NACDL
FOURTH
AMENDMENT
CENTER

OMNIBUS TECH DISCOVERY CHECKLIST

JANUARY 2026

This is a "cover-your-bases" checklist for discovery that can be referenced or automatically filed at the beginning of every case, even when you are unsure about which surveillance technologies may be at play. This list errs on the over-inclusive side for each of the sub-topics listed. If you are aware of the tech being utilized in your case, you can narrow down to the relevant, specific discovery demands tailored to that technology. Additionally, your jurisdiction may create paperwork, documentation, or data that is not listed here. However, this should also help identify possible discovery items to request in your case.

FACIAL RECOGNITION

1. Name & manufacturer of the facial recognition software used to conduct the search in this case, and the algorithm(s) version number(s) and year(s) developed, if available.
2. The original copy of the query or "probe" photo submitted to the [face recognition unit].
3. All edited copies of the query or "probe" photo submitted to the facial recognition system, noting if applicable which edited copy produced the candidate list the defendant was in, and a list of edits, filters, or any other modifications made to that photo.
4. Copy of the database photo matched to the query or "probe" photo and the percentage of the match, rank number, or confidence score assigned to the photo by the facial recognition system in the candidate list.
5. A list or description of the rank number or confidence scores produced by the system, including the scale on which the system is based (e.g. percentage, logarithmic, other).
6. A copy of the complete candidate list returned by the face recognition program or the first 20 candidates in the candidate list if longer than 20, in rank order and including the percentage of the match or confidence score assigned to each photo by the facial recognition system.
7. Parameters of the database used:
    a. How many photos are in the database;
    b. How are the photos obtained;
    c. How long the photos are stored;
    d. How often the database is purged;
    e. What the process is for getting removed from the database;
    f. Who has access to the database;
    g. How the database is maintained;
    h. The Privacy Policy for the database
8. The report produced by the analyst or technician who ran the facial recognition software, including any notes made about the possible match.
9. The name and training, certifications, or qualifications of the analyst who ran facial recognition search query.
10. Communications between case detectives/officers and the analyst(s) who ran the facial recognition search query.
11. Any audit logs related to searches conducted in this case.
12. Any records related to possible matches of individuals other than the defendant.
13. Any records indicating that a search related to this case resulted in no possible matches or searches where the probe image was rejected.
14. Error rates for the facial recognition system used, including false accept and false reject rates (also called false match and false non-match rates—FMR and FNMR). Documentation of how the error rates were calculated, including whether they reflect test or operational conditions.
15. Performance of the algorithm(s) on applicable NIST Face Recognition Vendor Tests, if available.

Face Rec: Additional Items to Consider

- Source code for the facial recognition algorithm(s) (if necessary).
- What measurements, nodal points, or other unique identifying marks are used by the system in creating facial feature vectors. If weighted differently, the scores given to each respective mark.

DATA FROM CLIENT'S DEVICE(S)

1. Search warrants, search warrant affidavits, or search warrant minutes
2. Consent to search forms
3. Device intake reports or vouchers
4. Chain of custody forms
5. Communication logs
6. Examination reports
7. The UFED Reader;
8. The portable file(s) or reports (UFDR or similar report) and any sub-reports created by law enforcement during the search or analysis of the device;
9. All raw data captured as a result of the extraction (*e.g.,* .bin files; ZIP/TAR files; etc.)
10. Any Standard Operating Procedures (SOPs), protocols, guidelines and written policies of the digital forensic laboratory.
11. Any laboratory accreditation documents (i.e. ANAB, IAS or other accreditation).
12. Any laboratory information management system records, any preliminary or final findings of nonconformance with accreditation, industry or governmental standards or laboratory protocols, and any conflicting analysis or results.
13. Name, business address, current curriculum vitae, and a list of any/all publications by the expert/examiner.
14. Degrees, certifications, proficiency tests and the results of any tests taken by the examiner within the past ten years.

