# AGENDA

# SURVEILLANCE ADVISORY BOARD REGULAR MEETING

**6:00 PM**

**HYBRID-MEETING**
www.CityOfVallejo.net

**Vallejo Room**
**Lower Level of JFK Library**
**505 Santa Clara Street**
**Vallejo, California**

**JANUARY 18, 2024**

**Board Members**
Andrea Sorce (Chair)
VACANT (Vice-Chair)
Michael Mcmillian
Brooke Reddell
Mike Moreno
Jasmine Chisley
Simon Lee

---

**IMPORTANT NOTICE**
This AGENDA contains a brief general description of each item to be considered. The posting of the recommended actions does not indicate what action may be taken. If comments come to the Surveillance Advisory Board without prior notice about an item not listed on the AGENDA, no specific answers or responses should be expected at this meeting per State law.

Pursuant to Government Code Section 54954.3 of the Brown Act, members of the public shall be afforded the opportunity to speak on any agenda item of interest to them after being recognized by the presiding officer. Members of the public wishing to be so recognized are requested to submit a completed speaker card to the Secretary of the Surveillance Advisory Board prior to the consideration of the item or raise their hand via ZOOM: https://Zoom.us/my/vallejoeoc (669) 900-6833. Enter Meeting ID: 851 502 7190#. Press * 9 to digitally raise your hand from the phone. For additional instructions on how to speak remotely during public comment, please visit www.cityofvallejo.net/publiccomment. In person speakers will be recognized first.

**Notice of Availability of Public Records:**
All public records relating to an open session item, which are not exempt from disclosure pursuant to the Public Records Act, that are distributed to a majority of the Surveillance Advisory Board will be available on the City of Vallejo website at www.cityofvallejo.net subject to staff's ability to post the documents prior to the meeting.

**Members of the Public will be able to participate in-person or remotely via Zoom. Meeting Location listed above will be open to members of the public 30 minutes prior to the start of the meeting.**

**PUBLIC COMMENT: Members of the public may provide public comments during the board meeting in person or via ZOOM (https://Zoom.us/my/vallejoeoc), or via phone, by dialing (669) 900-6833. Meeting ID 851 502 7190# For additional instructions on how to speak remotely during public comment, please visit, www.cityofvallejo.net/publiccomment**

**VIEW THE MEETING: There are three different ways you can view this public meeting:**

- **In Person**
- **Join the Zoom webinar: https://Zoom.us/my/vallejoeoc**
- **View the meeting on the city website.**

**1. CALL TO ORDER**

**2. PLEDGE OF ALLEGIANCE**

**3. ROLL CALL**

**4. COMMUNITY FORUM**

*Anyone wishing to address the Surveillance Advisory Board on any matter for which another opportunity to speak is not provided on the agenda, and which is within the jurisdiction of the Surveillance Advisory Board to resolve, is requested to submit a completed speaker card to the Board Secretary. When called upon, each speaker should step to the podium, state his /her name, and address for the record. The conduct of the community forum shall be limited to a maximum of fifteen (15) minutes, with each speaker limited to three minutes pursuant to Vallejo Municipal Code Section 2.20.300.*

**5. CONSENT CALENDAR AND APPROVAL OF AGENDA**

A. **Approval of Minutes November 16, 2023**
Recommendation: By Motion approve the meeting minutes
Contact: Naveed Ashraf, Board Secretary

**6. REPORT OF THE BOARD SECRETARY**

**7. REPORT OF THE CITY ATTORNEY**

**8. REPORT OF THE CITY COUNCIL LIAISON**

**9. REPORT OF THE CHAIRPERSON AND MEMBERS OF THE BOARD**

**10. ACTION ITEM**

A. **Selection of Vice Chair**
Recommendation: By motion, elect members of the board to serve as vice chair for the term January 2024 through December 2024.
Contact: Naveed Ashraf, Board Secretary

B. **Board Workshop -- Overview of Vallejo Police Department surveillance technology currently in use and future technology the department is interested in acquiring.**
Recommendation: In depth discussion of various surveillance technologies with the board.
Contact: Drew Ramsey, Police Captain

**11. INFORMATION ITEM**

A. **Technology usage reports: Drones, Cell site simulator, RAVEN gunshot detection beta project, and FLOCK ALPR cameras.**
Recommendation: Receive verbal reports from the Police Department.
Contact: Drew Ramsey, Police Captain

B. **Flock RAVEN gunshot detection beta project ad-hoc subcommittee report.**
Recommendation: Progress report to the board.

