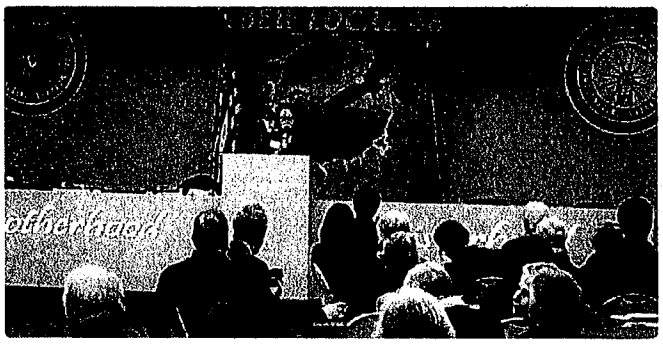
Erious J., Jr. @EriousEsq · Dec 13
Get it?! #alivewhileblack #blacklivesmatter

Home About



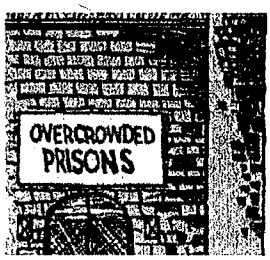
★ 1

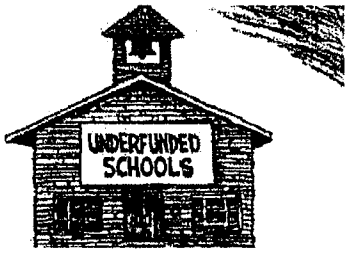
Erious J., Jr. @EriousEsq · Dec 13
Watching my boss, AG Ellen Rosenblum, rally thr Dems!



Erious J., Jr. @EriousEsq · Dec 13
My Sensei addressing the troops before feeding the homeless in Salem. #livegenerously

Erious J., Jr. @EriousEsq · Dec 11
#schoolproblems #discipline #prisonpipeline #AliveWhileBlack #BlackLivesMatter

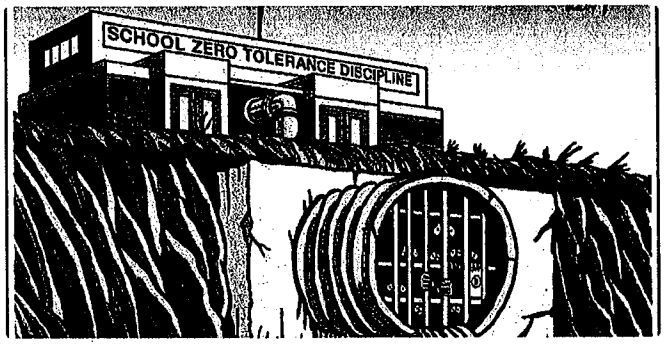




Home About

1

Erious J., Jr. @EriousEsq · Dec 11
#AliveWhileBlack #education #PrisonReform #educolor #RacismIsReal #prisonpipeline



4 2

Erious J., Jr. @EriousEsq · Dec 11
Portland is over the rainbow!!

1

Erious J., Jr. @EriousEsq · Dec 10
One of the reasons I love The Punisher: He's down with the Brown! #Superhero #nerdsrule #Marvel

Erious J., Jr. @EriousEsq · Dec 10

Home About

Search Twitter Have an account? Log in

#noindictment #AkaiGurley #EricGarner #MichaelBrown #TrayvonMartin #AliveWhileBlack #BlackLivesMatter

4 2

Erious J., Jr. @EriousEsq · Dec 9
#TamirRice #AliveWhileBlack #BlackLivesMatter

1

Erious J., Jr. @EriousEsq · Dec 9
#TamirRice #AliveWhileBlack #BlackLivesMatter

Erious J., Jr. @EriousEsq · Dec 8
Just so ya'll know. We are SUPER! Top Ten Black Superheroes: youtu.be/nwAkpD2sK28 via @YouTube

Erious J., Jr. @EriousEsq · Dec 8
Gone but not forgotten. #AliveWhileBlack #BlackLivesMatter #EricGarner #trayvonmartin #noindictment

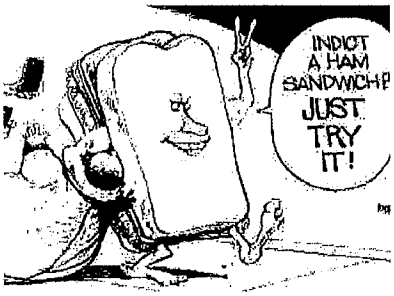
1

Erious J., Jr. @EriousEsq · Dec 8
Post Apocalypticism at its finest! Mad Max: Fury Road - Comic-Con First Look [HD]: youtu.be/akX3Is3qBpw via @YouTube

Erious J., Jr. @EriousEsq · Dec 8
@OrangemanMal29: this is what chicken and dumplings looks like playa. #blackmendocook

Home About

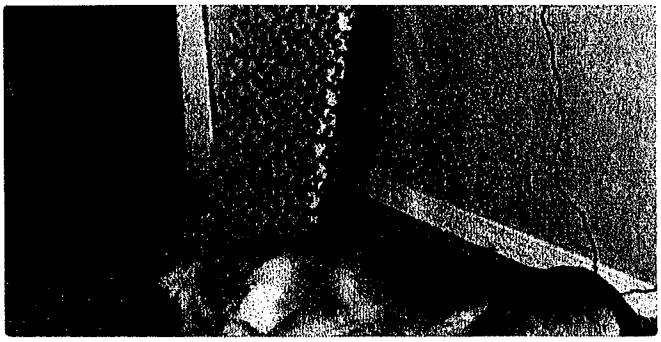
Erious J., Jr. @EriousEsq · Dec 8
#EricGarner #MichaelBrown #AliveWhileBlack #RacismInAmerica



Erious J., Jr. @EriousEsq · Dec 7
#RacismInAmerica #NativeLivesMatter #Redskins

4 2

Erious J., Jr. @EriousEsq · Dec 7
The calm before the storm.



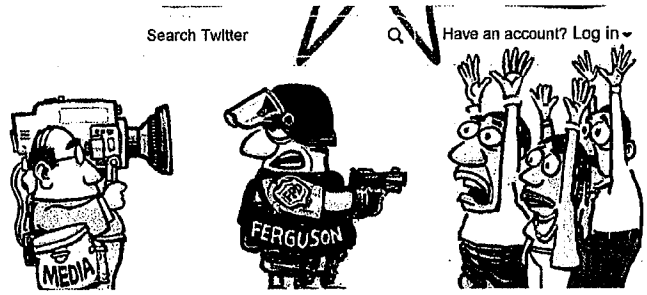
1

Erious J., Jr. @EriousEsq · Dec 4
#MikeBrown #FergusonDecision #NoJusticeNoPeace #NoIndictment

Home About

Search Twitter

Have an account? Log in



Erious J., Jr. @EriousEsq · Dec 4

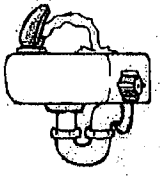
For my fellow geeks

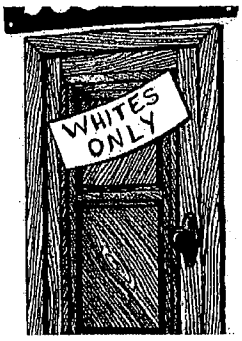
Erious J., Jr. @EriousEsq · Dec 4

While on the theme of justice...

Erious J., Jr. @EriousEsq · Dec 4

Hey..we do have a black president though.





Walker, Carolyn

From: Kirby David <david.kirby@doj.state.or.us>
Sent: Friday, November 13, 2015 9:49 PM
To: Tweedt Darin E
Subject: FW: Erious Johnson

Follow Up Flag: Follow up
Flag Status: Flagged

Here's the string

From: Tweedt Darin E
Sent: Thursday, October 08, 2015 3:57 PM
To: Tuttle Stephanie J
Cc: Kirby David
Subject: Re: Erious Johnson

Thanks.

Sent from a mobile device.

On Oct 8, 2015, at 12:21 PM, Tuttle Stephanie J <stephanie.j.tuttle@doj.state.or.us> wrote:

> Darin, I put it on your chair.
>
> Stephanie J. Tuttle
> Oregon Department of Justice
> 503.378.6347
>
> ---
>
> **From:** Tweedt Darin E
> **Sent:** Thursday, October 08, 2015 2:38 PM
> **To:** Kirby David
> **Cc:** Tuttle Stephanie J
> **Subject:** Re: Erious Johnson
>
> Thanks. I'll review next week.
>
> That posting was the logo for the rap group Public Enemy.
>
> Sent from a mobile device.
>
> On Oct 8, 2015, at 11:20 AM, Kirby David <david.kirby@doj.state.or.us> wrote:
>
> > Hello to you – most of the information is benign, but the one that bothers me is his post on January 19th where there is a police officer in rifle scope crosshairs with the caption 'PUBLIC ENEMY' and he says "Consider yourselves WARNED".

The packet was too big to send – Steph, I'm gonna put it in your office and then have you pass it along to Darin as I'm out of the office tomorrow.....

David Kirby
Special Agent in Charge | Criminal Justice Division
Oregon Department of Justice
2250 McGilchrist St. SE, Ste. 100
503.378.6347

EXHIBIT G
Page 2 of 2

Walker, Carolyn

From: McIntosh Steven <steven.mcintosh@doj.state.or.us>
Sent: Thursday, November 12, 2015 11:24 AM
To: [redacted]
Cc: Tweedt Darin E
Subject: Social Media Monitoring

Follow Up Flag: Follow up
Flag Status: Flagged

Effectively immediately all employees are to cease using any social media monitoring tool, and do not delete any saved searches off of your computer or software until further notice.

Steven McIntosh
Assistant Special Agent-in-Charge
Oregon Department of Justice | Criminal Justice Division
2250 McGilchrist St. SE, Suite 100
Salem, OR 97302
Office: 503-934-2034

EXHIBIT H
Page 1 of 1

Walker, Carolyn

From: Kirby David <david.kirby@doj.state.or.us>
Sent: Tuesday, November 17, 2015 1:50 PM
To: Umscheid Lisa M
Subject: FW: Social Media Tool Search Terms.

Follow Up Flag: Follow up
Flag Status: Flagged

From: McIntosh Steven
Sent: Monday, November 09, 2015 3:47 PM
To: Tweedt Darin E; Kirby David; Tuttle Stephanie J
Cc: 'McIntosh Steven'
Subject: Social Media Tool Search Terms.

Below is the response from my peeps regarding search terms used in the Social Media Monitoring tool. These are not all, but the ones that could be remembered.

Search Terms:

[redacted] Omg, mongolsmc, gjmc, 1%, blacklivesmatter, blackbloc, kkk, neonazi, whitesupremecy, whitepride, ISIS, ISIL, uccshooting, ucc, odoj, bomb, shoot, sickofschool, ymca, oregonstatecapital, salem government offices, mongolsnw, outlawsmc, Deckenlou, Free souls, Freesoulsmc, Hells Angels, oregonha, support81, lafferty, Julie senn, roadbrothersmc, roadbrotherssalem, vrooman, [redacted] nla, [redacted] marion county courthouse, marion county jail, threepercenters, blm, Tango Blast, anonymous, Coosbayschools, Sprague, Salem schools, Judsonms, SSHS, BCS, Crosslerms, CHS, CentralHS, Umpqua Shooting.

Steven McIntosh
Assistant Special Agent-in-Charge
Oregon Department of Justice | Criminal Justice Division
2250 McGilchrist St. SE, Suite 100
Salem, OR 97302
Office: 503-934-2034

EXHIBIT I
Page 1 of 1

Walker, Carolyn

From: [redacted]
Sent: Thursday, December 17, 2015 2:43 PM
To: Walker, Carolyn
Cc: Ederer Joseph E
Subject: Investigation

Ms. Walker, you asked in my interview on 12/15/15 if I had ever searched #blacklivesmatter. I did not think that I had and answered no at the time.

There was another hash tag that was circulating amongst fusion centers around the end of the summer, beginning of Sept. That hashtag was #FYF911. Unfortunately, I didn't realize that that hashtag was linked with #blacklivesmatter. At the time, the hashtag of #FYF911 was believed to be a threat to law enforcement and the general public. This information went out from the fusion center on 9/10/15.

I know that September was only three months ago, but I distribute a lot of information which makes it hard to remember.

Please let me know if you have any questions.

[redacted]
Criminal Intelligence Analyst
Oregon Department of Justice | Criminal Division | Oregon TITAN Fusion Center
2250 McGilchrist St SE, Ste. 100
Salem, OR 97302
[redacted]

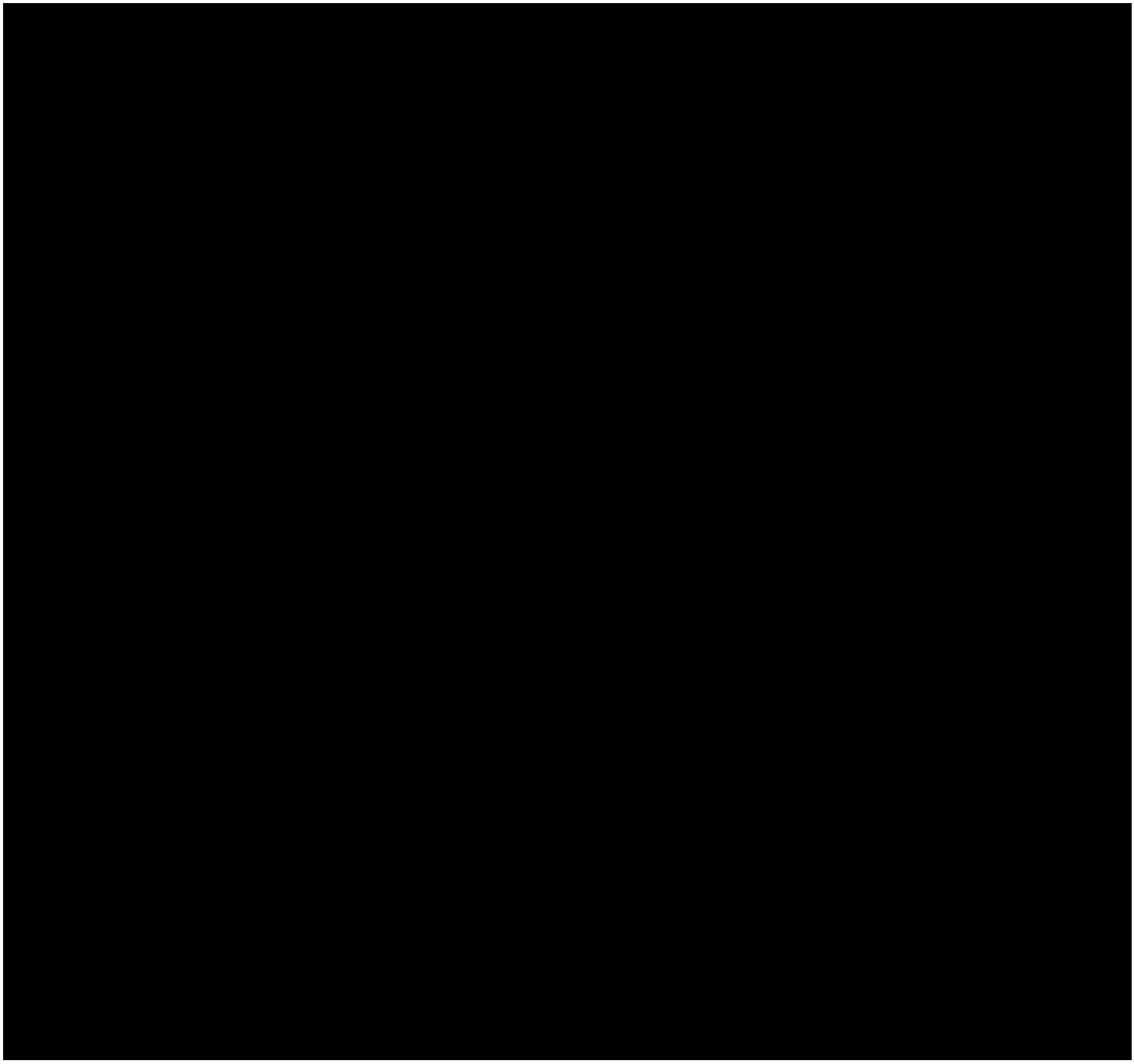
Walker, Carolyn

From: [redacted]@doj.state.or.us>
Sent: Thursday, December 17, 2015 3:54 PM
To: Walker, Carolyn
Subject: more information

Ms. Walker, this is what went out to our LE recipients on 9/10/15 from our office. Our non-sworn recipients received a shorter, redacted version.