GEOFENCES

1. All "geofence" warrants and their accompanying applications, served on Google or any other third-party entity;
2. All information provided to law enforcement in response to these geofence warrants, including the raw data files (".csv" file) and any accompanying letter and "Certificate of Authenticity" or similar documents;
3. All communications between law enforcement and Google/ the third-party regarding these geofence warrants, including any emails and records of phone conversations;
4. The name(s) and training, certifications, and qualifications of the law enforcement official(s) involved in the decision to seek the geofence warrant, the application for the geofence warrant, or the analysis of the geofence warrant return;
5. Training materials or other resources regarding the use of geofence warrants relied on by the official(s) involved in the decision to seek the geofence warrant, the application for the geofence warrant, or the analysis of the geofence warrant return;
6. Law enforcement policies, procedures, guidelines, training manuals, or presentations concerning the use of geofence warrants.
7. Any law enforcement testing or studies related to the accuracy of Google Location History data/the accuracy of the data produced by the geofence warrants here.

CELL-SITE LOCATION INFORMATION

1. Any warrants, applications, court orders, subpoenas, or exigent requests for real time cellular location tracking via the E911 system, and the resulting cellular location records from all cellular service providers such as, but not limited to;
   a. Location alert notifications (text messages, emails etc.),
   b. Subscriber information,
   c. Communications between the cellular provider and law enforcement.
2. Any warrants applications, court orders, exigent requests, sign-out logs, maintenance reports, and user manuals regarding the use of a cell-site simulator, "Stingray," a device that impersonates a wireless carrier's cell tower to force wireless devices within range to connect to it;
   a. All locations, dates, and times, across which Stingray signals were transmitted
   b. All unique electronic serial numbers, phone numbers, and locations procured
   c. Copies of any reports from any officers who utilized Stingray devices in this case and relevant training or certifications for these officers on Stingray use
   d. Policies and procedures and training materials applicable to the use of Stingrays in this case
   e. Contracts between manufacturer of Stingray and law enforcement
3. Any warrants, court orders, subpoenas, exigent requests, or preservation letters for cellular location records, and resulting cellular location records from all cellular service providers such as, but not limited to;
   a. Cell Site Location Information (Call Detail Records or "CDRs")
   b. Cell Site Lists
   c. Timing Advance, LOCDBOR, RTT, Data Sessions, True Call, MDT or other device location data
   d. Basic Subscriber information
   e. Keys

f. Time zone sheets

g. Communications with cellular providers

h. Maps, reports, PowerPoints, or other materials generated using the cellular location records obtained in this case.

4. Any warrants, warrant applications, court orders, subpoenas, exigent requests or preservation letters related to any "Tower Dump," including time period and number of locations sought, including records from all cellular service providers;

a. Cell Site Location Information (Call Detail Records or "CDRs")

b. Cell Site Lists from the providers and/or NDCAC

c. Timing Advance, LOCDBOR, RTT, Data Sessions, True Call, MDT or other device location data

d. Basic Subscriber information

e. Keys

f. Time zone sheets

g. Communications with cellular providers

h. Maps, reports, PowerPoints, or other materials generated using the cellular location records obtained in this case.

5. Any "area dump" warrants, warrant applications, court orders, subpoenas, exigent requests, or preservation letters ((these are warrants which seek to identify all cell phone users within a defined area, using location data dumped from nearby antenna, essentially a combination of Geofence warrants and Tower Dumps)—these can be referred to as "area dumps," "area searches", or "cellular area dump" warrants by mobile service providers and law enforcement agents):

a. Cell Site Lists from the providers and/or NDCAC

b. Timing Advance, LOCDBOR, RTT, Data Sessions, True Call, MDT or other device location data

c. Basic Subscriber information

d. Keys

e. Time zone sheets

f. Communications with cellular providers

g. "Timing Advance Request" forms or "Tower Area Dump" forms

h. Maps, reports, PowerPoints, or other materials generated using the cellular location records obtained in this case.

