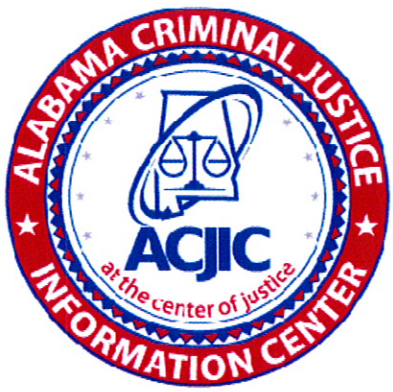
PRIVACY IMPACT ASSESSMENT

FOR THE

BOAT REGISTRATION DECAL QUERY COMPONENT OF THE ALABAMA LAW ENFORCEMENT TACTICAL SYSTEM (LETS)



Contact Point
Becki R. Goggins, Manager
Uniform Crime Reporting Division
Alabama Criminal Justice Information Center
334.517.2451

Reviewing Official
Jeff Matthews, Manager and Chief Security Officer
Information Technology Division
Alabama Criminal Justice Information Center
334.517.2501

Approving Official
Maury Mitchell, Director
Alabama Criminal Justice Information Center
334.517.2410

April 29, 2009

Introduction

In 2002, the Alabama Criminal Justice Information Center (ACJIC) – in cooperation with the Alabama Administrative Office of Courts (AOC) and the Alabama Department of Public Safety (DPS) – began operation of the Law Enforcement Tactical System (LETS). LETS is a secure web portal that allows authorized criminal justice officials to view and query data from approximately

30 separate databases using a single user sign-on and query engine. Since its inception, LETS has been modified and improved to produce an ever-increasing array of search results. LETS has become an important crime fighting tool within the state of Alabama with approximately 20,000 users. The purpose of this document is to provide a Privacy Impact Assessment (PIA) of the data made available through the boat registration decal (Boat Query) within LETS.

Section 1.0 - The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Within the boat query, the following personally identifying information is returned for persons with boats registered in Alabama: name, date of birth and address.

1.2 From whom is the information collected?

All persons who registers a boat (by purchasing a decal) in Alabama.

Section 2.0 - The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

To provide identifying information about boats and persons who have purchased boat registration decals in Alabama.

Section 3.0 - Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The registration information is used to: confirm the identity of persons pulled over in waterway stops, determine the possible identity of criminal suspects, provide identifying information concerning operators of boats to authorized criminal justice personnel, locate owners of recovered boats and identify potential relationship links between various persons based on address details.

Section 4.0 - Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within ACJIC and with other recipients.

4.1 With which internal components of ACJIC is the information shared?

Each division has access to the system, although only users with a "need to know" are authorized access to the system.

Section 5.0 - External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to ACJIC which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-ACJIC) recipient agencies is the information shared?

FBI, U.S. Attorneys, DPS, AOC, Department of Corrections (DOC), Fusion Center, Board of Pardons and Paroles, Department of Conservation, Alcoholic Beverage Control Board, Pharmacy Board, military police, municipal police departments, college police departments, sheriffs' offices, circuit courts, district courts and municipal courts, prosecutors, jails, community corrections agencies and other agencies employing sworn personnel.

Section 6.0 - Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Do individuals have an opportunity and/or right to decline to provide information?

No. All persons who elect to register a boat by purchasing a decal are included within the system. However, it is not mandated that persons have a boat.

6.2 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

No.

Section 7.0 - Individual Access and Redress

The following questions are intended to describe technical safeguards and security measures.

7.1 Which user group(s) will have access to the system?

Assistant district attorneys, state agency heads, information security officers, military investigators, corrections officers, district attorneys, judges, court clerks, dispatchers, field agents, fusion center personnel, probation officers, police officers, and sheriffs' deputies

Section 8.0 - Technical Access and Security

8.2 Will contractors to the ACJIC have access to the system? If so, please describe their role.

Yes. ACJIC is assisted by contractual developers who act as agents for ACJIC for the purposes of enhancing LETS. Their access is strictly limited to testing modifications to the LETS user interface and search services. Additionally, all developers must sign a confidentiality agreement with ACJIC and are required to submit to a fingerprint-based background check prior to being allowed access to the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes.

8.4 What procedures are in place to determine which users may access the system and are they documented?

ACJIC has implemented the Active Directory Authentication and Processing Tool (ADAPT) application to assign and manage user access. ADAPT allows privileges to be assigned based on a user's role within his or her agency (e.g. detective v. jail administrator). Privileges may also be added or removed on an individual basis. Each user agency is responsible for assigning an Agency Information Security Officer (AISO) who is responsible for user management within their agency.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

ACJIC's staff and developers routinely test the ADAPT system to ensure that privileges are being assigned correctly via the application. Additionally, ACJIC employs two full-time auditors. Their responsibilities include monitoring LETS usage to make sure only those authorized to access the system are doing so. Finally, ACJIC's Field Agents also work with agencies to ensure compliance with laws, rules and regulations governing access to the system.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

LETS generates an auditing report every 90 days which is reviewed by ACJIC's Field Agents. In the event it appears that a suspicious number of queries have been performed by a user or an agency, further investigation may be warranted. This report also gives a record of all transactions that can be randomly sampled to determine whether the searches performed were authorized for a legitimate criminal justice activity.

AISOs are required to validate all users associated with their agency to ensure that only active employees with appropriately assigned privileges are granted access to the system. To ensure that the monthly user validation occurs, the system automatically notifies the AISO that the validation needs to be performed. Failure to promptly validate users will result in suspension or termination of LETS privileges for the agency.

The system also supports ad hoc queries to determine if persons are misusing the system. For instance, the Field Services Division will periodically check to see if searches are being performed on famous entertainers or political figures in Alabama. In the event it is determined that users are querying the system to check out the driver's license photos or obtain other information about a person merely out of curiosity, the user may face administrative or criminal sanctions for misuse.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All AISOs are required to attend ACJIC-sponsored classed prior to becoming an AISO. During this class, instructors provide details on the permissible uses of LETS. Included in the training is information about how all transactions are logged so they can be reviewed by ACJIC auditors or investigative staff in the event misuse is suspected. AISO's are expected to inform departmental personnel about appropriate use of ACJIC systems. Beginning in 2009, ACJIC will add a special segment on privacy to its ongoing AISO classes.

8.8 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Since the boat registration information is available to thousands of criminal justice users via the internet, it is always possible that a person's privacy might be compromised through misuse of the system. However, ACJIC has taken great pains to ensure that every transaction is monitored and recorded. This gives ACJIC the ability to identify persons who perform illegal queries in the event there is a complaint.

ACJIC auditors and Field Agents periodically review transaction reports to identify individuals and/or agencies that are running an unusually high volume of queries. They also match the times queries are run against the known work hours of individuals suspected of misuse. For instance, inquiries performed under a user's account when he or she is off duty can be an indication of misuse.

ACJIC also requires all agencies to sign an Agency Access Agreement that explains proper usage of the system and provides detailed information concerning civil and criminal penalties for misusing ACJIC applications. Additionally, the ACJIC Security Policy requires all agencies with access to ACJIC to meet rigid technical security standards which are evaluated periodically as a part of their technical audits. The Security Policy also defines additional policies related to privacy and the protection of confidential information.

Conclusion

The primary goal of making the boat registration available through the LETS portal is to provide criminal justice personnel with an accurate, reliable and convenient method for establishing the identity of subjects. To this end, the program has been very successful. While potential threats to privacy have been identified, ACJIC has taken significant steps to mitigate these possibilities.

Responsible Official Signatures

Jeff Matthews, Information Security Officer

Maury Mitchell, ACJIC Director