I hope to hear from you soon.

[redacted]



[redacted]
Criminal Intelligence Analyst
Oregon Department of Justice | Criminal Division | Oregon TITAN Fusion Center
2250 McGilchrist St SE, Ste. 100
Salem, OR 97302
[redacted]

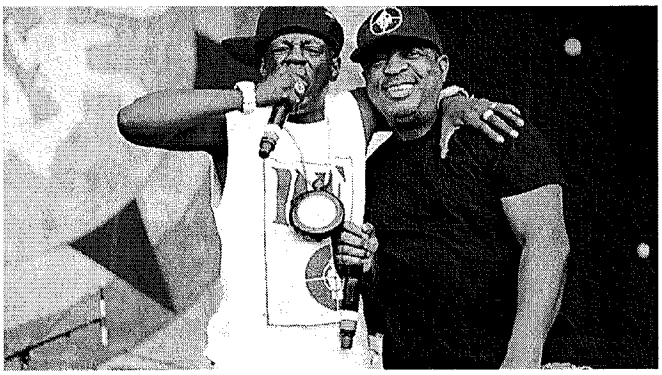
immediately delete the message and any attachments from your system.

****

Public Enemy Reveal Origins of Name, Crosshairs Logo

The group also teamed with eyewear company Arnette for some specially branded shades

BY KORY GROW August 18, 2014



Flavor Flavor Flav of Public Enemy in New Orleans, LA, on April 25, 2014. Tim Mosenfelder/Getty Images

Sunglasses company Arnette Eyewear, which has previously made branded shades for metal thrashers Slayer and hardcore legends Bad Brains, recently hooked up with a musical group known more for revolution than fashion: Public Enemy. Beginning Monday, the company is offering a limited-edition Public Enemy Collection as part of its "Uncommon Projects" initiative. The glasses play off Arnette's Witch Doctor frames and feature interchangeable arms in black and white, sporting the group's logo, as

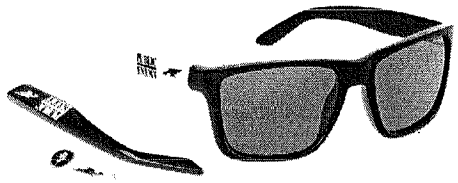
EXHIBIT K
Page 1 of 4

well as a micro-fiber cloth that also features the group's logo.

SIDEBAR

Hour of Chaos: The Best of Public Enemy »

"I like to wear sunglasses, but I don't like to wear sunglasses at performances," the group's Chuck D says. "We decided to do this because we were tired of not having things for people. We're not going to go do some lucrative vodka shit, where it's the rapper goes big and has his own vodka. I can't do that. I'm not part of that one. But I hope these do well."

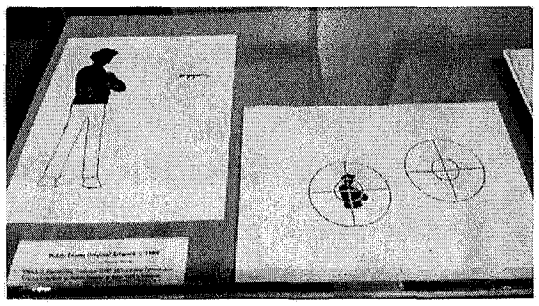


Public Enemy x Arnette Eyewear Courtesy of Arnette Eyewear

Since the frames feature both Public Enemy's name and their logo – a man in the crosshairs of a gun sight that the group constructed in 1986 – Chuck D explained their significance to *Rolling Stone*. "The crosshairs logo symbolized the black man in America," he says. "A lot of people thought it was a

EXHIBIT K
Page 2 of 4

state trooper because of the hat, but the hat is one of the ones that Run-DMC wore. The B-Boy stance and the silhouette was more like the black man on the target."



Chuck D Follow
@MrChuckD

1986 the construction of the logo, magic markers -white out copy machine -Exacto knife ..no computer or Photoshop

6:21 PM - 2 Aug 2014

2,828 2,883

The group's name has more historical origins. "The United States Constitution once considered black people to be three-fifths of a human being," Chuck D says. "If this is a public document, obviously we must be the enemy, so that's where the name Public Enemy came from."

Earlier this year, Public Enemy celebrated the 25th anniversary of their song "Fight the Power," which played heavily in the Spike Lee movie *Do the Right Thing*, where it got repeat

EXHIBIT K
Page 3 of 4

plays. "I feel like Pete Seeger singing 'We Shall Overcome,' [when we perform it]," Chuck told *Rolling Stone* this past June. "'Fight the Power' points to the legacy of the strengths of standing up in music."

Courtesy of Arnette Eyewear

Topics: Public Enemy | Logo

EXHIBIT K
Page 4 of 4

Walker, Carolyn

From: McCauley Matthew <matthew.mccauley@doj.state.or.us>
Sent: Monday, November 16, 2015 4:51 PM
To: Tweedt Darin E
Subject: FW: 2015 OC/INTEL conference
Attachments: JUSTICE-#6345425-v1-Intel_Conference_2015 _How_to_Collect_Protected_Information.PPTX; JUSTICE-#6336446-v1-OC_INTEL_conference_notes_for_legal_presentation_2015.DOCX

Follow Up Flag: Follow up
Flag Status: Flagged

I taught at the LE conference in March 2015. The power point shows that I did a 1st Amendment protected Civil Rights presentation.

From: McCauley Matthew
Sent: Monday, March 16, 2015 3:30 PM
To: McCauley Matthew
Subject: 2015 OC/INTEL conference

Matthew R. McCauley
Sr. Assistant Attorney General
Oregon Department of Justice
Criminal Justice Division
Organized Crime Section
Phone (503) 378-6347

Key Cases from 2014

For Detectives and Command Staff

SEARCH AND SEIZURE—PRIVACY INTERESTS: Defendant does not have a protected privacy interest under Art. I, § 9, in his bank-account records.

State v. Ghim, 267 Or App __, __ P3d __ (December 10, 2014) (Washington) (AAG Dave Thompson). Defendant was charged with first-degree theft and aggravated first degree theft based on a real-estate investment scam he ran with his codefendant wife. He moved to suppress records obtained by subpoena from banks where he and his wife had accounts. He argued that he had a protected privacy interest in those bank records under Art. I, § 9, and that, because the subpoena the state used to obtain those records was not the equivalent of a warrant issued by a neutral magistrate, the state violated his state constitutional rights. The trial court (Judge Gayle Ann Nachtigal) disagreed, denied the motion to suppress, and admitted those records into evidence at trial. Defendant was convicted as charged.

National City Bank
West Falls, VA 21521

Factory Workers Local 888
2210 Elm Street
West Falls, VA 21521

CHECKING ACCOUNT 00002215607

Beginning Date	July 1, 2000
Ending Date	July 31, 2000
Beginning Balance	$1,878.95
Total Deposits	$2,928.70
Total Debits	$2,571.36
Ending Balance	$2,236.29

TRANSACTIONS	DATE	DEBIT AMOUNT	CREDIT AMOUNT	DAILY BALANCE
Check 1605	June 29, 2000	$ 2.53		$1,876.42
Check 1606	July 5, 2000	$ 25.56		$1,850.86
Deposit	July 10, 2000		$2,920.85	$4,771.71
Check 1607	July 14, 2000	$ 118.27		$4,653.44
Check 1608	July 15, 2000	$ 500.00		$4,153.44
Check 1609	July 19, 2000	$ 300.00		$3,853.44
Check 1610	July 24, 2000	$1,475.00		$2,378.44
Check 1611	July 30, 2000	$ 150.00		$2,228.44
Credit Memo	July 31, 2000		$ 7.85	$2,236.29

Held: Affirmed (Sercombe, P.J.). The trial court correctly denied the motion to suppress. Defendant's privacy rights under Art. I, § 9, did not extend to the records held by his banks. The Oregon appellate courts have consistently held that, under Art. I, § 9, an individual does not have protected privacy interest in business records held by a third-party service provider—whether a phone carrier, an internet provider, or a hospital. *See State v. Johnson*, 340 Or 319, 336 (rejecting the defendant's argument that the state needed a warrant, rather than a subpoena, to obtain "records kept by a third party, his cellular telephone provider, respecting his cellular telephone usage"); *State v. Delp*, 218 Or App 17, 20, 26-27 (2008) (no constitutionally protected privacy interest in records independently maintained by the defendant's Internet service provider, which contained "the name, address, telephone number, subscriber number, local and long distance telephone billing records, length of service, and types of service utilized" for the defendant's account); *State v. Gonzalez*, 120 Or App 249, 251 (1993) (no constitutionally protected privacy interest in hospital records that "included the results of defendant's blood alcohol test and a statement by one of the examining physicians… that defendant 'appeared intoxicated,'" as "[t]he records subpoenaed by the state were owned, made, kept and guarded by the hospital"). http://www.publications.ojd.state.or.us/docs/A152065.pdf

SEARCH & SEIZURE—CONSENT: Although defendant's roommate had actual authority to consent to a search of their shared bedroom, she did not have actual authority to consent to search a closed container that belonged solely to defendant.

State v. Bonilla, 267 Or App __, __ P3d __ (December 3, 2014) (Douglas) (AAG Pamela Walsh). A deputy and probation officer went to a home to investigate a report of drug use by a parolee. The address consisted of two houses—a front house and a back house (a freestanding garage). In addition to the parolee, several people lived there, including defendant and her elderly mother. The officers knocked on the door of the front house, and defendant's brother answered; he told them that the parolee was not home, but took them to the back house to talk to the parolee's girlfriend, allowing them to go through a closed storage area to get to the back house. They knocked on the door of the back house, and the parolee's girlfriend answered. While still standing in the storage area, the officers smelled an "overwhelming" odor of marijuana. They told the girlfriend that they were looking for the parolee; she invited them inside. Defendant was sitting in the living room. The officers asked about the marijuana, and the girlfriend said that it was probably coming from defendant's mother in the back bedroom. The officer asked if he could to go the back bedroom, and the girlfriend said yes and led him

there. Defendant's mother admitted that she was using marijuana and gave a bag of it to the officer. She also consented to the officer checking the bedroom for additional drugs. In searching the bedroom with the mother's consent, the officer found a wooden box near the bed, and opened it, finding methamphetamine. The officer asked the mother if the drugs were hers, and she said that it must belong to her defendant. The officer asked why defendant's belongings would be there, and the mother said that she and defendant shared the bed. The officer then went into the living room to talk to defendant. When the officer asked her where she slept, she said she slept in the bedroom with her mother. The officer then told her that her mother had consented to a search of the room and that, during the search, the officer found methamphetamine. Defendant admitted that it was hers. The officer obtained her consent to conduct a second search of the bedroom, and found "snort tubes" with residue. Defendant moved to suppress, arguing that the officers did not have actual authority to perform the search. The trial court (Judge Ronald Poole) denied the motion. On appeal, defendant argued that (1) defendant's brother did not have actual authority to consent to the officers' entry into the storage area to get to the door of the back house; and (2) defendant's mother lacked actual authority to consent to a search of the box in their shared bedroom.

Held: Reversed and remanded (Haselton, C. J.). The trial court erred by denying the motion to suppress. [1] The Court of Appeals did not reach defendant's first argument, because it agreed with her second—that her mother lacked actual authority to consent to the search of the box, even though she had authority to consent to a search of the shared bedroom generally. "Access to joint space and access to personal items within that space are qualitatively distinct. The former does not determine the latter." Nothing in the record indicated that the mother used the wooden box, or that defendant consented to her having access to or using the box. [2] That the officer acted in good faith is immaterial; the state bears the burden of proving actual authority and it presented no evidence to show that the mother used, or had access to, the wooden box. [3] Because there was no valid consent, the warrantless search of the wooden box was unlawful. The daughter's admissions, and the subsequent discovery of the snort tubes, derived from the unlawful search, and therefore should have been suppressed.
http://www.publications.ojd.state.or.us/docs/A153808.pdf

SEARCH & SEIZURE—PRIVACY INTERESTS: Because defendant does not have a privacy interest protected by Art. I, § 9, in the electric company's records of the power usage for his residences, the state did not need a warrant to obtain those records.

State v. Sparks, 267 Or App __, __ P3d __ (November 26, 2014) (Lane) (AAG Andrew Lavin). Defendant ran a marijuana operation out of three residences. He lived in one of those residences with his girlfriend and her two young children. The police conducted surveillance and observed activity that was consistent with marijuana manufacturing. A prosecutor issued a grand-jury subpoena to the electric company for the power records for the residences. The records revealed power use consistent with marijuana grows. Using the evidence from the surveillance and from the power records, police obtained and executed search warrants on the residences. Defendant was charged with unlawful manufacture and delivery and with child neglect, ORS 63.547(1)(a)(B). He moved to suppress the evidence from the searches, arguing that the state

unlawfully obtained the power records without a warrant. The trial court (Judge Debra Vogt) denied that motion. At trial, the court denied his motion for judgments of acquittal. And over defendant's objection, the trial court instructed the jury that a "person has control of a child either by virtue of their relationship to the child or by virtue of the person's ability to control the premises where the child is physically present." A jury found defendant guilty on all charges.

No Privacy interest in records kept by third party on a defendant's electrical usage. Also relates to cell phone bill, internet bill etc... Police can use subpoena.

Held: Convictions for drug convictions affirmed (Nakamoto, J.). The trial court correctly denied defendant's motion to suppress and motion for judgments of acquittal. **Motion to Suppress:** [1] The record shows that the power records were "generated and maintained" by a third party for the party's "own, separate, and legitimate business purposes (such as billing)." Accordingly, "we hold here that defendant has failed to establish that he has a constitutionally cognizable privacy interest" in the power records and that, therefore, "the state did not need to get a warrant to obtain those records." [2] Even if defendant is correct that the grand-jury subpoena in this case was procedurally deficient, he was not entitled to suppression of the power records because ORS 136.432 precludes the exclusion of evidence as a remedy for such a statutory violation. [3] Given the evidence from the power records and from the police surveillance, the affidavits in support of the warrants established probable cause for the search of the residences and the searches were therefore lawful.
http://www.publications.ojd.state.or.us/docs/A150323.pdf

Note: The Court of Appeals did not resolve whether it is improper for a district attorney to use a "grand-jury subpoena" to obtain records when there is not actually an on-going criminal investigation being conducted by the grand jury to which those records may relate.

WEAPONS OFFENSES: "Ninja climbing claws" are not "metal knuckles" for purposes of ORS 166.270(2), which prohibits felons from owning specified weapons.

State v. Behee, 267 Or App __, __ P3d __ (November 19, 2014) (Benton) (AAG Erin Galli). Police executing a search warrant at defendant's home to look for evidence of child pornography found (in addition to child pornography) a set of "ninja climbing claws"—"an elongated, oval-shaped metal band with metal spikes, or claws, on one side; the band fits over the fingers, but does not have separate finger holes. Defendant was charged with felon in possession of a

restricted weapon, ORS 166.270(2), which prohibits felons from possessing, as relevant here, "metal knuckles." At trial, an officer testified that the claws were like metal knuckles in that they were metal, fit over the knuckle area, and could use them to hit someone and inflict injury. Defendant moved for a judgment of acquittal, arguing that the state failed to establish that the claws were "metal knuckles" for purposes of the statute. The trial court (Judge Janet Schoenhard Holcomb) denied the motion, reasoning that whether the item constituted "metal knuckles" was a jury question. The jury found defendant guilty.

Note: The record does not reflect whether defendant is, in fact, a ninja.