Contact: Andrea Sorce, Board Chair

**12. FUTURE AGENDA ITEM**

A. **Explore additional multi-agency hopping issues with FLOCK data.**
Recommendation: Future agenda item to be agendized for discussion.
Contact: Naveed Ashraf, Board Secretary

B. **Discuss AB-642 (Facial Recognition Technology), the implications of the law on Vallejo citizens. Possibly create/adopt a resolution to document SAB's official position concerning facial recognition technology.**
Recommendation: Future agenda item to be agendized for discussion.
Contact: Naveed Ashraf, Board Secretary

C. **Use of encrypted text messaging apps on VPD cell phones.**
Recommendation: A request was made via e-mail by Board Member McMillian to consider this topic for future discussion. Boardmember McMillian supplied 2 articles to the board secretary. These articles are being attached here for the board's distribution.
Contact: Michael McMillian, Board Member

**13. ADJOURNMENT**

---

I, Naveed Ashraf, Surveillance Advisory Board Executive Secretary, do hereby certify that I have caused a true copy of the above notice and agenda to be delivered to each of the members of the Surveillance Advisory Board, at the time and in the manner prescribed by law and that this agenda was posted at City Hall, 555 Santa Clara Street, CA at 5:00 P.M., January 12, 2024

Dated: January 12, 2024

Chief Innovation Officer & IT Director

# DRAFT

## SURVEILLANCE ADVISORY BOARD
## REGULAR MEETING MINUTES

**NOVEMBER 16, 2023**

**Vallejo Room**
**505 Santa Clara Street, Vallejo, California**

1. **CALL TO ORDER**

   The meeting was called to order at 6:01 p.m.

2. **PLEDGE OF ALLEGIANCE**

3. **ROLL CALL**
   **Present:** Chair Sorce, Boardmembers Chisley, Lee, McMillian, Moreno, and Reddell
   **Absent:** None
   **Staff present:** Secretary Ashraf

4. **COMMUNITY FORUM –** None.

5. **CONSENT CALENDAR AND APPROVAL OF THE AGENDA**
   ***Action****: Moved by Boardmember Moreno, seconded by Boardmember Lee, and carried unanimously to approve the Agenda and the Consent Calendar.*

   A. **Approval of Minutes – September 21, 2023.**
      ***Actions****: Approved minutes.*

6. **REPORT OF THE BOARD SECRETARY** – None.

7. **CITY ATTORNEY REPORT** – None.

8. **REPORT OF THE CITY COUNCIL LIAISON** – None.

9. **REPORT OF THE CHAIRPERSON AND MEMBERS OF THE BOARD**

   In response to a question from Chair Sorce, Staff Secretary Ashraf provided a status update on the efforts to fill the vacant District 3 seat to the committee.

10. **ACTION ITEM**

    A. **Board Workshop – overview of Vallejo Police Department surveillance technology currently in use and future technology the department is interested in acquiring**

       Police Captains Ramsey and Knight provided a comprehensive overview of current technology used by the Police Department and responded to questions from Boardmembers.

Mike Katz-Lacabe (Oakland Privacy) provided a separate presentation to the Board and provided highlights related to AB 34.

Following discussion, the Board agreed to create a final document with information about each technology it reviews.

**B. Investigate how private entities are sharing Flock ALPR data.**

Staff responded to questions from Boardmembers. Boardmembers provided comment.

## 11. INFORMATION ITEMS

**A. Technology usage reports: Drones, Cell Site Simulator, RAVEN Gunshot Beta Project, and Flock ALPR Cameras**

Usage report will be presented at a future meeting.

**B. Flock Raven Gunshot Detection Beta Project Ad-hoc Subcommittee Report**

Chair Sorce provided an update noting the ad-hoc committee has not had an opportunity to meet.

## 13. FUTURE AGENDA ITEMS

- Explore Additional Multi-Agency Hopping Issues with Flock Data
- Discuss AB-642 (Facial Recognition Technology). Implications of the Law on Vallejo Citizens. Possibly Create/Adopt a Resolution to Document SAB's Official Position Concerning Facial Recognition Technology

## 14. ADJOURNMENT

The meeting adjourned at 7:55 p.m.

