

Northern California Regional Intelligence Center Initial Privacy Impact Assessment for The Use of Facial Recognition Software

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 Facial Recognition software through FERET (Facial Recognition Technology) System.

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 Facial Recognition data at the NCRIC (NCRIC Facial Recognition Policy).

Scope of this Initial Privacy Impact Assessment

This Privacy Impact Assessment applies to Facial Recognition Use and Data collected by the NCRIC and NCRIC partner agencies and analyzed using software hosted by the Western States Information Network (WSIN). 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 Facial Recognition Systems

Facial Recognition Use

The FERET System provides investigative lead support to FBI field offices, operational divisions, and legal attachés by comparing the facial images of persons associated with open assessments and investigations against facial images available in state and federal face recognition systems. In its support of our approved partners and with a valid "right-to-know" and "need to know", FERET accepts unclassified photographs of subjects of, and persons relevant to, open assessments and investigations. These photographs are called "probe photos." FERET only accepts probe photos that have been collected pursuant to

applicable legal authorities as part of an authorized investigation. Upon receipt of a probe photo, FERET uses face recognition software to compare the probe photo against photos contained within government systems.

After comparison and evaluation, which includes both automated face recognition software and manual review by a trained biometric images specialist, FERET may identify photos that are likely matches to the probe photo. These photos are called “candidate photos” because they serve only as investigative leads. Unlike fingerprints, face recognition results do not constitute positive identification of an individual. Textual data that accompanies probe photos are searched against other databases. In many instances, no candidates are returned. If a likely candidate is found in one of these systems, FERET generally confirms with the record owner that the record is valid and active and requests permission to disseminate the information.

FERET maintains a Work Log in which it retains the Image Search Requests received from the approved partner. These Image Search Requests generally include the name of the requesting agent, the case number, and some biographic information related to the subject of the probe photo, such as name and date of birth. The Work Log also serves as a workflow management tool for FERET and, as such, documents all work transactions. Information may include the analyst assigned to the case, general comments, dates when probe photo information was added and/or modified, dates and types of search conducted, and disposition of the FERET analysis. Notably, FERET maintains only the probe photos and limited biographic information in the FERET Services Work Log. FERET performs “deconfliction” of the probe photos maintained in the Work Log, meaning that it compares the photos against one another to determine if the same person appears in multiple investigations. If so, the relevant case agents will be informed. Access to the Work Log is limited FERET Analysts and other authorized personnel who require the information for performance of their official duties.

By using face recognition technology to search probe photos for matching candidate photos, FERET provides unique and specialized value to the NCRIC’s mission to provide support to their Law Enforcement partners. In many instances, face recognition results in information that is not available with any other investigative method.

Adoption and Efficacy of the Use of Facial Recognition Technology

Cities across the United States from Orlando to Oregon were surveyed in 2014 who indicated that they are using Facial Recognition technology as a tool in investigations. Police agencies around the country have reported notable successes using Facial Recognition technology in the successful identifying of wanted criminals. The FBI located and arrested a fleeing child abuse and kidnapping suspect in Nepal, while the Sacramento California Sheriff’s Office identified an individual wanted for Homicide. NYPD has

conducted over 8,500 facial recognition, which has led to 3,000 possible matches and almost 2,000 arrests¹.

Privacy and Civil Liberties Implications of the Use of Facial Recognition Technology

To date, United States courts and federal and state legal authorities have not found a legitimate expectation of privacy for individuals in Facial Recognition usage 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. However, the Florida First District of Appeal is deciding whether the use of facial recognition technology used in a drug arrest was sufficient for conviction². Nonetheless, the NCRIC recognizes that the benefits to public safety of the effective use of FERET by law enforcement are tempered by anticipated public concerns about potential risks posed -- by inadvertent or intentional misuse of such data -- to individual privacy and civil liberties, and, more broadly, to the fundamental freedoms that make our society strong.³

Potential Individual Privacy and Civil Liberties Concerns

Identification of Individuals. Although Open Source Social Media Data, by itself, does not necessarily identify individuals by name or provide other personal information, social media content, including real names, photos, geolocation and associate information can sometimes be used to determine the identity of an individual. If misused, such information could result in undesired effects on 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 Facial Recognition databases, it is possible that individuals could be misidentified as criminal suspects.

Data Quality and Accuracy Issues. Related to misidentification are the challenges of data quality and accuracy. If Facial Recognition databases 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.

Potential Societal Harms

¹ <http://www.policemag.com/channel/technology/articles/2016/11/facial-recognition-comes-of-age.aspx>;

² <https://statescoop.com/upcoming-facial-recognition-case-ruling-to-set-precedent-for-law-enforcement>

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.