Held: Conviction for felon in possession of restricted weapon reversed; remanded for resentencing; otherwise affirmed (Garrett, J.). The trial court erred in denying defendant's motion for judgment of acquittal. Climbing claws are not "metal knuckles"; they "have a demonstrable purpose that metal knuckles do not"—climbing trees—and "their design is inconsistent with the essential characteristic of metal knuckles, which is to enable more powerful punching." Even if the claws *could* be worn in a manner similar to metal knuckles, "whether an object *can* be used for a particular purpose is not the correct inquiry under ORS 166.270(2).
http://www.publications.ojd.state.or.us/docs/A152813.pdf

SEARCH & SEIZURE—PRIVACY INTERESTS: When police officers obtained possession of a cell phone that belonged to someone other than defendant and they then used that phone to exchange text messages with her to set up a drug deal, that exchange did not violate a constitutionally protected privacy right of hers.

State v. Carle, 266 Or App __, __ P3d __ (October 8, 2014) (Marion) (AAG Jake Hogue). Police officers rousted a man sleeping in a stolen truck. They arrested him and searched the truck, finding a cell phone. He told them the phone was not his and instead belonged to "Duane." While the officers were processing the incident, a text message popped up on the phone asking, "Do you know anybody that wants a 30?" The officer knew that to be a request for drug transaction, and he texted back and forth with the caller and eventually arranged a transaction. At the appointed time, defendant showed up and the officers arrested her. Defendant was charged with conspiracy to deliver methamphetamine, and she moved to suppress the text conversation with her that the officers had conducted on Duane's phone. The trial court (Judge Vince Day)

denied the motion, ruling that defendant did not have a constitutionally protected interest that was invaded by the officers. Defendant was convicted on stipulated facts.

Held: Affirmed (Sercombe, J.). The trial court correctly denied defendant's motion to suppress. [1] "The police searched a phone that purportedly belonged to "Duane," not defendant. Accordingly, we are not concerned with any privacy interest that defendant had in any digital copies of the sent text messages on her own phone. Nor are we concerned with what privacy interests Duane had with respect to the text messages on his phone. That is because evidence may be suppressed only if police invaded the personal rights of the person who seeks suppression; the violation of someone else's rights is not enough." [2] When defendant sent a text message to Duane's phone, she may have expected that police would not see it. But once a copy of the text message arrived on Duane's phone, she lost all ability to control who saw that message. As a result, under Art. I, § 9, she "had no protected privacy interest in the digital copy of the message that police found on that found." [3] The result is the same under the Fourth Amendment: "The general notion that a person has a reasonable expectation of privacy in letters or text messages does not compel the conclusion that she has a reasonable expectation of privacy in a copy of a sent text message that is found on the recipient's phone. With respect to letters or goods sent through the mail via the United States Postal Service or a common carrier, courts have held that a sender's reasonable expectation of privacy, to the extent it is based solely upon the fact of his being the sender, terminates once delivery of the goods has been made." http://www.publications.ojd.state.or.us/docs/A150975.pdf

Note: The court noted that it did not matter, for purposes of analyzing whether defendant's constitutionally protected privacy rights were invaded, whether "Duane" had viewed her text messages: "we find it dispositive that, once the message reached that phone, defendant could not control what Duane or anyone else did with the message."

BURGLARY: Evidence that defendant possessed a device consisting of a handle attached to a spark plug that is commonly used for breaking car windows, and that he knew that such a thing is used for that purpose, was not sufficient to support conviction for possessing a burglary tool, ORS 164.235(1).

State v. Cook, 265 Or App __, __ P3d __ (September 17, 2014) (Multnomah) (AAG Peenesh Shah). Defendant, a transient, was found in possession of a device that consisted of multiple spark plugs attached to handle, which is a tool commonly used for breaking car windows. He was charged with possessing a burglary tool, ORS 164.235(1), based on an allegation that he possessed it "with intent to use it to commit and facilitate a theft by physical taking." At trial, the evidence also showed that he knew that the device had an illegal purpose and that he associated with "car prowlers." The case was tried to the court, and defendant moved for judgment of acquittal, arguing that the evidence was insufficient to prove his intent to use the tool for car theft. The trial court (Judge Leslie Roberts) denied the motion, and found him guilty.

If you Google "spark plug used to break window" this is what you get. Sooo.....

Held: Reversed (Hadlock, J.). The trial court should have granted defendant's motion for acquittal. [1] Because "intent" means that "a person acts with a *conscious objective* to cause the result or to engage in the conduct so described," ORS 161.085(7), a factfinder may find a defendant guilty of the charged crime only if the state proved both that (1) he possessed a burglary tool or theft device, and (2) he had the conscious objective to use the burglary tool or theft device to commit or facilitate a theft by a physical taking. [2] A person's knowledge that an item may be put to unlawful use is not sufficient to establish that he intended to use it in that manner. An unlawful intent cannot be inferred from lack of legitimate uses for a particular burglary tool. Therefore, the evidence was not legally sufficient to prove that defendant had the unlawful intent that is an element of the charged offense.
http://www.publications.ojd.state.or.us/docs/A152843.pdf

Notes: [a] The court noted that "the record does not reflect that defendant obtained the spark plugs in a way that, by itself, suggested he intended to use them to commit a crime. Nor does the record reflect that he was located near parked cars when the officer encountered him, that any car prowls or other thefts had just occurred in that area, that he was engaged in any conversation or activity that suggested he planned to commit a theft, or that he had collaborated with other residents of the transient camp to commit other crimes in the past." [b] Judge Sercombe dissented: "Where, as here, the device that defendant possessed had no plausible use other than to commit theft, the factfinder need not resort to too great an inferential leap or a 'stacking of inferences' to conclude that defendant intended to use the device to commit theft."

INTERFERINGWITH POLICE OFFICER: Trial court correctly denied defendant's motion for acquittal on charge of interfering with a police officer, ORS 162.247, despite his claim that his conducted constituted only "passive resistance."

State v. Patnesky, 265 Or App __, __ P3d __ (September 10, 2014) (Jackson) (AAG Karla Ferrall). A police officer went to defendant's residence to talk with him about a hit and-run incident. Defendant was in his driveway trying to put the doors and top back on a Jeep. When the officer tried to get his attention, defendant became "hostile and aggressive" and refused to cooperate. One thing led to another, and the officer ordered him to put down the top he was holding as he approached the officer. When he failed to comply, the officer shot him with a Taser. Another officer arrived on the scene, and they took him into custody despite his resistance. Defendant was charged with interfering with a peace officer, ORS 162.247, among other charges. At trial, he argued that his conduct constituted at most "passive resistance" per ORS 162.247(3)(b) and ORS 162.315, and moved for a judgment of acquittal, contending that he was not violent and did not physically resist when he refused to obey lawful orders by police officers. The trial court (Judge Lorenzo Mejia) denied the motion, and defendant was found guilty.

Held: Affirmed (Ortega, J.). The trial court correctly denied defendant's motion for judgment of acquittal. [1] The text, context, and legislative history of ORS 162.247 show that the legislature intended that the "passive resistance" exception applies when an individual is engaging in "an act or technique of noncooperation that is commonly associated with government protest or civil disobedience." [2] The evidence was sufficient for a jury to find that defendant was not engaged in passive resistance and that he had committed interfering with a peace officer. http://www.publications.ojd.state.or.us/docs/A149433.pdf

RACKETEERING: The evidence sufficiently established that an organized shoplifting group that committed similar thefts in several Safeway stores in the same manner, and that stole the same type of merchandise, were an "enterprise" for purposes of ORICO, ORS 166.720(3).

State v. Walker, 356 Or App 4, __ P3d __ (2014) (Clatsop) (AAG Pamela Walsh). Defendant and Williams stole "high dollar" items—frozen shrimp, beer, Huggies diapers, and Tide detergent valued at more than $1,000—from the Safeway store in Seaside. Video surveillance obtained from Safeway showed that, on two other occasions about two months earlier, the same two men stole the same types of items from a Safeway store in Sandy. Defendant was charged with one count of first-degree theft and one count of racketeering, ORS 166.270(3). At trial, he moved for a judgment of acquittal, arguing that the state failed to prove an "enterprise" for purposes of ORS 166.720(3). The trial court (Judge Philip L. Nelson) denied the motion, and the

jury found defendant guilty on both counts. On appeal, he reasserted his argument that there was insufficient evidence that he was involved in an "enterprise." A divided panel of the Court of Appeals affirmed.

Held: Affirmed (Linder, J.). The trial court correctly denied defendant's motion for judgment of acquittal. [1] The text and context of the statute at issue, ORS 166.720(3), together with the legislative history of ORICO and decisions under the federal RICO Act, show that the term "enterprise" is expansive and "includes casual and informal associations of individuals in fact, as well as organizations with formal structures." Such an "enterprise" can exist "regardless of whether the association or entity has an existence separate from, and is independent of, its membership or activities. The key is whether the association or entity is engaged in ongoing, coordinated criminal activity." [2] "The relationship between defendant and Williams may have been at the 'loosely organized' end of the 'associated-in- fact' spectrum. But no *formal* organization or structure was required. From the multiplicity and distinctive similarity of the thefts that defendant and Williams committed, the jury could find that the criminal conduct in which they engaged was based on a plan or design, that it was purposeful and systematic, and that defendant and Williams had an organized relationship of some longevity, even if it was solely for the purpose of carrying out the racketeering activity. In short, this is a case in which the evidence that permitted the jury to find that defendant engaged in a 'pattern of racketeering activity' coalesced to also permit the jury to find that defendant was part of an association-in-fact entity with sufficient purpose, relationship between the participants, and longevity to qualify as an enterprise under ORICO. No formal structure or existence separate from the association's membership was required. Accordingly, there was sufficient evidence from which the jury could find that defendant was associated with an 'enterprise' for the purpose of ORS 166.720(3)." http://www.publications.ojd.state.or.us/docs/S060828.pdf

Notes: [a] The particular items that defendant and Williams stole were ones that can be readily sold on the black market. Although the state did not present evidence that they had been selling such items, the Supreme Court noted that "the nature and volume of the merchandise readily permitted that inference." [b] This case demonstrates that an association-in-fact enterprise can be proven by what the entity does, rather than by an abstract examination of its structure. Here, the planning and organizing behind each crime was apparent from the consistent pattern in which defendant and Williams committed the thefts.

SEARCH & SEIZURE—SEARCHES PURSUANT TOWARRANT: [1] The police lawfully obtained a warrant pursuant to ORS 136.583(1) to obtain, from Yahoo in California, records of defendant's email communications with the victim. [2] The warrant was sufficiently particular for purposes of Art. I, § 9.

Google

State v. Rose, 264 Or App __, __ P3d __ (July 2, 2014) (Polk) (AAG Doug Petrina). The victim is a 16-year-old girl, and defendant is the stepfather of her friend. After some sexually explicit online communications between them, and at his prompting, she emailed him, in June 2010, two

topless pictures she had taken of herself. Pursuant to ORS 136.583, the police obtained a search warrant for all email records of the victim and defendant stored by Yahoo!, a California-based company; the warrant was executed in California. The pictures were included among those emails. Defendant was charged with using a child in a display of sexually explicit conduct, ORS 163.670. Defendant moved to suppress, arguing that the warrant was invalid, because the warrant authorized the search and seizure of items located outside of Oregon and because the warrant was insufficiently particular. The trial court (Judge Fred Avera) denied the motion, and defendant was found guilty.

Held: Affirmed (Nakamoto, J.). The trial court correctly denied defendant's motion to suppress. [1] Under ORS 136.583(1), criminal process, including a search warrant, may be issued to a recipient regardless of whether the recipient or the items sought are located within Oregon, so long as the criminal matter is triable in Oregon and the exercise of jurisdiction over the recipient is not inconsistent with the Oregon or federal constitutions. The statutory jurisdictional requirement requires the court issuing the warrant to have personal jurisdiction over the recipient, and here that was not disputed. Accordingly, ORS 136.583 authorized the court to issue the out-of-state warrant. [2] Even though the probable cause related to emails in June 2010, the warrant was sufficiently particular for purposes of Art. I, § 9, because the warrant was limited to a particular location, and the description of the items to be seized left the officers with no discretion in the matter. [3] The "scrupulous exactitude" test that limits searches for material protected by the First Amendment does not apply here, because the warrant sought "material as evidence of a crime, and not for the ideas that it contains."
http://www.publications.ojd.state.or.us/docs/A147635.pdf

Notes: [a] The Court of Appeals assumed, without deciding, "that defendant had a protected privacy interest in the emails and electronic files produced under the warrant." [b] The opinion contains an extended discussion of the various provisions in the Stored Communications Act, 18 USC § 2701 *et seq.*

UNITED STATES SUPREME COURT
SEARCH & SEIZURE—INCIDENT TO ARREST: Searches of digital data on cell phone do not fall within the Fourth Amendment exception for searches incident to arrest, and generally require a warrant.

Riley v. California, 573 US __ (June 25, 2014). In two unrelated cases, police searched the cell phones of defendants whom they had arrested, without warrants, under the search incident-

to-arrest exception to the Fourth Amendment's warrant requirement. In the first case, *Riley*, police found evidence on defendant's smart phone that defendant was a member of the Bloods gang, which led to his prosecution for crimes (including attempted murder) committed during a gang shooting a few weeks earlier. In the second case, *Wurie*, police found evidence on defendant's flip phone that enabled them to identify an apartment associated with suspected drug activity, which they secured while they obtained a drug warrant; the subsequent warrant search turned up evidence that led to defendant being charged with drug and firearms offenses. Both defendants moved to suppress, arguing that the searches of their phones were not valid searches incident to arrest.

Held: Reversed and remanded (Roberts, C.J.). [1] As a general rule, police must obtain a search warrant to search digital data on a cell phone. The rationales underlying the search incident to arrest doctrine as applied to physical objects—the government interests of ensuring the safety of police officers and preventing the destruction of evidence—have little force when applied to the search of digital data on a cell phone. "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.... Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person,"—specifically, their "immense storage capacity" and pervasiveness in modern life. "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." [2] "Our answer to the question of what police must do before searching a cell phone is accordingly simple—get a warrant." But "other case-specific exceptions [than search incident to arrest] may still justify a warrantless search of a particular phone" based on exigency.
http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

SEARCH & SEIZURE—SCHOOL SEARCHES: After receiving information that youth threatened to bring a gun to school and shoot a particular fellow high-school student, school principal's limited search of youth's backpack was reasonable under Article I, section 9.

State v. A. J. C., 355 Or 552, __ P3d __ (May 30, 2014) (Washington) (SG Anna Joyce). Youth is a high-school student. One evening, he called V, a fellow student with whom he had a relationship, and told her that he was going to bring a gun to school to shoot her and other students. The next morning, V reported the threat to her school counselor, who then informed the principal, Smith. Smith was not familiar with V, who was new to the school, but knew youth, who had a history of disciplinary issues. Although he considered the threat to be "outside the realm" of what he thought could happen, he did not believe he could disregard the threat without further information. Smith searched youth's locker, finding no gun. He then went to youth's classroom, where youth was seated at a desk with his backpack under his seat. Smith asked youth to accompany him to his office, and Smith carried youth's backpack.

In the principal's office waiting for them were youth's mother and a police officer. Smith informed youth that V had reported that he had threatened to bring a gun to school and shoot her; youth denied making the threat, but admitted that he had a relationship with V. After several minutes, Smith told youth that he had to investigate the threat, and was going to search youth's backpack. Youth did not object or give consent. Smith opened the largest compartment of the backpack first, and found nothing incriminating. He then opened a smaller second compartment, and found several .45-caliber bullets. In a third compartment, he found a .45-caliber handgun wrapped in a bandana. The police officer then arrested youth, and the state petitioned the juvenile court to take jurisdiction of youth for conduct that, if committed by an adult, would constitute possession of a firearm in a public building, unlawful possession of a firearm, and menacing. Before trial, youth moved to suppress the evidence that Smith found in youth's backpack, arguing that the search violated Art. I, § 9, because Smith lacked reasonable suspicion, and because the search was not justified under the circumstances. The juvenile court (Judge James Fun) denied the motion, ruling that the search was lawful under the school-safety exception to the warrant requirement, as articulated in *State ex rel. Juv. Dept. v. M.A.D.*, 348 Or 381 (2010). The juvenile court (Judge James Fun) found youth within its jurisdiction, and youth appealed. The Court of Appeals affirmed, and the Supreme Court granted review. On review, youth abandoned his argument that the principal lacked reasonable suspicion, and argued only that the search of the backpack was unreasonable because any immediate safety risk had dissipated.