6. Any information related to forensic radio surveys or "drive tests" conducted in this matter including but not limited to:

a. Raw survey result data

b. Maps derived from the survey

c. The survey device used and settings at the time of the survey

d. The type of survey being conducted

e. Any pre-survey preparation plan or notes

f. Contemporaneous survey notes or progress maps

7. Any training manuals, presentations, or documents related to cell site information, timing advance, LOCDBOR, RTT, Data Sessions, True Call, MDT, forensic survey or other device location data

8. The name and training, certifications, or qualifications of the analyst who handled the location data in this case or intends to testify at trial.

9. A description of the intended testimony regarding the location data in this case including, but not limited to, a description of any testimony regarding tower coverage areas or the potential location of the target device(s).

AUTOMATIC LICENSE PLATE READERS

1. All records regarding ALPR software or SaaS, including:

a. the plan(s) enrolled in by the agency or the software purchased,

b. invoices for the purchase of ALPR software or SaaS,

c. sales materials and fact sheets supplied by vendors describing their products,

2. All records regarding the use of ALPR hardware, including:

a. the make and model of the ALPR units and associated hardware,

b. invoices for the purchase of ALPR hardware,

c. sales materials and fact sheets supplied by vendors describing their products,

3. All records regarding the storage of data obtained using ALPR technology, including:

a. the retention period of the data,

b. the number of license plate scans the agency currently stores,

c. other policies relating to the retention or removal of the data,

4. All records regarding access to ALPR data, including:

a. the legal justification required before an individual accesses ALPR data,

b. purposes for which the data may be accessed,

c. purposes for which the data may not be accessed,

d. who may access the data, what procedures they must go through to obtain access, and who must authorize access,

e. the identity of any records access officers or individuals within the agency responsible for access to ALPR data,

5. All records regarding the sharing of data obtained through ALPR technology, including:
    a. the types of data shared,
    b. the databases to which the agency contributes ALPR data,
    c. third parties, governmental or private, that may access your agency's ALPR data, including what procedures third parties must go through in order to access the data and any restrictions placed on third parties regarding further sharing of the agency's ALPR data,
    d. any agreements to share ALPR data with outside agencies, corporations or other entities,
6. All records regarding the creation of lists identifying plate numbers of stolen vehicles or individuals of interest (hereinafter "hotlists" or "alert lists") including:
    a. the agency's policy on maintaining hotlists, including:
        i. the policy for adding license plates to hotlists,
        ii. the policy for removing license plates from hotlists,
    b. what agencies contribute to the agency's hotlist,
    c. what government databases, if any, the agency uses to populate the hotlist,
    d. the hotlist maintenance policy for each agency contributing to the agency's database,
    e. any procedures for ensuring the accuracy of data added to any hotlist by outside agencies,
    f. the number of plates currently in the hotlist,
7. All audit trails or audit logs related to State license plate number _____ , including but not limited to:
    a. when State license plate number _____ was added to the hotlist,
    b. any officers obtaining real time or historical updates on State license plate number _____ ,
    c. any and all officers who searched the database for State license plate number _____
8. All records regarding obtaining ALPR data from third parties, including which databases the agency can access,
9. All training materials used to instruct members of the agency in ALPR deployment, data management, or operation of automated records systems that contain ALPR data to which any member of the agency has access, including regional or shared ALPR databases.
10. Information on the particular search
    a. Any and all alerts, analytic reports, or other reports resulting from the identification of or related to license plate (or vehicle) X
    b. All documents including investigative reports, notes, and emails related to the enrollment of license plate (or vehicle) X on any hotlists and the basis of suspicion for that enrollment.
    c. The specific vehicle information, such as partial or whole plate and description of vehicle enrolled on any ALPR hotlists.
11. Camera Information
    a. Camera information for each camera that captured license plate X (or vehicle), including: camera ID number, make, model, date of installation, and whether the camera is fixed or mobile.
    b. Location information for each camera that captured license plate (or vehicle) X including: precise location, position, angle, and number of lanes captured by the camera.
    c. All service, error, calibration, and other logs for each camera listed above
    d. Location of all fixed and mobile cameras included in the ALPR system at the time the searches for license plate (or vehicle) X were conducted.
12. Database information
    a. Any search queries or reports requested resulting in the identification of license plate (or vehicle) X including search terms, parameters, and results.
        i. The audit trail pertaining to all searches run pursuant to the investigation of license plate (vehicle) X.
    b. The specific dataset against which any query was run or report requested and the company or agency responsible for maintaining the dataset.
    c. The identity of the individuals who ran any query, search, or report request pertaining to the identification or location tracking of license plate (or vehicle) X.
    d. Database records showing the number of historical vehicle scans currently in the database and the number of unique vehicle scans.
    e. Any routine audit or use records produced pertaining to the ALPR database.
13. System information
    a. Police department's policies and procedures for ALPR systems, including: training requirements, deployment options, operating procedures, hot list management, proper use and maintenance of the technology, data usage (including collection, access, retention, and sharing of data), and sanctions for non-compliance with policies.
    b. Any and all activity reports provided to other governmental agencies detailing the use of [Department's] ALPR systems.
    c. Memoranda, email, or other document relating to joint operation of the ALPR system or data sharing between [Department] and other law enforcement agencies