_____
ANDREA SORCE, CHAIR

ATTEST:

_____
NAVEED ASHRAF
CHIEF INNVOATION OFFICER/IT DIRECTOR

# Vallejo Police Department
# Cell Site Simulator (CSS)
# Deployment Log

## Calendar Year 2023

The Vallejo Police Department recognizes the public interest in ensuring that cell site simulator technology is appropriately used and monitored and seeks to be transparent with its usage. Please note that the cell site simulator is merely an investigative tool to find a cell phone. Results from the cell site simulator alone are never used establish probable cause for an arrest or search.

A deployment is defined as any time the cell site simulator is turned on and used to find a target phone. The cell site simulator might be deployed several times to find the same phone even if previously successfully located. Each deployment in the log is not necessarily a separate phone that was searched for. An arrest is not necessarily effected even if a phone is located. There are many factors that determine when and arrest will be effected.

Authorized Purpose Codes:

(A) Locate missing persons

(B) Locate at-risk individuals

(C) Locate victims of mass casualty incidents

(D) Assist in felony investigations

(E) Apprehend fugitives

| # | DATE | Affiant/Operator | Case Number | Crime Code | Located (Y/N) | Search Warrant Obtained Prior to Deployment | Used under Exigency (Y/N) | Warrant Obtained After Use (Y/N or N/A) | Arrest Made (Y/N) | Purpose Code (Y/N) |
|---|---|---|---|---|---|---|---|---|---|---|
| | JANUARY | | | | | | | | | |
| 1 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | Y | D |
| 2 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | N | D |
| | | | | | | | | | | |
| | February | | | | | | | | | |
| 3 | [redacted] | [redacted] | [redacted] | 211 | Y | Y | N | N/A | Y | D |
| 4 | [redacted] | [redacted] | [redacted] | 211 | N | Y | N | N/A | N | D |
| | March | | | | | | | | | |
| 5 | [redacted] | [redacted] | [redacted] | 211 series | Y | Y | N | N/A | N | D |
| 6 | [redacted] | [redacted] | [redacted] | 211 series | Y | Y | N | N/A | N | D |
| | April | | | | | | | | | |
| | NO USE | | | | | | | | | |
| | May | | | | | | | | | |
| | NO USE | | | | | | | | | |
| | June | | | | | | | | | |
| 7 | [redacted] | [redacted] | [redacted] | 187x4 | N | Y | N | N/A | N | D |
| 8 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | N | D |
| 9 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | N | D |
| | July | | | | | | | | | |
| | NO USE | | | | | | | | | |
| | August | | | | | | | | | |
| 10 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | N | D |
| | September | | | | | | | | | |
| | NO USE | | | | | | | | | |
| | October | | | | | | | | | |
| 11 | [redacted] | [redacted] | [redacted] | 187x2 | Y | Y | N | N/A | N | D |
| | November | | | | | | | | | |
| 12 | [redacted] | [redacted] | [redacted] | 187 | Y | Y | N | N/A | Y | D |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | DECEMBER | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