Held: Affirmed (Baldwin, J.). The principal's search of youth's backpack was lawful under the school-safety exception. [1] In *M.A.D.*, the Supreme Court held that, although students are entitled to the protections of Art. I., § 9, those protections "may yield to permit school officials to undertake reasonable protective measures—such as conducting a limited search—in response to credible safety threats in a school setting. … If the protective actions taken by a school official—such as a limited search—are based on specific and articulable facts, and are reasonable, the school official's conduct does not violate Article I, section 9." [2] In determining "whether a school official's actions were reasonable under the totality of the circumstances, the unique features of the official's responsibilities and the school setting must factor into the assessment," so the analysis is not identical to the one that applies to officer-citizen interactions outside the school setting. [3] "Smith's search of youth's backpack was reasonable under the circumstances present when he conducted the search." Smith knew that the threat was more than a generalized safety threat, and youth's admission that he had a relationship with V strengthened the credibility of the information that Smith had already received. "Taken as a whole, the totality of the information known to Smith was sufficient for him to reasonably suspect that youth possessed a firearm for the purpose of shooting one or more students." [4] In addition, "Smith's actions in responding to the threat were particularized to the circumstances known to him." At the time of the search, he did not know what type of gun might be involved, or where it might be; he knew

only that the gun was not in youth's locker. "No matter where the gun was located, whether it was in youth's immediate possession or not, it presented a danger to students. As a result of those factors, the threat of harm to others remained imminent at the time of the search." [5] For those reasons, Smith's "limited search of the parts of youth's backpack that could contain the gun was therefore reasonable." Because the search was limited to compartments that could contain a gun, and because Smith stopped searching once he found the gun, the search was not overly intrusive. "We will not now uncharitably second-guess his actions or demand that he could have performed the least intrusive search that we can conceive with the benefit of hindsight." [6] The court emphasized, however, that "the permissible range of options available to Smith was not unlimited. ...[S]chool officials are not licensed to engaged in an unlimited search of students and their belongings on campus based on generalized threats to safety." http://www.publications.ojd.state.or.us/docs/S061191.pdf

SEARCH & SEIZURE: Seizure of property from defendant's home by employee constitutes "state action" and is invalid under Article I, section 9; because that initial seizure led police to apply for a warrant to seize additional items from defendant's home, the trial court should have suppressed evidence seized pursuant to that warrant.

State v. Sines, 263 Or App __, __ P3d __ (June 4, 2014) (Deschutes) (AAG Rolf Moan). Two of defendant's employees—a housekeeper and a business assistant—regularly worked in defendant's home; they suspected that he was sexually abusing the victim, his nine-year-old daughter. The housekeeper reported her suspicions to a DHS worker, telling him that she had seen "discharge" on the victim's underwear, and asked what authorities might learn from the underwear if she took it from defendant's house. The DHS worker said he could "hook her up" with law enforcement officials who could test the underwear. The housekeeper asked what would happen if she obtained the underwear, and the DHS worker said he "could not tell her to do that," but also noted that "we can't do anything without physical evidence." That same day, the DHS worker contacted a sheriff's deputy. DHS policy required the "completion of a safety check within 24 hours of a report of possible abuse" absent "good cause for a delay." The DHS worker and deputy concluded that there was a "good likelihood that the case was going to get stronger when [the housekeeper] made [her] decision," and decided to "assign the case as a five day response" instead of responding immediately. They did not tell the housekeeper about DHS's safety-check policy or tell her that the safety check was being delayed. Also that same day, the housekeeper reported her conversation with DHS to defendant's business assistant. The assistant was scheduled to work the next day and agreed to seize a pair of the victim's underwear; the next day, she took a pair of the victim's underwear from defendant's laundry room and delivered it to the housekeeper. The housekeeper delivered the underwear to the police the following day; the underwear tested positive for sperm heads. Later that day, police—based on the test results and on information from the housekeeper, defendant's business assistant, and the DHS worker—obtained a search warrant for defendant's home. They seized additional clothing of the victim's while executing the warrant, and testing revealed sperm heads on those items also. Defendant was charged with several sexual offenses, and he moved to suppress evidence, "including derivative evidence," obtained through the initial warrantless search and seizure, and obtained through the testing of the initial pair of underwear. The trial court (Judge Alta Brady) concluded, however, that no "state action" occurred when defendant's employee seized the initial pair of underwear. It thus denied the motion to suppress.

Held: Reversed (Duncan, J.). The trial court should have granted the motion to suppress. [1] Although no state actor retrieved the underwear from defendant's house, there was nevertheless "state action" for purposes of Art. I, § 9 because "the state was sufficiently involved that the seizure of the underwear was state action" because the DHS worker (a) "knew what the [housekeeper] planned to do and that she was likely to do it," (b) "communicated with [her] about her plans and offered law-enforcement support if she conducted the seizure," and (c) "delayed the safety check to allow [her] to accomplish the planned seizure." Because the seizure involved state action, was conducted without a warrant, and was not justified by any exception to the warrant requirement, suppression was required. [2] The error in denying the motion to suppress was not harmless, because the results from the tests of the underwear led police to apply for and obtain the warrant that led to discovery of additional evidence on other clothes found in defendant's house. Under *State v. Hall,* 339 Or 7 (2005), defendant therefore proved that the seizure of the other clothes—although obtained during a warrant search—"derived from the seizure of the underwear" by the housekeeper, and the trial court should have suppressed it.
http://www.publications.ojd.state.or.us/docs/A146025.pdf

Note: The Court of Appeals appears to have concluded that the warrant could not authorize the search even assuming that the remaining evidence in the search-warrant affidavit— that is, evidence aside from the sperm heads found on the underwear seized by defendant's employee—provided probable cause to search defendant's home.

SEARCH & SEIZURE—INVENTORY SEARCHES: Marion County post-booking inventory policy that allows officers to open all closed containers is unconstitutionally overbroad.

State v. Cherry, 262 Or App __, __ P3d __ (May 5, 2014) (Marion) (AAG Susan Howe). An officer arrested defendant for giving false information to a police officer and took him to jail. There, a corrections deputy inspected the contents of the pockets of defendant's jacket, discovering stolen checks. An investigation led to defendant being charged with identity theft. He moved to suppress the checks, arguing that the inventory was unlawful. At the hearing, the prosecutor introduced a county policy that instructed corrections officers to, post-booking, open all of an inmate's closed containers to look for proof of identification, cash, valuables, medications, or contraband. The trial court (Judge Joseph Ochoa) denied the motion to suppress. Defendant entered a conditional plea of guilty.

Held: Reversed and remanded (Duncan, J.). The trial court should have granted defendant's motion to suppress. [1] The policy provision introduced, if standing on its own, was overbroad, because it authorizes deputies to open all closed containers. The prosecutor did not introduce the county's *pre*-booking policy provision, which required officers to remove all items from a suspect's pockets prior to booking, and would have provided a sound basis for the officer's actions. [2] The Court of Appeals refused to take judicial notice of the un-introduced policy provision, concluding that the trial record most likely would have developed differently if that policy had been introduced at trial.
http://www.publications.ojd.state.or.us/docs/A148450.pdf

SEARCH & SEIZURE—PRIVACY INTERESTS: Officers did not violate either Art. I, § 9, or the Fourth Amendment by entering defendant's tent, which he had erected unlawfully on a city sidewalk.

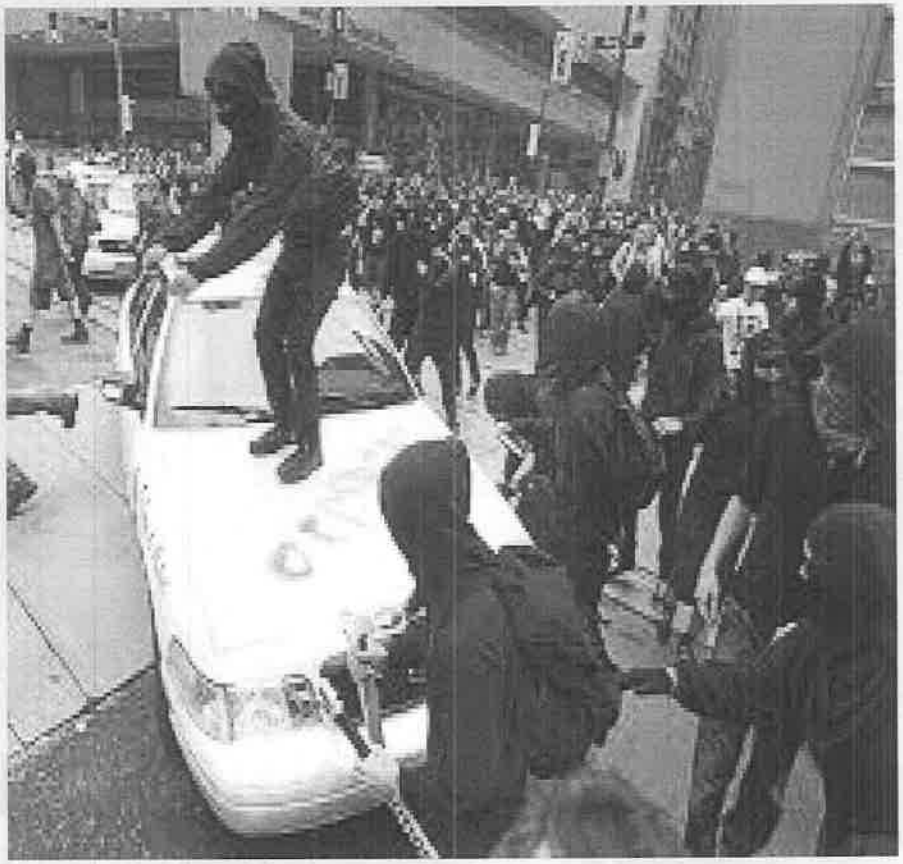
State v. Tegland, 269 Or App 1, __ P3d __ (2015) (Multnomah) (AAG Carson Whitehead). Defendant lived in a temporary tarp structure that he had erected partially on private land and partially on a City of Portland sidewalk, in violation of city code. Officers had previously asked him to remove the structure. Later, officers considered removing the structure and lifted a corner of the tarp. They saw defendant with drugs and drug paraphernalia and arrested him. He was charged with possession of methamphetamine. He moved to suppress, arguing that the officers performed an illegal search under Art. I, § 9, and the Fourth Amendment when they lifted the corner of the tarp without a warrant. The trial court (Judge Janice Wilson) denied the motion, and he was found guilty.

Held: Affirmed (Haselton, J.). [1] "Although the fact that the referent space was someone's residence is highly significant, it is not *per se* dispositive. Rather, the touchstone, for purposes of Article I, section 9, is whether the space is a place that *legitimately* can be deemed private." [2] Defendant did not have a right to privacy in his tarp structure protected by Art. I, § 9, because (a) the structure violated city code; (b) the officers had authority to summarily abate the structure because it obstructed the right of way; and (c) the officers had previously warned him that the structure was illegal. [3] The officers' entry into defendant's tent did not violate the Fourth Amendment, because "a person has no reasonable expectation of privacy in a temporary structure illegally built on public land, where the person knows that the structure is there without permission and the governmental entity that controls the space has not in some manner acquiesced to the temporary structure."
http://www.publications.ojd.state.or.us/docs/A148797.pdf

HOW TO LAWFULLY COLLECT PROTECTED INFORMATION

HISTORY AND NOW

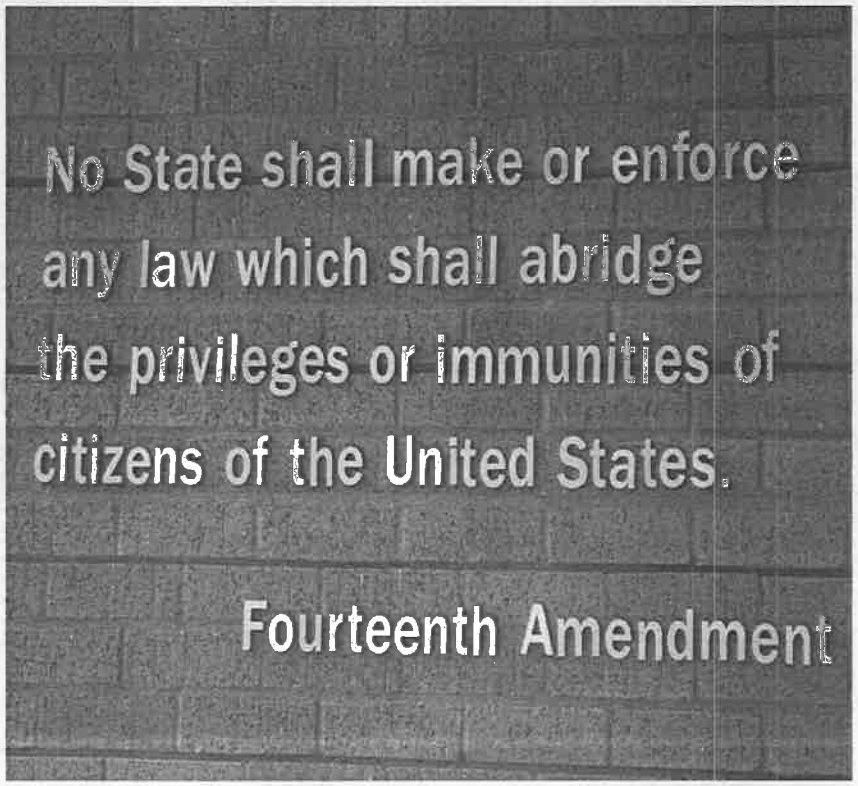
Protecting Civil Liberties

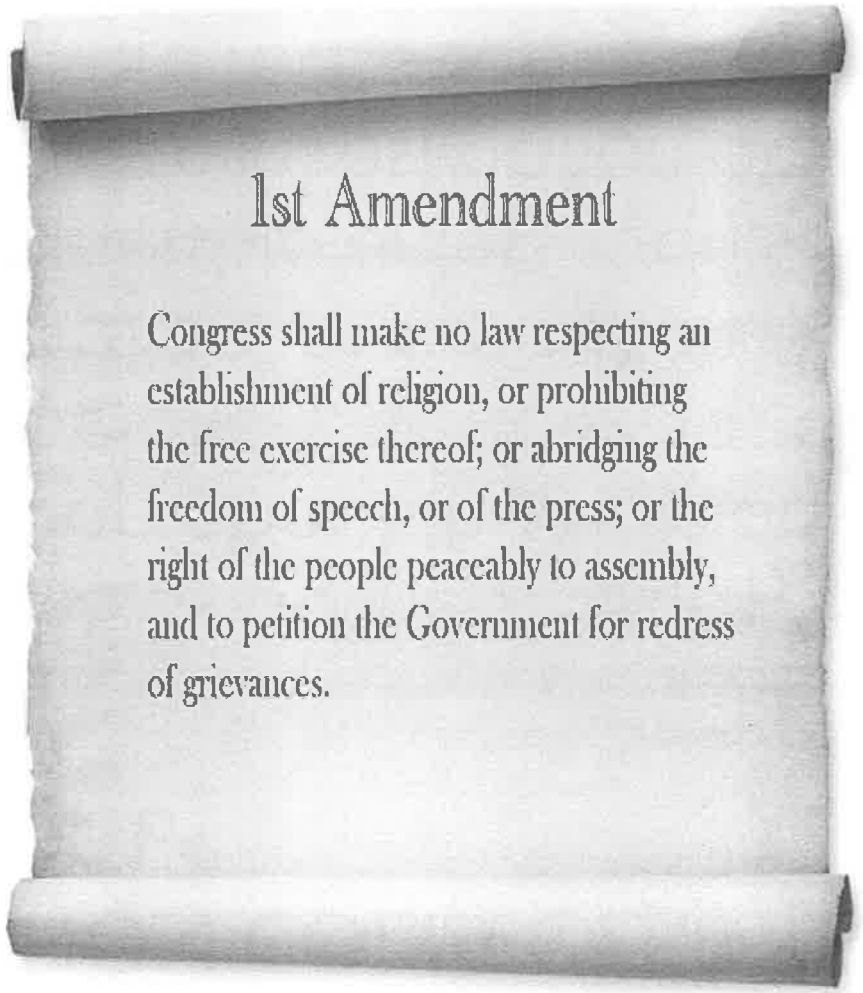


While identifying criminals

PROTECTED INFORMATION IS…

Information relating to Areas Protected by the 1st and 14th Amendments





LIMITING INFORMATION COLLECTED BY POLICE

ORS 181.575:

No law enforcement agency, as defined...,may collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

BREAKING IT DOWN

"Law enforcement agency" covers:

1. County Sheriffs
2. City Police Departments
3. Oregon State Police
4. Law enforcement agencies of other states and
5. Federal law enforcement agencies

BREAKING IT DOWN

Information Relates to:

- Political
- Religious
- Social

- Views
- Associations
- Activities

BREAKING IT DOWN

Unless....