Perhaps of even greater long-term concern than the risks to individual privacy and civil liberties 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 Open Source Social Media Data becomes accessible to law enforcement, there is a risk to society that the tools open the door for abuses of power and it has been observed “the way to solve crimes is to go after people who are suspected of specific criminal acts, not spying on the general public”⁴ and in the 2014 United States Supreme Court heard case *Elonis v. US*, Justice Elena Kagan expressed concern about the potential chilling of legitimate free speech.⁵ These same concerns can be applied to Facial Recognition Data and its usage.

Protecting Privacy and Civil Liberties

The NCRIC Facial Recognition 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, detect, and control against misuse of Facial Recognition Data reasonably likely to implicate these types of societal concerns.

Privacy and Civil Liberties Protections for NCRIC Facial Recognition Data

Although extensive privacy policies already are in place, the NCRIC recognizes that Facial Recognition 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 Threat Assessment System (STAS Privacy Policy), which includes one State Fusion Center, four Regional Threat Assessment Centers and one Major Urban Area Fusion Center. The STAS 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.

⁴ [http://www.lowellsun.com/todayshadlines/ci_27581830/aclu-questions-possible-purchase-online-monitoring-service-by#ixzz3TH0JtE10.](http://www.lowellsun.com/todayshadlines/ci_27581830/aclu-questions-possible-purchase-online-monitoring-service-by#ixzz3TH0JtE10)”

⁵ <http://www.csmonitor.com/USA/Justice/2014/1201/Are-Facebook-rants-threats-or-free-speech-Supreme-Court-takes-up-case.-video>

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

The NCRIC recognizes, however, that the use of Facial Recognition Data may, in some cases, present privacy and civil liberties challenges and protective requirements different from those addressed in the STAS 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 STAS Privacy Policy to the handling of Facial recognition 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 STAS Privacy Policy, the NCRIC, and all assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in the NCRIC or any other STAS Component, shall comply with all applicable laws protecting privacy, civil rights, and civil liberties.

Use for Authorized Law Enforcement and Public Safety Purposes Only

FERET Data will be used only for authorized law enforcement and public safety purposes. Approved users are authorized to access Facial Recognition Data to include but not limited to:

- Locate individuals subject to arrest or otherwise lawfully sought by law enforcement;
- Locate missing or wanted persons sought by law enforcement;
- Locate witnesses of a criminal investigation;
- Locate missing or stolen goods
- Support local, state, federal, and tribal public safety department in the identification of targets of ongoing criminal investigations;
- Provide information to organizers and public safety officials during public events to ensure the safety of the public; and
- Protect critical infrastructure sites.

Consistent with the NCRIC Facial Recognition Policy, information sharing, access control, and use control technology will be utilized to: (1) record and audit the authorized use for

which Facial Recognition Data is being accessed or used in each instance; and (2) incorporate measures designed to prevent attempted access or use of Facial Recognition Data for non-authorized purposes.

Collection of Facial Recognition Data

NCRIC receives Facial Recognition Data from its partner entities, but also utilizes Facial Recognition search tools to collect data 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 Facial Recognition Data will be disseminated only to authorized law enforcement or public safety officials with proper authority, and for authorized purposes. Information sharing, access control, and use control technology will be utilized to enforce and audit these requirements.

Facial Recognition 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 Facial Recognition Data with commercial or other private entities or individuals.

Safeguarding and Protecting Facial Recognition Data

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

Data Quality and Accuracy

The NCRIC will take all reasonable measures to ensure that Facial Recognition 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 Facial Recognition Policy will establish policies and guidelines requiring human evaluation and verification in determining the relevance of Facial Recognition Data to an

active investigation or other authorized law enforcement or public safety effort. To the greatest extent feasible, Facial Recognition 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

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 Facial Recognition Data. During this period of analysis, the NCRIC will adopt a default, system-wide, one-year retention standard under which Facial Recognition Data will be purged, which is consistent with the California Attorney General Guidelines for data retention. 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 Facial Recognition Data, and based on consultations with privacy and civil liberties experts, the NCRIC will continue to develop and refine specific Facial Recognition 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.

Utilizing guidance from the California State Legislature, the passage of AB1442 (Social Media Privacy) calls for the school districts who utilize social media monitoring tools to “(3) (A) Destroy information gathered from social media and maintained in its records within one year after a pupil turns 18 years of age or within one year after the pupil is no longer enrolled in the school district, county office of education, or charter school, whichever occurs first.”⁶ The NCRIC will adhere to these same guidelines as it pertains to Facial Recognition Data.

Training Obligations of NCRIC Personnel

All personnel with access to NCRIC Facial Recognition Data will be provided with appropriate training, including privacy and security training.

6

http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442

Auditing and Accountability

All NCRIC personnel with access to Facial Recognition Data will be responsible for strict compliance with the NCRIC Facial Recognition 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 Facial Recognition 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 Facial Recognition 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 Facial Recognition Policy.