Northern California Regional Intelligence Center
Initial Privacy Impact Assessment for
Automated License Plate Reader Technology

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens of the fifteen Bay Area counties within its area of responsibility from the threat of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

Fundamental to carrying out the NCRIC's responsibilities is doing so in a way that effectively protects the privacy and civil liberties of individuals and the security and confidentiality of sensitive information. To that end, and although not required by law to do so, the NCRIC has developed this initial Privacy Impact Assessment (PIA) for use, analysis, dissemination, retention, and destruction of data derived from the operation of NCRIC Automated License Plate Readers (ALPR) and ALPR systems of our partner law enforcement entities (ALPR Data).

In addition, the NCRIC has initiated development of, and will continue to refine, specific policy and guidelines for the use, analysis, dissemination, retention, and destruction of ALPR Data at the NCRIC (NCRIC ALPR Policy). To the greatest extent feasible, the NCRIC ALPR Policy will be made publicly available for review and comment.

Scope of this Initial Privacy Impact Assessment

This Privacy Impact Assessment applies to ALPR Data collected by the NCRIC and NCRIC partner agencies and shared with other regional law enforcement agencies, accessed, and analyzed using software hosted by the NCRIC. It is not intended to apply, and does not apply, to any other types of data accessed or used at the NCRIC or to any collection, use, or handling of any data at individual NCRIC member or contributing entities.

Use and Efficacy of Automated License Plate Reader Data

Automated License Plate Reader Technology

ALPR systems function to automatically capture an image of a vehicle's license plate, transform that image into alphanumeric characters using optical character recognition software, and store that information along with relevant metadata (i.e., geo-location and temporal information, as well as data about the ALPR unit).

At the NCRIC, such ALPR Data is accessed and analyzed using customized software to enable:

- Searches of full plates, with full color pictures of identified vehicles for plate read verification;
- Partial plate searches that return possible matches to assist in identifying suspects' vehicles;
- Geo-spatial searches of ALPR Data to assist in identifying possible suspects' vehicles in cases where other vehicle identification information exists;
- Creation of alert mechanisms for identification of license plates associated with, for example, active criminal investigations, Amber Alerts, and/or other authorized law enforcement and public safety purposes; and
- Use of these search capabilities across ALPR Data from contributing NCRIC member entities within a single interface and subject to the use, analysis, retention, destruction, sharing, and disclosure restrictions of the NCRIC and of the entities contributing the ALPR Data.

Adoption and Efficacy of ALPR Technology

More than 70% of U.S. police agencies surveyed in 2012 indicated that they are using ALPR technology.[1] Police agencies around the country have reported notable successes using ALPR technology in identifying suspects in domestic kidnappings, solving homicide cases, support for bomb detection units, reducing auto theft, and stolen vehicle recovery.[2]

Privacy and Civil Liberties Implications of ALPR Data

To date, United States courts and federal and state legal authorities have not found a legitimate expectation of privacy for individuals in ALPR Data and, as of the date of this initial PIA, no federal or California statutes applicable to the NCRIC or its partner agencies regulate the use of such data. Nonetheless, the NCRIC recognizes that the benefits to public safety of the effective use of ALPR Data by law enforcement are tempered by the risks posed by inadvertent or intentional misuse of such data to

[1] *How Innovations in Technology are Transforming Policing*, Police Executive Research Forum, 2012, at 1 (http://policeforum.org/library/critical-issues-in-policing-series/Technology_web2.pdf)
[2] *Id.* at 28-32.

individual privacy and civil liberties, and, more broadly, to the fundamental freedoms that make our society strong.[3]

Potential Individual Privacy and Civil Liberties Harms

Identification of Individuals. Although ALPR Data, by itself, does not identify individuals by name or provide other personal information, a license plate number can be used to determine the registered owner, and information about that person from, for example, state motor vehicle data. However, images taken by ALPR cameras may at times inadvertently include more information than just a license plate number. If misused, such information could result in harm to individuals, including but not limited to: assumptions about an individual's behavior or associations, personal agendas of individuals accessing the data, or furthering government objectives that are legitimate but beyond the permissible scope for which access to such data was authorized.

Misidentification. Without careful, rigorous, and technically-controlled access and use of ALPR Data, significant risks of individuals being misidentified as criminal suspects can arise.

Data Quality and Accuracy Issues. Related to misidentification are the challenges of data quality and accuracy. If ALPR Data associated with individuals and information analyzed along with such data is not kept up to date and accurate, governmental action may be improperly taken against such individuals and unwarranted investigative assumptions may be made.

Non-relevant data. Data regarding a vehicle's location – particularly when collected over an extended period of time – could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities. By precisely and proportionally limiting access to ALPR Data, the risks of such misuse can be reduced and the likelihood of inferring protected/non-relevant character attributions can be minimized.