1. Such information directly relates
2. to an investigation of criminal activities,
3. and there are reasonable grounds to suspect
4. the subject of the information
5. Is or may be involved in criminal conduct.

"Reasonable Grounds" = Reasonable Suspicion

EASY OR DIFFICULT TO DO?

Clearly a Crime?

Clearly Not?

BUT WHAT ABOUT THIS?

Do you want to know who these people Are?

"SPEECH" OF A POLITICAL VIEW THROUGH A POLITICAL ACTIVITY

A PETA event – Not real dead people

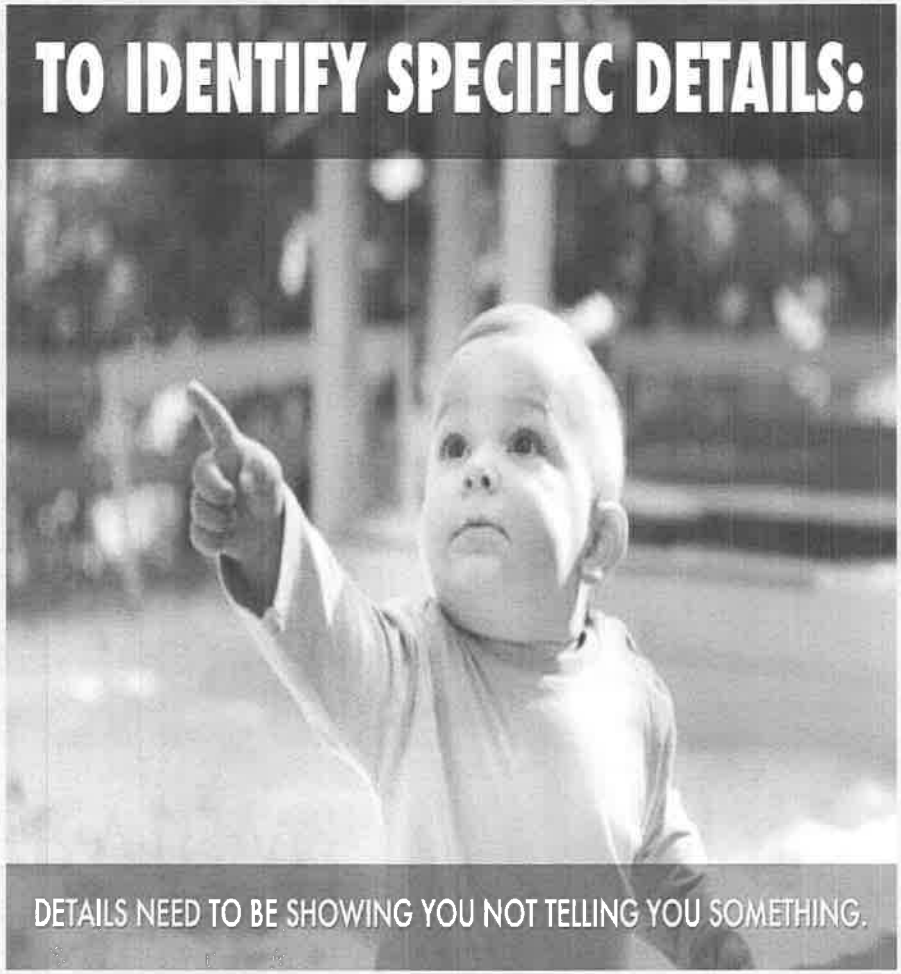
REASONABLE SUSPICION
AN OVERVIEW

Reasonable suspicion means that an officer holds a belief that is reasonable under the totality of the circumstances existing at the time and place the officer acts.

Thus, reasonable suspicion must be based on a subjective belief by the officer that a crime has been or will be committed, and that subjective belief must be **objectively reasonable under the totality of the circumstances**.

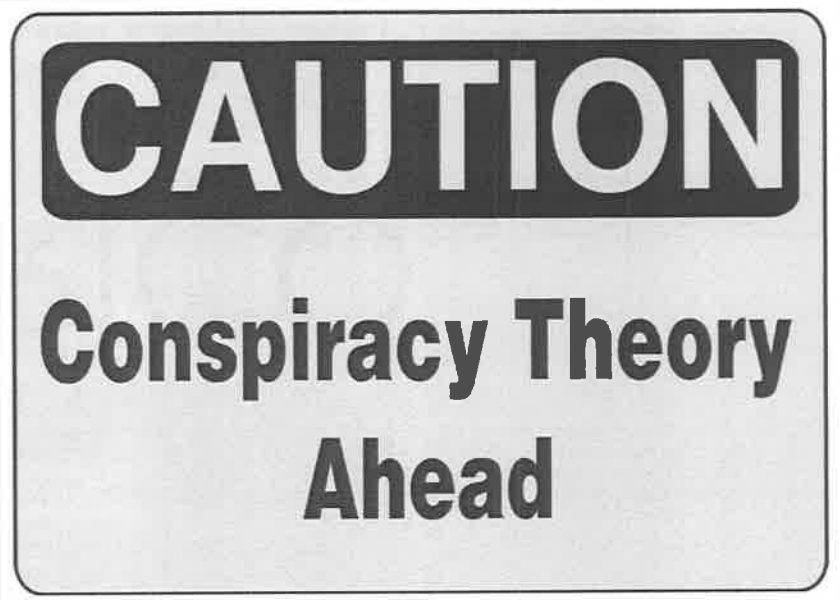
REASONABLE SUSPICION
AN OVERVIEW

Be able to have Specific and Articulable facts to support your belief.



CRIMES AND ORGANIZATIONS

- Conspiracy = agreement
- Aid and Abet
- Facilitate



TYPES OF CRIME

Any crime will do -
but look for...

Trespassing

Criminal mischief

Disorderly Conduct

Harassment

Tax Crimes

Explosives

Weapons offenses,
and...

RICO

WHAT'S RICO? (1 OF 4 WAYS)

- It is unlawful for any person associated with an enterprise to conduct or **participate directly or indirectly** in the enterprise through a **pattern of racketeering activity**

- It is unlawful for any person to **conspire to commit** any form of racketeering.

This is a Class A Felony with 20 year prison maximum

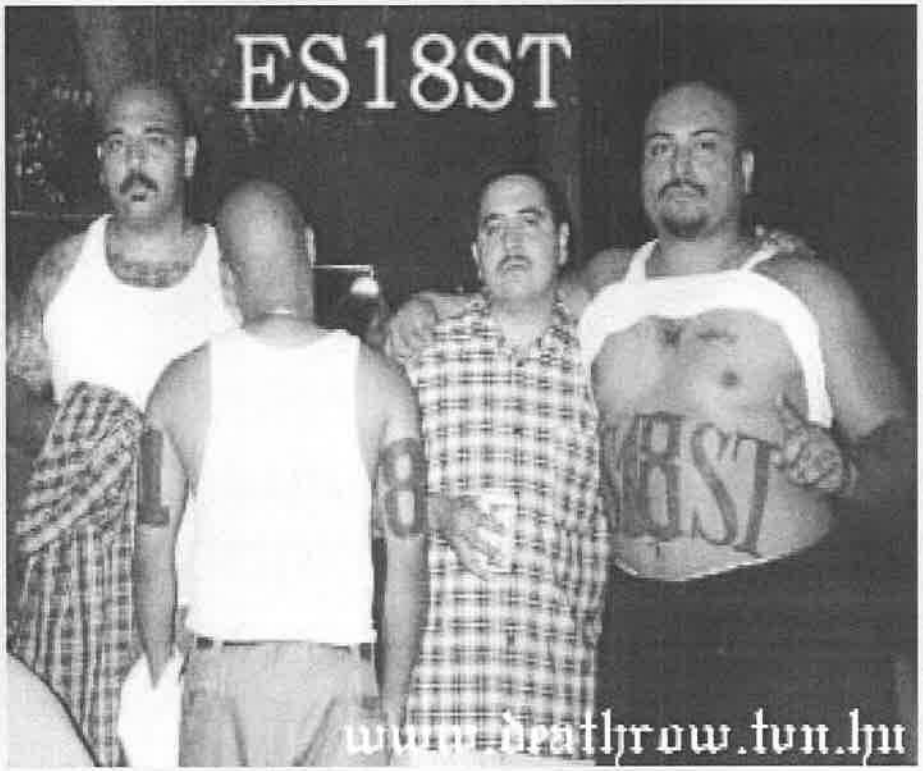
WERE HIS POLITICAL VIEWS GOOD TO KNOW?

- How would you link information you had about his politics to reasonable suspicion of a crime?

Timothy McVeigh – Oklahoma City Bombing

WHAT DOES THIS DEPICT?

- A social group or a criminal organization?
- What information on these guys can you collect and keep if any?



BUT WHAT ABOUT GANG DOCUMENTATION?

There is no Oregon law requiring "gang documentation" prior to collecting gang related criminal intelligence.

There is an Oregon requirement that criminal intelligence involving personal identifying information have reasonable suspicion of a crime for a person or a group.

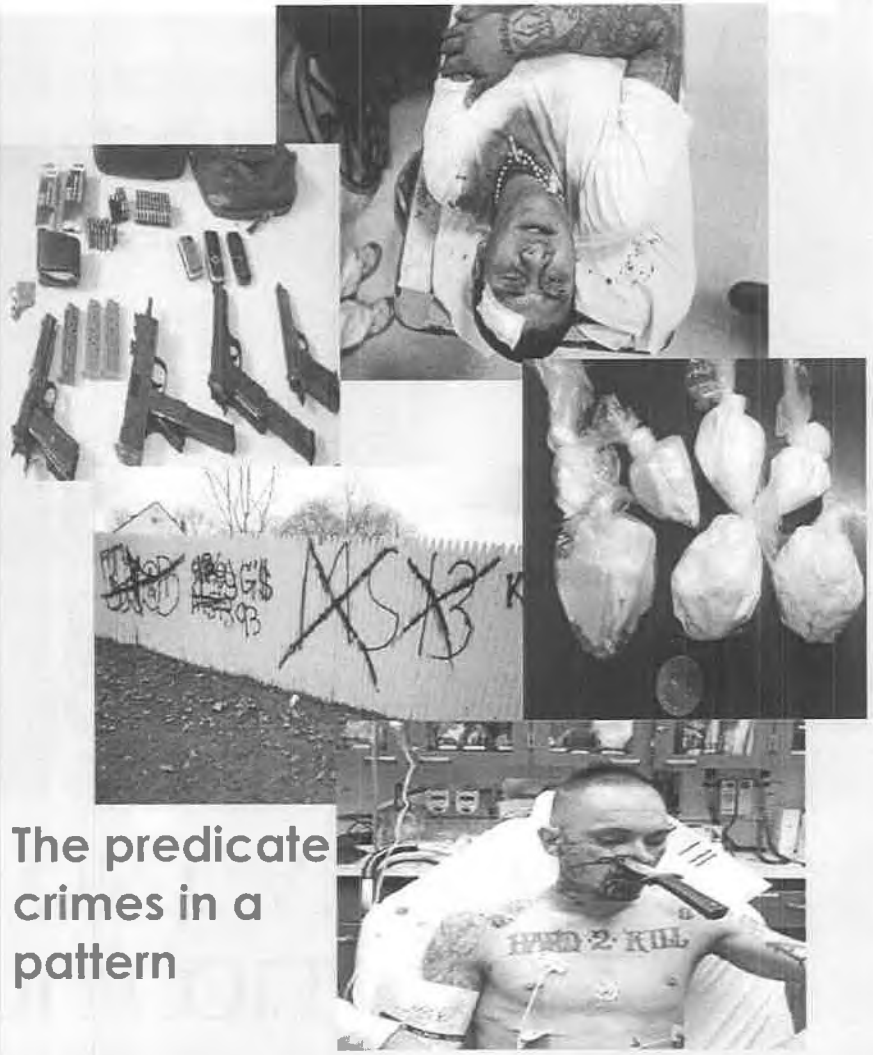
Soooo…What's the crime?

SO HOW DO YOU COLLECT INFORMATION ON GANGS?

- Focus on the "gang" as an "enterprise" and use RICO "enterprise theory" to build RS that gang is a RICO enterprise.
- See RICO "association in fact."
- Gang members then are associates or participants in RICO Enterprise.
- RS for each member can then be assembled.

THE GANG AS ENTERPRISE – THE MEMBER AS ASSOCIATE

The "associate"



The predicate crimes in a pattern

The "enterprise"

RECORDING GANGS AS ENTERPRISES

Identify the criminal organization:

- Colors
- Tats
- Togetherness
- Rules
- Members commit crime
- Membership facilitates crime
- Admissions – self descriptions

Putting the Associate (member) with the Enterprise (Gang)

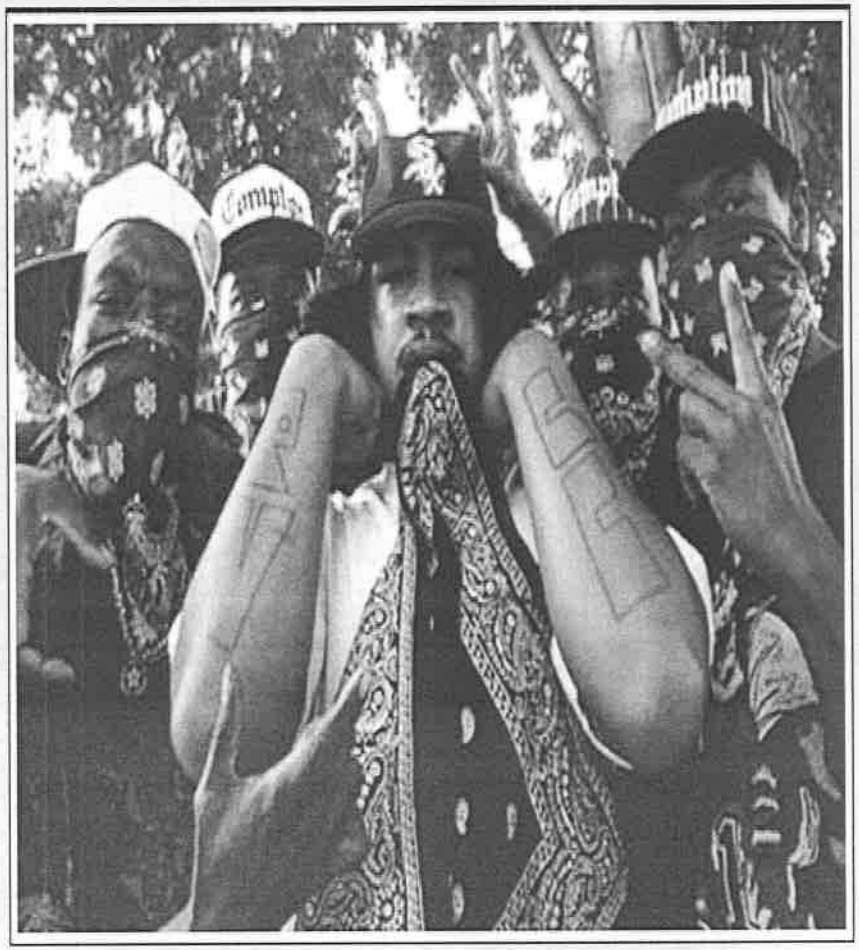
- Colors (only by members)
- Tats (only by members)
- Crime – linked to Gang
- Associations with other members
- Gang facilitates crimes of members
- Self admits

KEY QUESTIONS?