DRONES

Internal Agency Records

1. Purchase orders for the UAV device used by the Officer piloting the UAV.
2. Purchase orders for any software used in conjunction with the UAV devices (there are companies out there like DroneSense that have "hardware agnostic" add-on software to make drones fly autonomously, connect with docks, integrate into other systems like Evidence.com or RTCCs, etc.)
3. Related, system information for any management and collaboration platforms used in conjunction with the drone/drone program.
4. Information on any remote docks used in conjunction with the drone/program (a lot of systems like "drone as first responders" include remote docks spread throughout a city that means drones have a much broader range than if they were just deployed from a headquarters)
5. Device manuals or operating instructions.
6. Departmental training materials for UAV use and care.
7. Departmental regulations for UAV use.
8. Departmental policies and procedures for UAV systems including training requirements; deployment options; operating procedures; proper use and maintenance of the technology; data collection, access, retention, sharing of data; sanctions for non-compliance with policies

Licensing Records

1. Special airworthiness certificate. 91.303(a)(1)
2. Aircraft registration. 107.13
3. Aircraft registration application, accompanying notarized affidavit, and any other accompanying documents including but not limited to proof of ownership.
4. N-number or Remote ID assigned to the UA.
5. Remote pilot certificate of the Officer piloting the UAV. 107.12(a)(1)
6. Application for a remote pilot certificate of the Officer piloting the UAV. 107.63
7. Any flight logbooks for the drone(s) used (not required under current FAA rules but is a best practice)
8. Declaration of Compliance. 107.160
9. The State UAS permit (many states require these in addition to an FAA license)
10. Any waivers under Part 107 issued to the department or the Officer piloting the UAV, including but not limited to night waivers, or Beyond Visual Line Of Sight (BVLOS) waivers.

BODY WORN CAMERAS

1. All footage from Body Worn Cameras on dates _____ preceding contact with client, during contact with client, and following contact with client;
2. Audit trails and device information (including but not limited to serial numbers, repair history, version) for each camera used;
3. Any evidence analysis software or reports generated pursuant to the body worn camera footage, including but not limited to "Draft One" reports;
4. User information for each body worn camera present on date _____ ;
5. User manuals for each body worn camera present on date _____ ;

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL's mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the NACDL Foundation for Criminal Justice (NFCJ)

NACDL's Fourth Amendment Center is supported by contributions made to the NACDL Foundation for Criminal Justice (NFCJ), a 501(c)(3) charity. The mission of the NFCJ is to preserve and promote the core values of America's justice system guaranteed by the Constitution — among them due process, freedom from unreasonable search and seizure, fair sentencing and effective assistance of counsel — by educating the public and the legal profession to the role of these rights and values in a free society.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL or by making a tax-deductible donation to the NFCJ. Learn more by visiting **NACDL.org/Landing/JoinNow** or **NFCJ.org/support**.

About the Fourth Amendment Center

NACDL's Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges. To request assistance or additional information, contact **4AC@nacdl.org**.

For litigation assistance and other resources contact 4AC@nacdl.org

NACDL FOURTH AMENDMENT CENTER