These, of course, are not the only potential individual privacy and civil liberties harms from misuse of ALPR Data. Such potential harms have been widely discussed in recent years, including in the 2009 ALPR Privacy Impact Assessment produced by the International Association of Chiefs of Police, and resources cited therein, and by the American Civil Liberties Union.[4]

---

[3] Such concerns have been reflected in recent judicial and legislative activities. *See, e.g., United States v. Jones* (quoted below); California Senate Bill 1330. A right to privacy is explicitly enshrined in Section 1 of the California Constitution.

[4] http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87 (This "Privacy impact assessment report for the utilization of license plate readers," published by the

Potential Societal Harms

Perhaps of even greater long-term concern than the risks to individual privacy and civil liberties harms discussed above, which are inherent in any governmental access, use, and storage of information about individuals, are the emerging risks to our societal values themselves. The American Civil Liberties Union has warned, for example, that as ALPR Data becomes more voluminous and analysis of that data more powerful, there is a risk to society that ALPR Data could cease "to be simply a mechanism enabling efficient police work and [become] a warrantless tracking tool, enabling retroactive surveillance of millions of people."[5]

In the landmark 2012 United States Supreme Court decision in *US v. Jones*, Justice Alito discussed historical expectations of society with regard to government surveillance of our movements:

> Society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[6]

The ACLU and others have expressed concern that ALPR systems potentially pose similar risks, particularly if deployed and used on a mass scale and pervasively across jurisdictional boundaries.[7] Not only actual government surveillance, but perceived government surveillance as well, can have a chilling effect on Americans' protected rights of free expression, free association, protest, political participation, and even our right to visit locations which some might find controversial or embarrassing.

Protecting Privacy and Civil Liberties

The NCRIC ALPR Policy, and the deployment of access control, auditing, revisioning, and data correction and purging technologies, applied to the privacy and civil liberties concerns articulated herein, will provide increased protection for data currency and accuracy, thereby helping to mitigate risks of misidentification, misuse of non-relevant information, and poor data quality. Concepts of proportionality, authorized use, accountability, and other policy and technical controls, will be incorporated, to deter,

---

International Association of Chiefs of Police, served as a primary information source for this Initial NCRIC PIA) (http://www.aclu.org/blog/tag/license-plate-scanners)

[5] American Civil Liberties Union of Iowa website discussion of Automatic License Plate Readers (ALPRs) in Iowa (http://www.aclu-ia.org/automatic-license-plate-readers-aplrs-in-iowa/)

[6] *United States v. Jones* 132 S.Ct. 945, 964 (2012).

[7] *See, e.g.,* "You Are Being Tracked. How License Plate Readers Are Being Used to Record Americans' Movements." American Civil Liberties Union, New York, NY, July 2013, (http://www.aclu.org/alpr)

detect, and control against misuse of ALPR Data reasonably likely to implicate these types of societal concerns.

Privacy and Civil Liberties Protections for NCRIC ALPR Data

Although extensive privacy policies already are in place, the NCRIC recognizes that ALPR Data has unique attributes that must be addressed through additional measures.

From its inception, the NCRIC has taken the issue of privacy and civil liberties seriously. To that end, the NCRIC follows the Information Privacy Policy adopted by the California State Terrorism Threat Assessment System (STTAS Privacy Policy)[8], which includes one State Fusion Center, four Regional Threat Assessment Centers and one Major Urban Area Fusion Center. The STTAS Privacy Policy was developed primarily to address the use and handling of criminal intelligence and related information as governed by 28 C.F.R. Part 23, the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files, and other applicable legal authorities.

To the extent individual elements of the STTAS Privacy Policy are applicable to ALPR Data, the NCRIC will adapt these elements to its handling of such data.

The NCRIC recognizes, however, that the use of ALPR and other locational data may, in some cases, present privacy and civil liberties challenges and protective requirements different from those addressed in the STTAS Privacy Policy and, as appropriate, the NCRIC will develop and implement additional protections. In addition, the NCRIC will adapt, to the extent reasonably feasible, the Fair Information Principles described in the STTAS Privacy Policy to the handling of ALPR Data. These principles include:

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

Compliance with Applicable Law

As a threshold matter, and as mandated by the STTAS Privacy Policy, the NCRIC, and all

[8] As of the date of release of this document, the "STTAS Privacy Policy" title has not yet been revised to reflect the renaming from State Terrorism Threat Assessment System (STTAS) to State Threat Assessment System. Hence, all references to the policy preserve the "STTAS" acronym, while references to the organization use the modified "STAS" acronym.

assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in the NCRIC or any other STTAS Component, shall comply with all applicable laws protecting privacy, civil rights, and civil liberties.

Use for Authorized Law Enforcement and Public Safety Purposes Only

ALPR Data will be used only for authorized law enforcement and public safety purposes. Approved users are authorized to access ALPR Data to:

- Locate stolen, wanted, and subject of investigation vehicles;
- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;
- Locate witnesses and victims of violent crime;
- Locate missing children and elderly individuals, including responding to Amber and Silver Alerts;
- Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;
- Protect participants at special events; and
- Protect critical infrastructure sites.