- Can anyone wear a gang tat?
- Can anyone tag the gang name?
- Can anyone wear the gang colors?
- Can anyone pose as a gang member?
- What happens if they do without permission?

ENTERPRISE AND ASSOCIATE= GANG AND GANG MEMBER

- Information should be articulated in a police report.
- Opening a RICO case or referring to the crime does NOT mean you have to file it – but it does allow you to "document" a RICO enterprise.



HOW DO YOU TAKE ON A CRIMINAL ORGANIZATION?

Center: Paul Castellano, Former Boss, Gambino Crime Family, NYC.

- OC cases are best handled as long term proactive investigations.
- Consider wire intercept and task force approach.

Just FYI: The Gambino Family used free trade zones in California owned by an Oregon "businessman" to move illegal cigarettes from China which came via Texas and were headed to NYC.

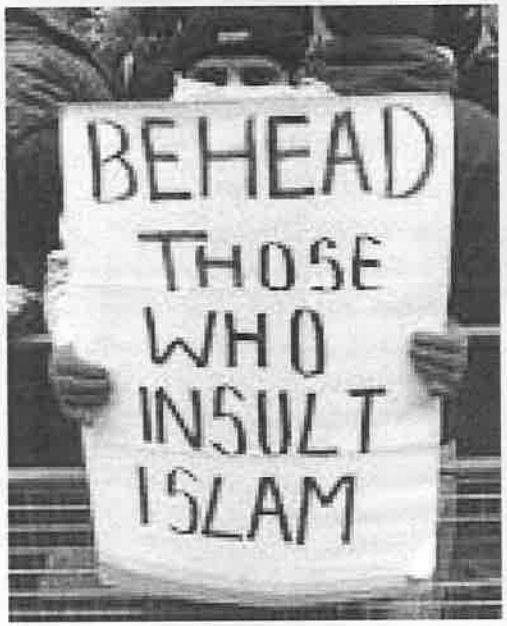
WHAT IF YOUR INFORMATION INCLUDES A POLITICAL VIEW?

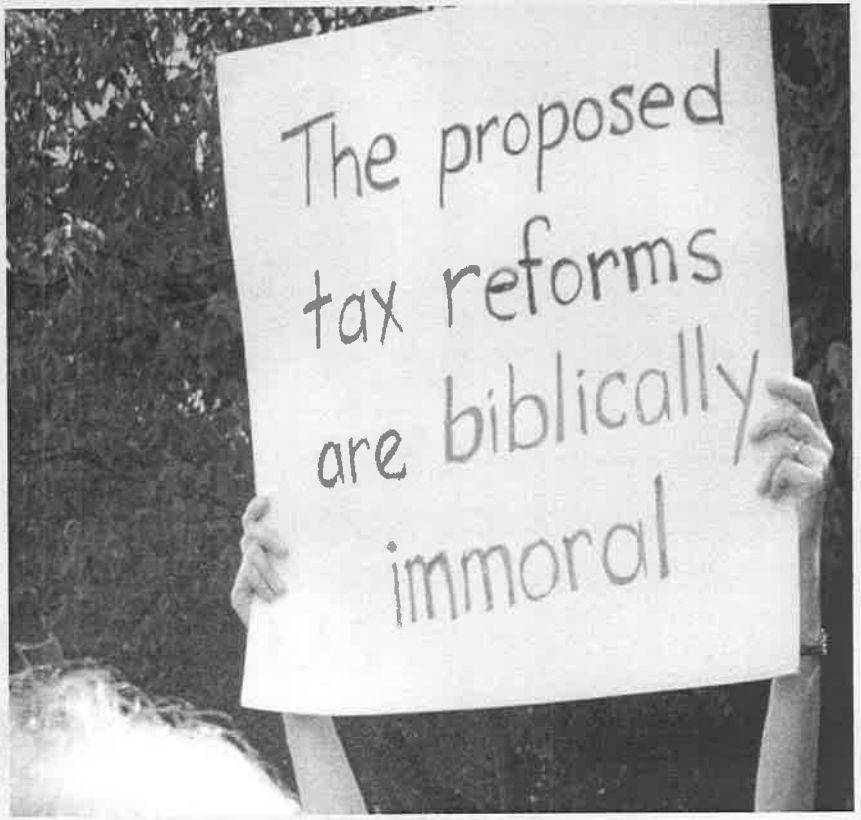
Is there any crime for which reasonable suspicion applies?

VIOLENT ANARCHISTS

Downtown Portland Oregon – Organized? Criminal? A Pattern?

OR A RELIGIOUS VIEW?

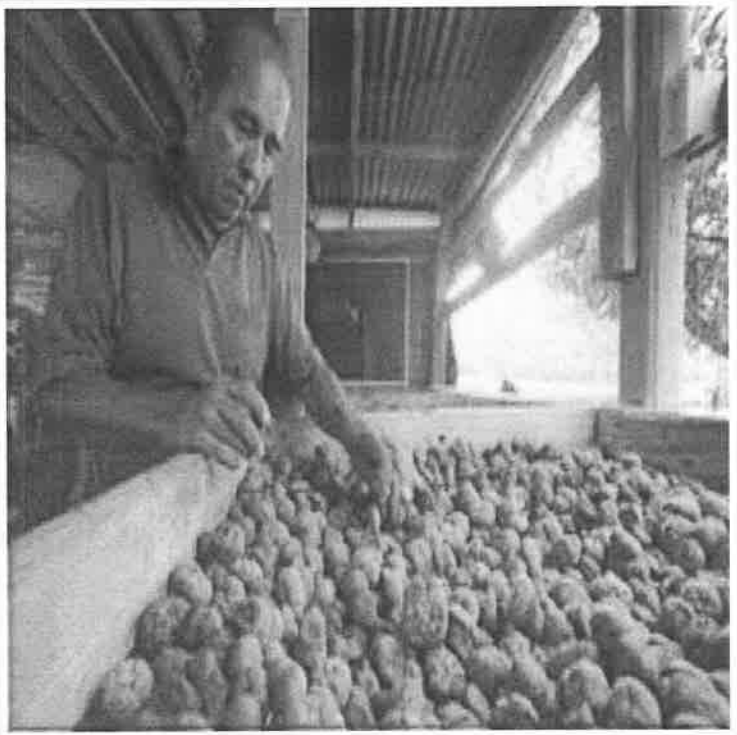




WHAT IF YOU GATHER CRIMINAL
INFORMATION AND THERE IS CONNECTED
POLITICAL ACTIVITY?

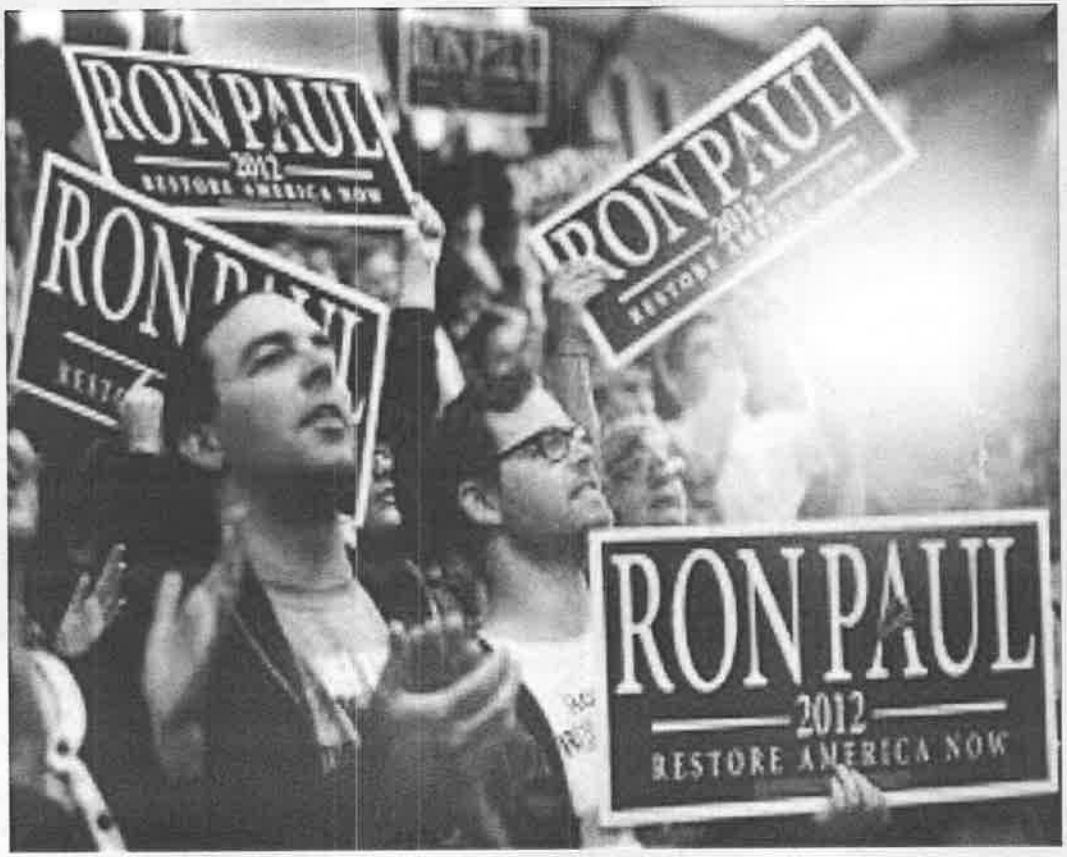
WHAT IF THE INVESTIGATION GATHERS INFORMATION ABOUT A RELIGIOUS ACTIVITY

Peyote manufacture and use

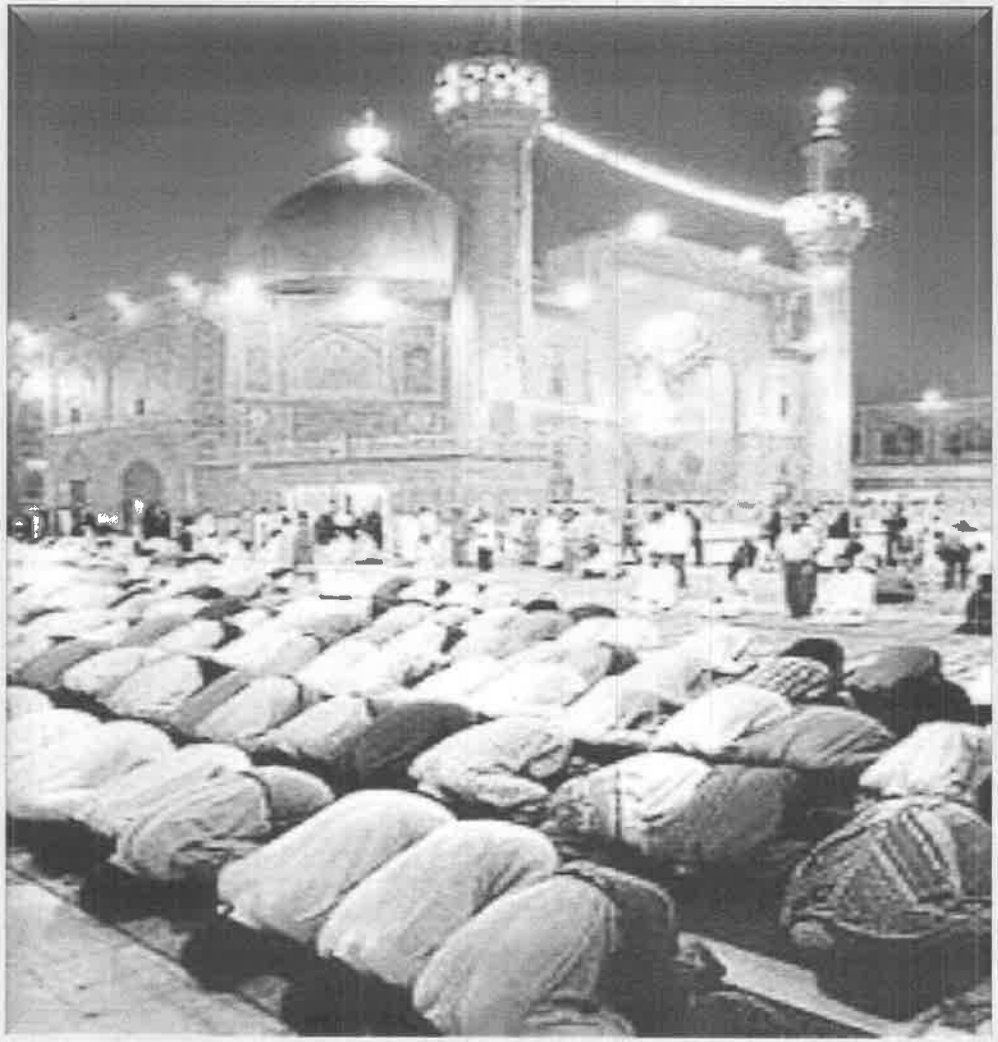


ARE THESE SOCIAL ASSOCIATIONS &ACTIVITIES OR A MEETING OF A CRIMINAL ORGANIZATION?

CAN YOU TRACK A CRIMINAL'S POLITICAL ASSOCIATIONS & ACTIVITIES?



WHEN CAN YOU GATHER INFORMATION ON A PERSONS RELIGIOUS ASSOCIATIONS & ACTIVITIES?



CAN YOU TRACK THESE SOCIAL ASSOCIATIONS & ACTIVITIES?

SUMMARY OF 181.575

1. If information you are collecting involves a religious, social or political view, activity or association you MUST have reasonable suspicion of a crime related to the subject.
2. Use creativity and articulate your reasonable suspicion in some way.
3. Think of a wide variety of crimes to form the basis of collecting information you need.

A DISCUSSION ABOUT CRIMINAL INTELLIGENCE

THE MISSION OF CRIMINAL INTELLIGENCE

The general mission of criminal intelligence is:

1. to develop knowledge about individuals or groups who are involved in criminal conspiracies;
2. and to understand how they function;
3. And to describe their current activities;
4. and forecast future actions they may undertake.

IT IS ENTERPRISE/CONSPIRACY FOCUSED!!

TWO CONCEPTS

1st Information collection:

Requires a legitimate law enforcement purpose

2nd Criminal intelligence requires reasonable suspicion

WHAT ARE THE RULES FOR INTEL PROGRAMS?

The two primary sources for state and local agencies criminal intelligence efforts are the **Association of Law Enforcement Intelligence Units Criminal Intelligence (LEIU) File Guidelines** and the **Code of Federal Regulations, Title 28, Part 23 (28 CFR).**

The **LEIU guidelines are not statutory** and are not mandatory for any agency.

The provisions of **28 CFR are statutory**, but technically apply only to agencies accepting federal funds pursuant to the Omnibus Crime and Safe Streets Act for the purpose of creating or sustaining an intelligence operation.

HOWEVER…NO ONE WANTS TO GET SUED

- The ACLU and other groups have successfully challenged police intelligence collection schemes around the country.
- The LEIU standards and those set out in 28 CFR offer the best guidance and protection to the agencies and officers.