Consistent with the NCRIC ALPR Policy to be further developed over the coming months, information sharing, access control, and use control technology will be utilized to: (1) record and audit the authorized use for which ALPR Data is being accessed or used in each instance; and (2) incorporate measures designed to prevent attempted access or use of ALPR Data for non-authorized purposes.

Collection of ALPR Data

NCRIC receives ALPR Data from its partner entities, but also operates a limited number of ALPR units. Such NCRIC ALPR units may be used to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

Dissemination, Secondary Uses, and Commercial/Private Entity Data Sharing

NCRIC ALPR Data will be disseminated only to authorized law enforcement or public safety officials with proper authority, for authorized purposes, and as consistent with standing Memoranda of Understanding (MOUs) or as otherwise authorized by source agencies. The NCRIC ALPR Policy will incorporate controls on secondary uses of ALPR Data. Information sharing, access control, and use control technology will be utilized to enforce and audit these requirements.

ALPR Data may be shared with owners or operators of critical infrastructure locations in circumstances where reasonable evidence suggests the location is the target of a terrorist attack or other criminal activity.

Except as noted above with regard to critical infrastructure, the NCRIC will not share NCRIC or partner agency ALPR Data with commercial or other private entities or individuals.

Safeguarding and Protecting ALPR Data

The NCRIC will take all reasonable physical, technological, administrative, procedural, and personnel measures to protect the confidentiality and integrity of ALPR Data, whether in storage or in transit.

Data Quality and Accuracy

The NCRIC will take all reasonable measures to ensure that ALPR Data is accurate and up-to-date. When errors are discovered, corrections will be made promptly and reasonable efforts will be taken to identify, locate, and update information that has been shared with other entities pursuant to the dissemination policy.

Data Vetting and Decision Making

The NCRIC ALPR Policy will establish policies and guidelines requiring human evaluation and verification in determining the relevance of license plate data to an active investigation or other authorized law enforcement or public safety effort. To the greatest extent feasible, ALPR data utilized in investigations will be corroborated by other information prior to using such data as the basis for subsequent law enforcement action.

Data Retention and Destruction

While continuing to refine its ALPR Policy, the NCRIC will incorporate reasonably feasible procedural and technological measures to enforce data retention and destruction requirements imposed by the originators of data received and electronically stored by the NCRIC. The NCRIC will collect and analyze empirical data to support an evaluation of reasonable retention standards for ALPR Data. During this period of analysis, the NCRIC will adopt a default, system-wide, one-year retention standard under which ALPR Data received from contributing agencies will be purged. Under these standards, if such data does not meet established retention requirements based on relevance to an ongoing criminal investigation (for which other retention standards may apply), it will be removed entirely from NCRIC databases.

Utilizing data gathered over the next year to evaluate the use and efficacy of ALPR Data, and based on consultations with privacy and civil liberties experts, the NCRIC will continue to develop and refine specific ALPR data retention and destruction policies, with additional restrictions applied based upon the intended authorized use. For example, further restrictions on temporal, geospatial, relational, and other factors may be implemented.

According to a recent survey,[9] albeit with a relatively small number of voluntarily responsive agencies, retention periods for ALPR Data vary widely, from none to infinite, with 46% retaining ALPR Data for one year or less, 13% between two and five years, and 14% indefinitely. Utilizing sophisticated analytic software, the NCRIC will consider, in consultation with member entities, the efficacy of ALPR Data of various ages in determining its data retention and destruction requirements.

Training and Non-Disclosure Obligations of NCRIC Personnel

All personnel with access to NCRIC ALPR Data will be provided with appropriate training, including privacy and security training, and will be required to sign non-disclosure agreements with regard to ALPR Data, as well as other information to which they will have access at NCRIC.

Auditing and Accountability

All NCRIC personnel with access to ALPR Data will be responsible for strict compliance with the NCRIC ALPR Policy, and all other applicable legal, regulatory, and policy requirements. The NCRIC will employ auditing technologies to enable tracking of, and accountability for, individual NCRIC participant actions to access, use, disseminate, retain, and/or destroy ALPR Data. Violations of applicable requirements will result in appropriate disciplinary action, including, if appropriate, denial of additional access to NCRIC facilities and data.

Updates and Revisions to the NCRIC ALPR PIA

This is an initial Privacy Impact Assessment only. It will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing, and other relevant considerations. Additionally, updates to this Privacy Impact Assessment may be used to inform continued refinements to the NCRIC ALPR Policy.

---

[9] *ALPR Systems Policy Operational Guidance for Law Enforcement,* International Association of Chiefs of Police, 2012, at 29 (http://www.theiacp.org/portals/0/pdfs/IACP_ALPR_Policy_Operational_Guidance.pdf)