CRIMINAL INTEL SUPPORTS THE LAW ENFORCEMENT CEO

The CEO must know:

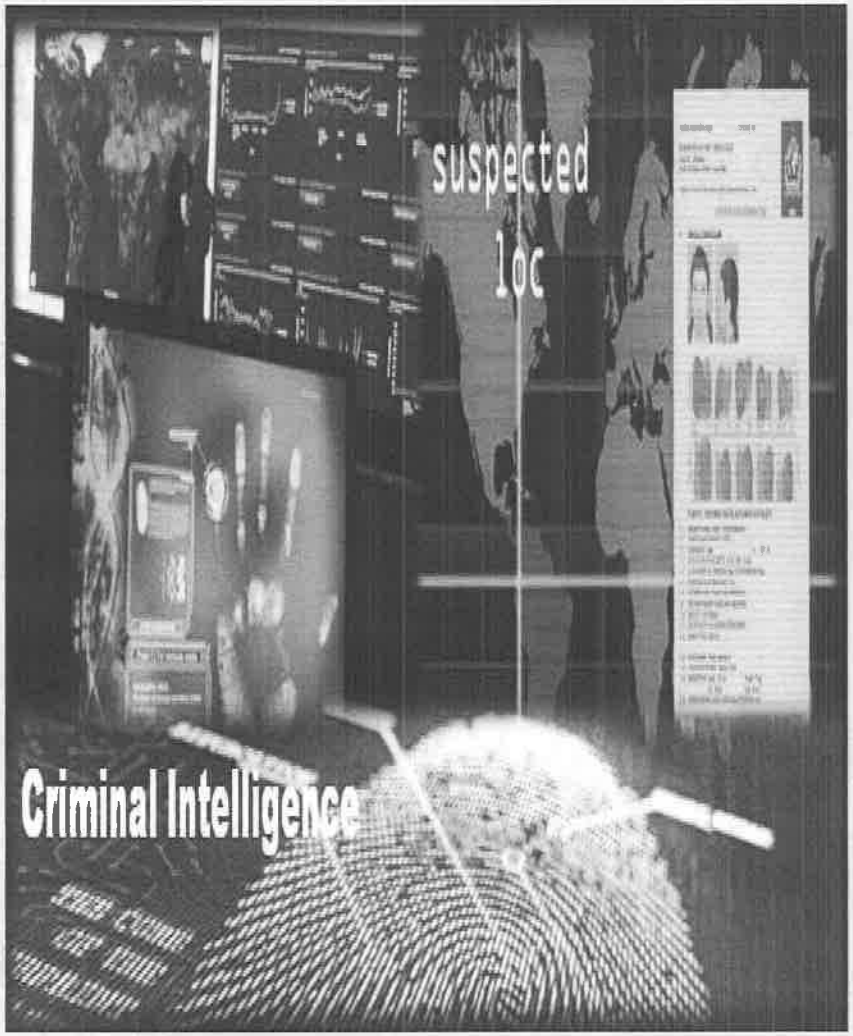
1. The full picture of the criminal groups within the jurisdiction.
2. The #'s, strength, influence, criminal pursuits and possible future activities of criminal groups.

UNDERSTANDING CRIMINAL INTELLIGENCE AND INFORMATION

- **1st – what is "criminal intelligence"?**
  - Information which has been evaluated to determine that it: (1) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity; and (2) meets the submission criteria required by 28 CFR § 23.20(b).

CRIMINAL INTELLIGENCE

- Information;
- Evaluated;
- Relevant to identification of a person or organization;
- And the person or organization is reasonably suspected of involvement in criminal activity.



WHAT IS NOT CRIMINAL INTELLIGENCE

- Criminal investigative reports;
- Case management systems (regardless of whether they are individual or multi-jurisdictional);
- Fingerprint storage and identification systems;
- Criminal History data systems.

WHAT IS 28 CFR & WHY SHOULD YOU CARE

28 CFR § 23 is the United States Code of Federal Regulations section which covers all criminal intelligence systems operating through support under the Omnibus Crime control and Safe Streets Act of 1986 (or any of its amendments).

It is the standard by which all intelligence systems/operations are likely to be judged in a court challenge for protection of civil liberty and privacy protection.

If you have an intelligence system covered by 28 CFR 23 then you should know those rules and procedures.

WSIN (Western States Information Network) and HSIN are covered by 28 CFR 23 rules.

WHAT WILL 28 C.F.R. § 23 BE APPLIED TO?

Criminal Intelligence Systems/Operations that:

Collect and maintain criminal intelligence for the purpose of analysis and multijurisdictional shared dissemination.

REMEMBER THAT EVEN IF 28 CFR DOES NOT APPLY TO YOU...ORS 181.575 DOES

TWO TYPES OF CRIMINAL INTELLIGENCE USE

Tactical Intelligence

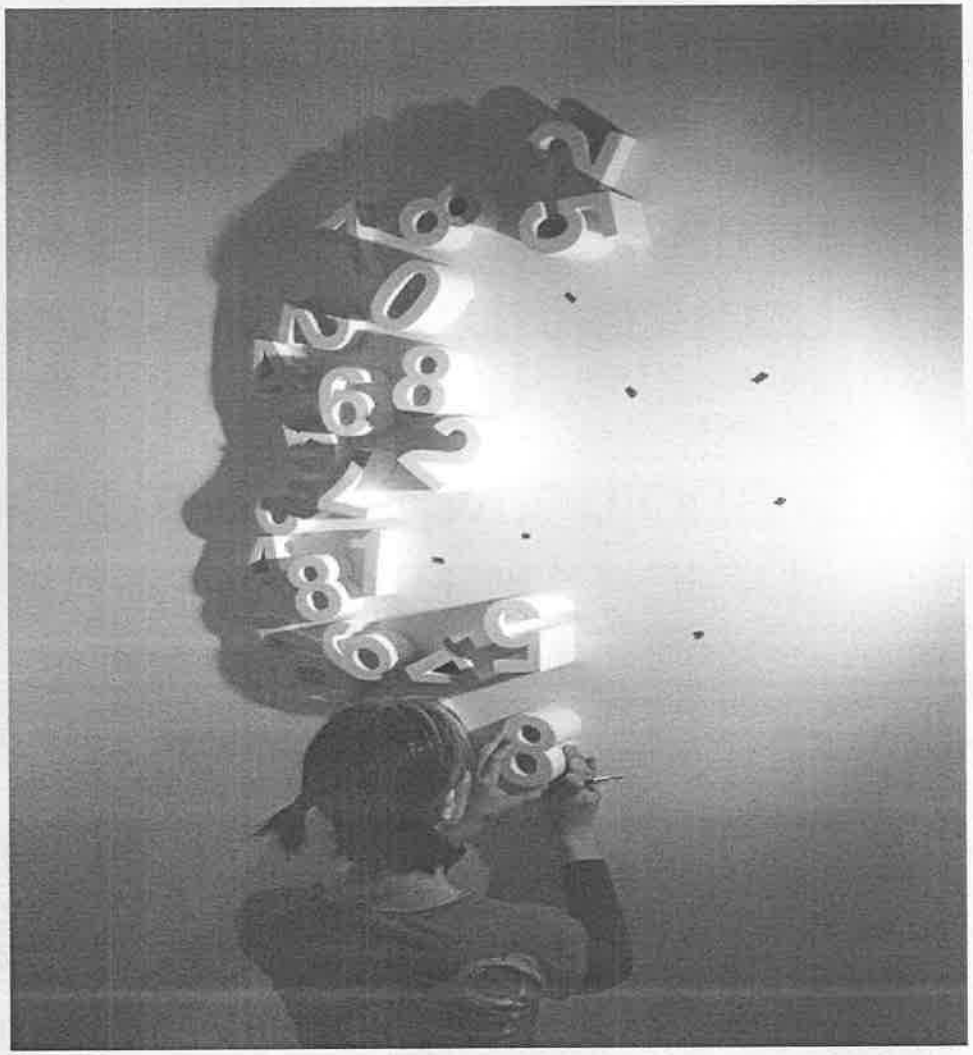
Tactical intelligence is used to develop methods to counteract immediate criminal threats and is usually directed at a specific crime or criminal entity.

Strategic Intelligence

Strategic intelligence provides a broader view of the abilities, strengths, weaknesses, and trends of criminal enterprises. It is an informed judgment on which conclusion are drawn about future criminal endeavors. It is used for long-range planning; enabling LE to make informed decisions on budgets, resources and policy.

TACTICAL AND STRATEGIC INTELLIGENCE

Tactical intelligence can provide the pieces of information that are the building blocks on which intelligence professionals build their strategic analysis.



TACTICAL INTEL SHOULD CREATE INFORMATION FOR STRATEGIC INTEL

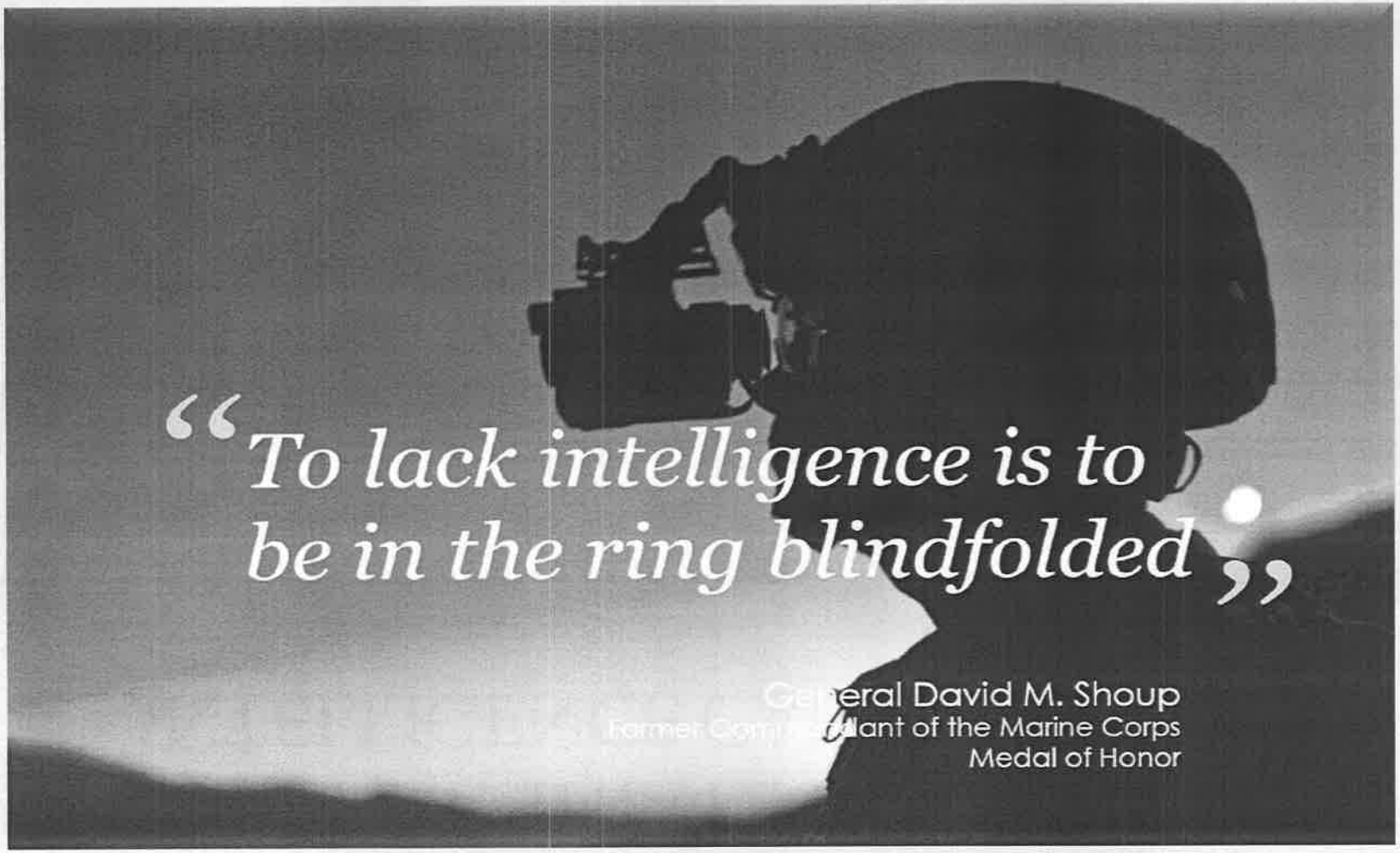
Tactical:

- How does this group package meth?
- How does this group protect stash house?
- How does this group move money?

Strategic:

- Can we find drug groups by unique packaging?
- What risks do stash houses pose for LE?
- How can we intercept drug $$ in transit?

WHY CRIMINAL INTELLIGENCE?

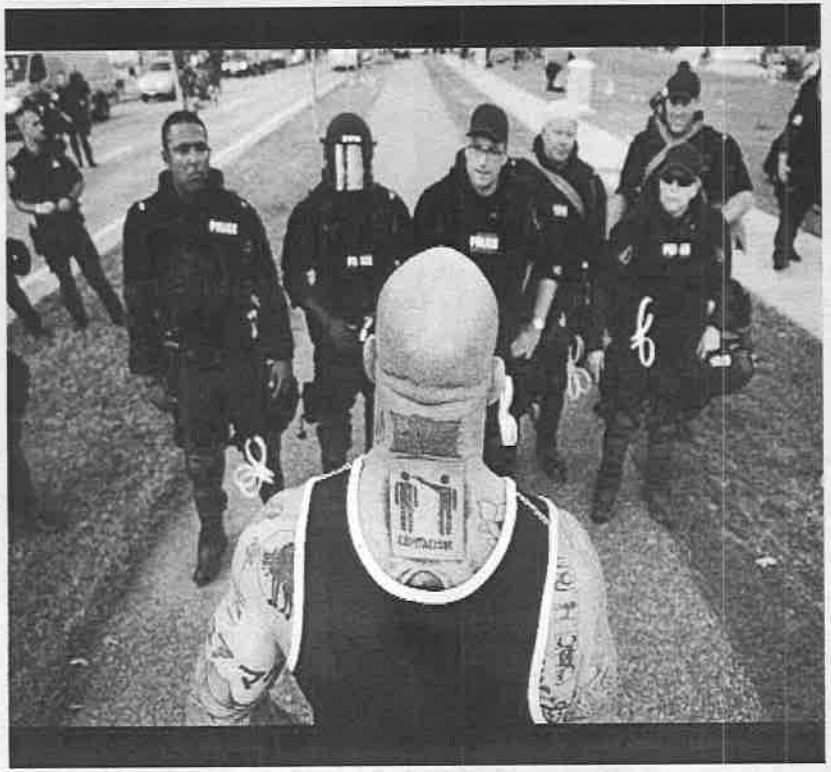


WHAT REAL STRATEGIC CRIMINAL INTELLIGENCE CAN PROVIDE

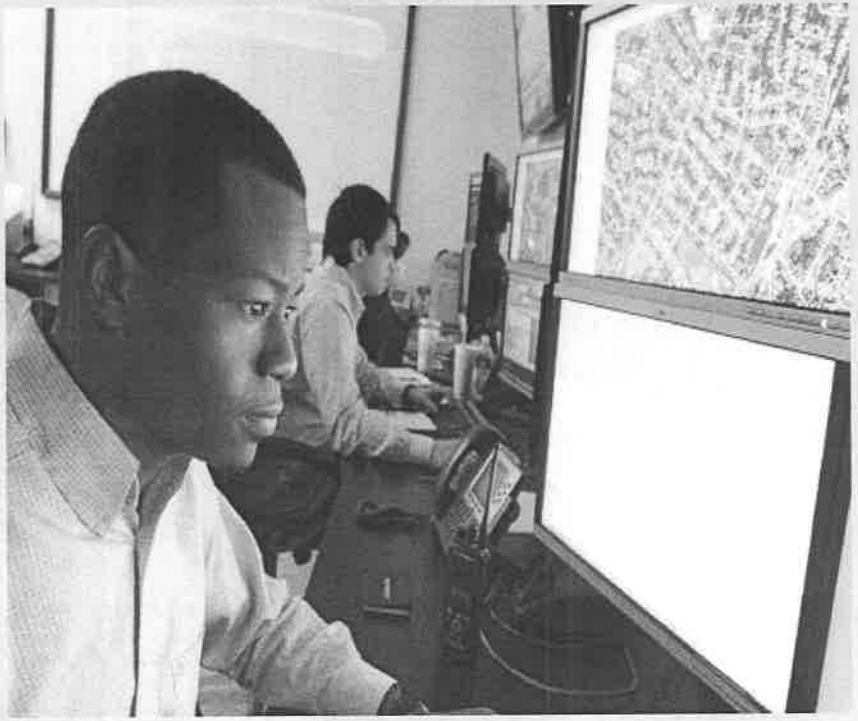
Criminal intelligence provides knowledge that allows law enforcement authorities to **establish a pro-active response to crime.** It enables law enforcement agencies to **identify and understand criminal groups** operating in their areas. Once criminal groups are identified and their habits known, law enforcement authorities may begin to **assess current trends in crime and to forecast**, and possible prevent, future criminal activities. Criminal intelligence also provides the knowledge on which to base decision and **select appropriate targets for investigations.** It also provides law enforcement agencies with the **ability to effectively manage resources**, budget and meet their responsibility to forecast community threats in order to prevent crime.

THE COP AND THE ANALYST
THE CRIMINAL INTELLIGENCE TEAM

Police are the best collectors of information



Analysts Need that information to create intelligence



CRIMINAL INTEL MAINLY LOOKS AT GROUPS, ORGANIZATIONS & ENTITIES

Criminal enterprise?

Criminal enterprise?

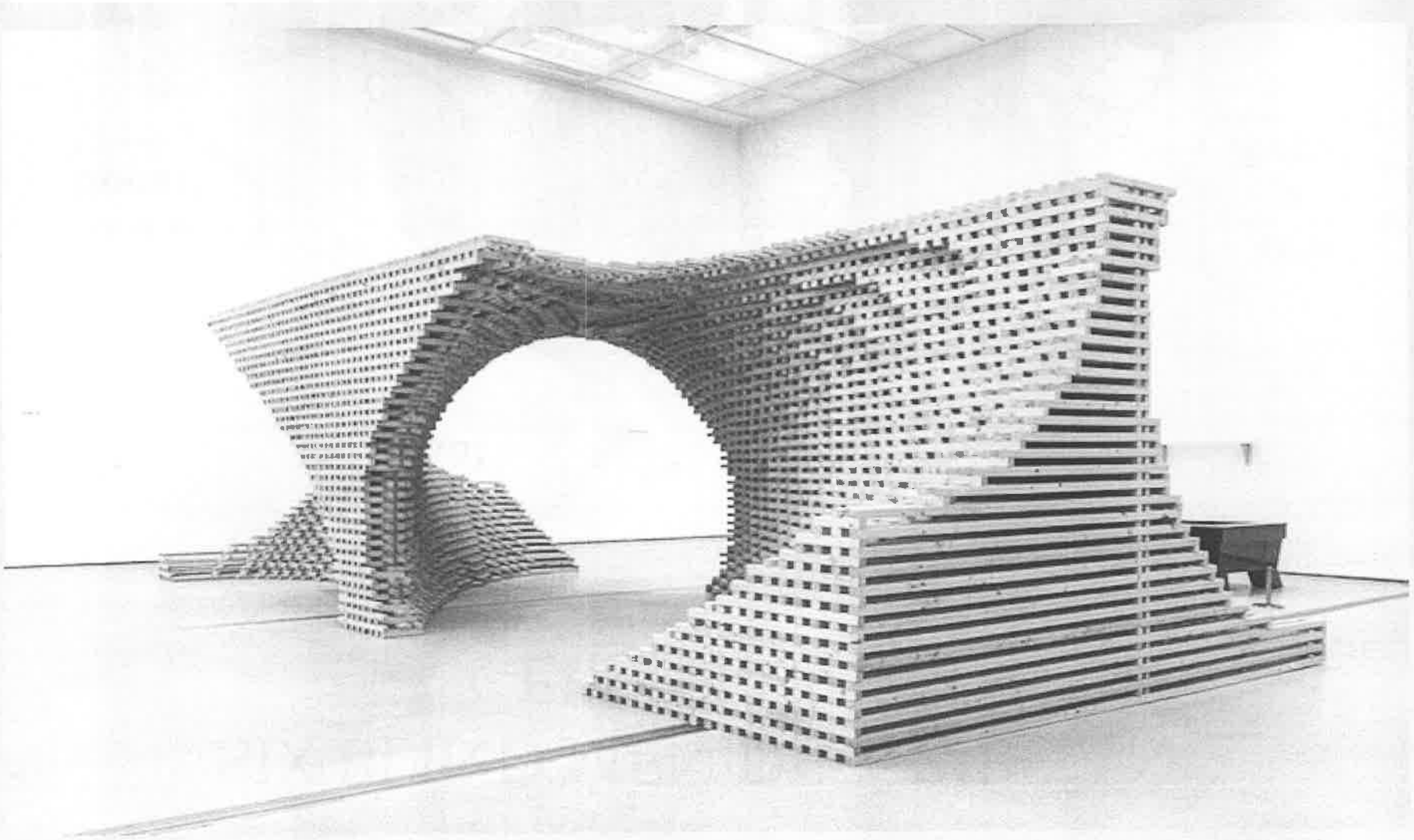
WE DON'T KNOW WHAT WE DON'T KNOW…

- Do Oregon's drug groups use small rural air strips?
- Do Crip and Blood sets take direction from larger East Coast leaders?
- How do Portland gangs get so many guns?
- How large is EK in Oregon?
- How many crimes in Oregon are gang related?
- What parts of the State have the worst ID theft problems?

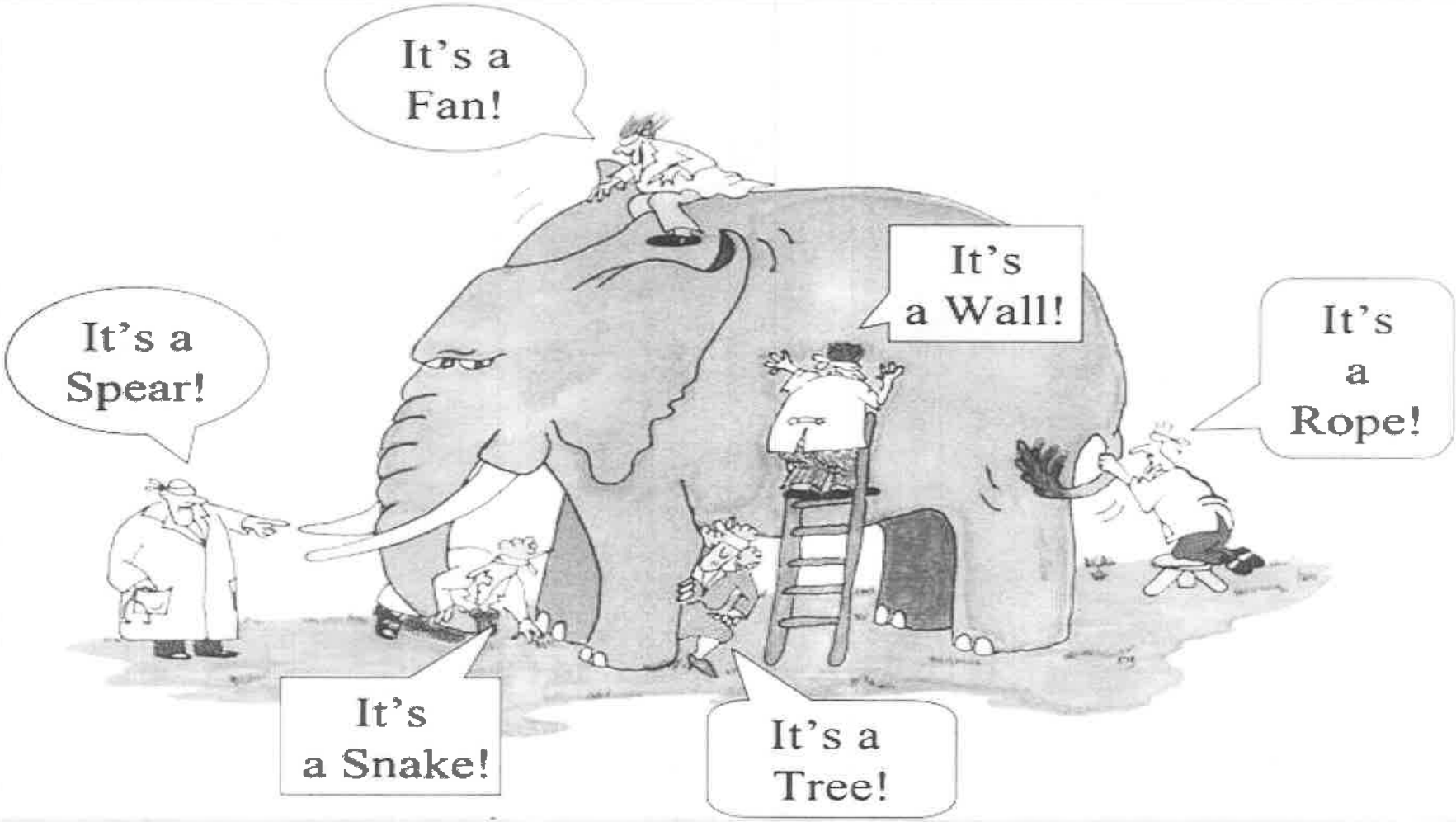
WE DON'T KNOW WHAT WE DON'T KNOW

- Who are the violent anarchists in Oregon and where are they?
- Is ISIS recruiting in Oregon?
- Are Oregon's Sovereign Citizens dangerous?
- Where are white supremacists most active and what are their targets?
- Quantify the danger to Oregon from street gangs.
- What groups in Oregon are the most threatening to critical infrastructure?

THE PROCESS OF TAKING PARTS TO BUILD A WHOLE

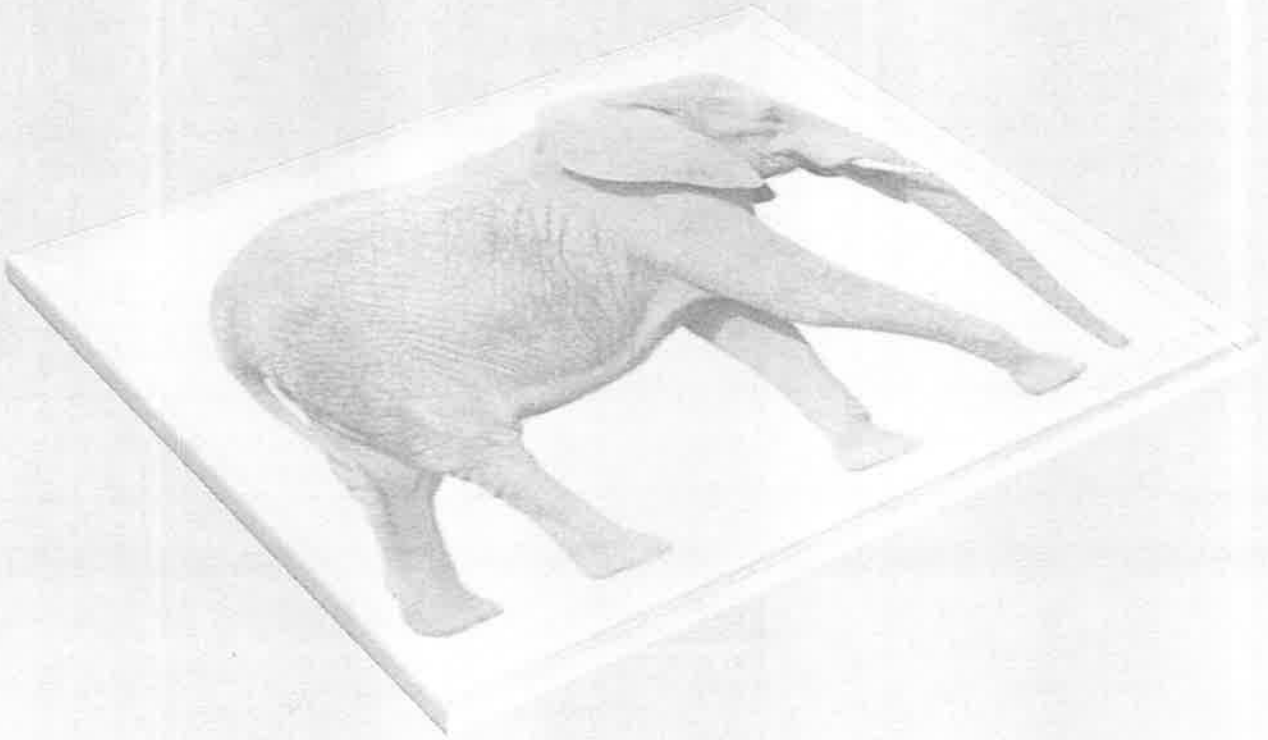


SIX BLIND MEN DESCRIBE AN ELEPHANT



THE GOAL OF CRIMINAL INTELLIGENCE IS TO SEE THE WHOLE AS IT REALLY IS

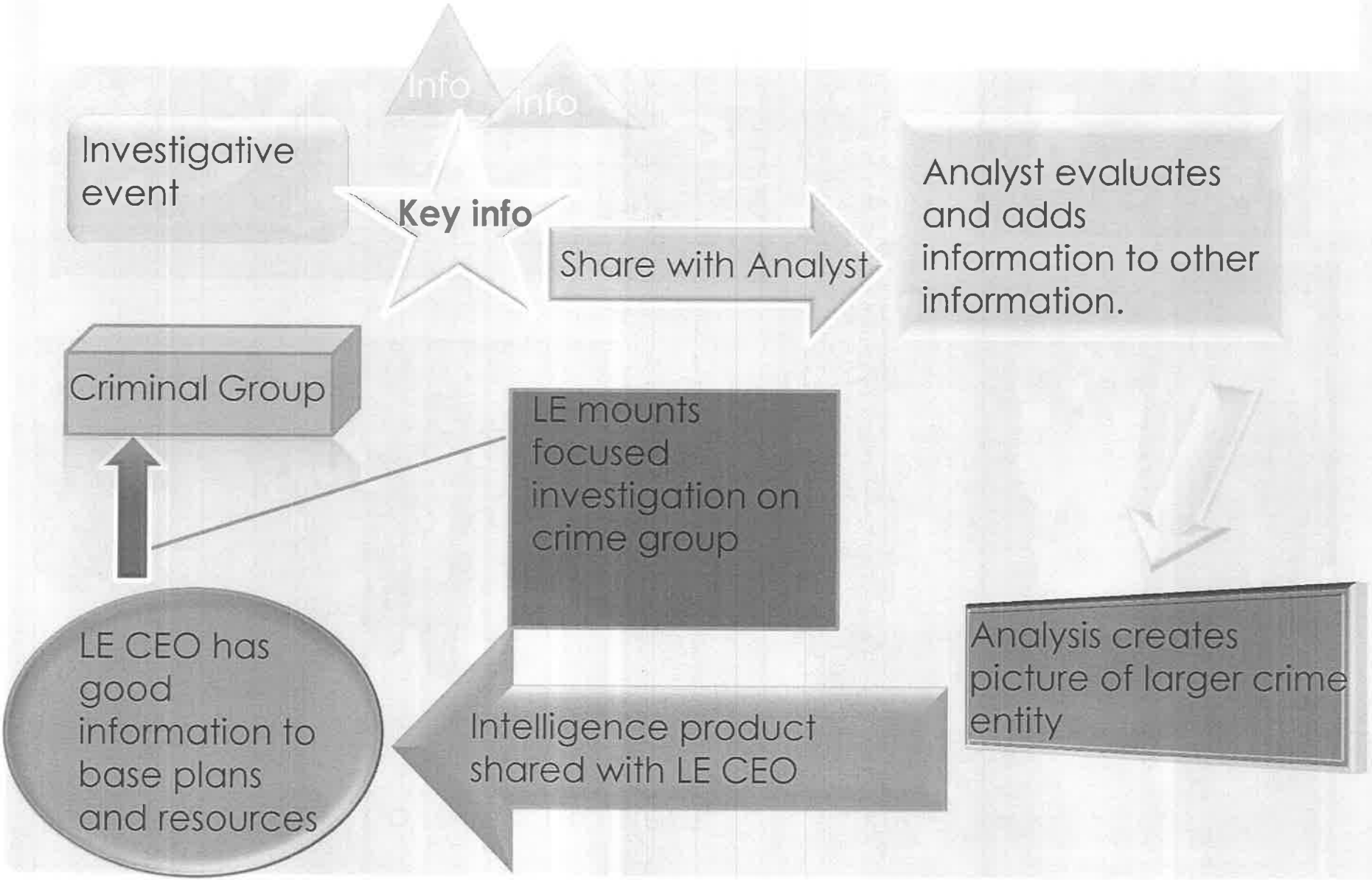
Only through strategic criminal intelligence analysis can you know what you really have to deal with.



Don't have officers deployed for this problem...

When you really have this problem.

LOOK, SEE, UNDERSTAND & SHARE



QUESTIONS?

CONTACT MATT MCCAULEY AT OREGON DOJ BY EMAIL AT MATTHEW.MCCAULEY@DOJ.STATE.OR.US