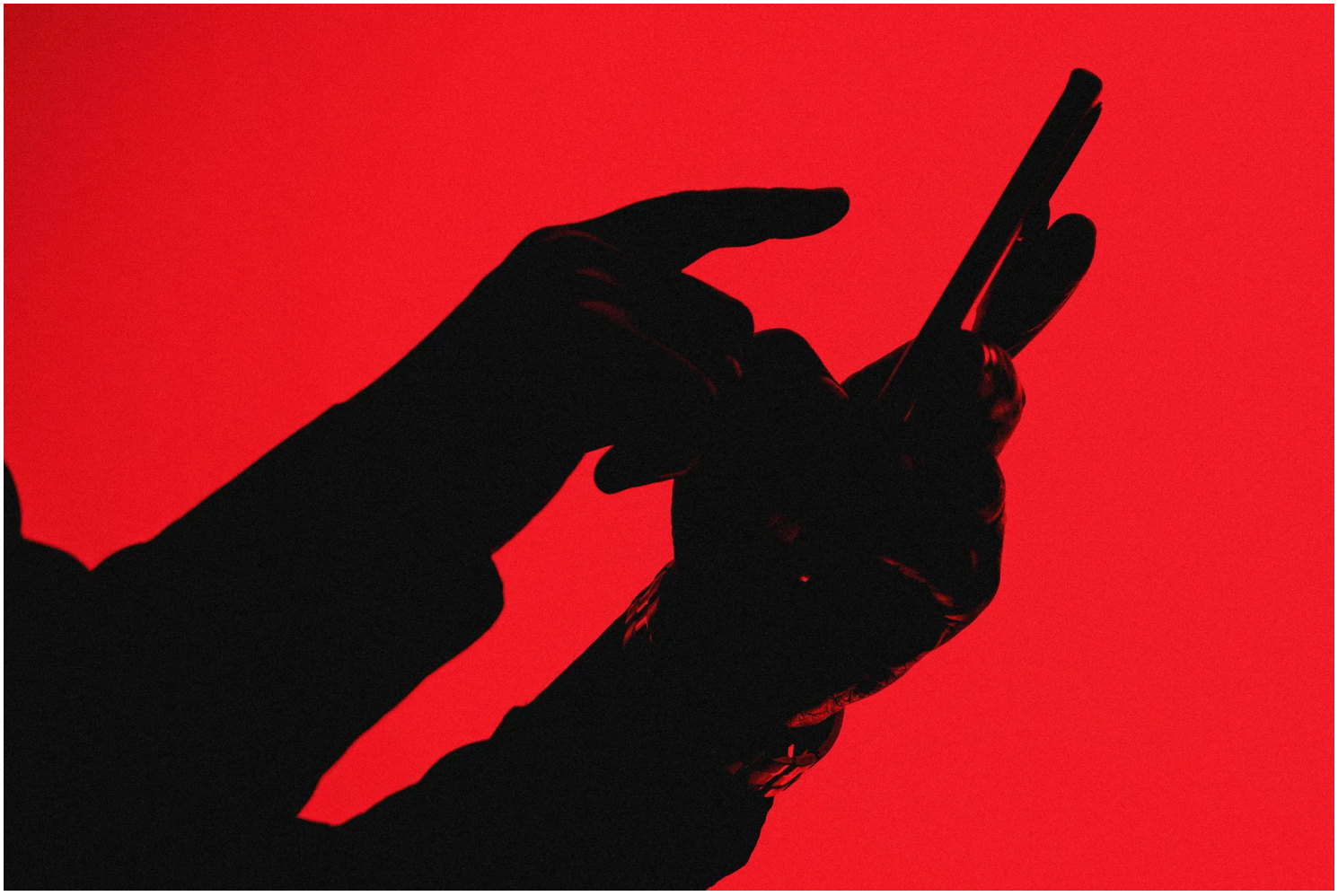
| Date | Time | UAS | Mission | Case Number | Length (min) | Airspace | D/N |
|---|---|---|---|---|---|---|---|
| 1/23/2023 | 1000 | Mavic 3 | ESU | 23-653 | 10 | G | Day |
| 1/24/2023 | 600 | Matrice | ESU | 23-653 | 35 | G | Day |
| 1/25/2023 | 1000 | Mavic 3 | Patrol | 2301250050 | 20 | G | Day |
| 2/2/2023 | 1000 | Mavic 3 | ESU | 23-1206 | 10 | G | Day |
| 2/9/2023 | 1130 | Avata | Patrol | 23-1539 | 10 | G | Day |
| 4/16/2023 | 1400 | Mavic 3 | Patrol | 23-3634 | 25 | G | Day |
| 4/29/2023 | 1500 | Mavic 3 | Patrol | TBD | 15 | G | Day |
| 4/30/2023 | 1330 | Mavic 3 | Patrol | 23-4149 | 2 | G | Day |
| 6/16/2023 | 1401 | Mavic 3 Pro | Patrol | 23-5832 | 55 | G | Day |
| 7/8/2023 | 1920 | Mavic 3 Pro | Fire | 23-6549 | 6 | G | Day |
| 7/11/2023 | 1306 | Mavic 3 Pro | Fire | 23-6549 | 6 | G | Day |
| 7/14/2023 | 1916 | Mavic 3 Pro | ESU | 23-6933 | 20 | G | Day |
| 7/14/2023 | 700 | Mavic 3 | ESU | 23-6977 | 60 | G | Day |
| 7/17/2023 | 1200 | Mavic 3 | Patrol | 23-6828 | 10 | G | Day |
| 7/21/2023 | 722 | Avata | ESU | 23-6933 | 18 | D | Day |
| 7/24/2023 | 932 | Mavic 3 Enterprise | Patrol | 23-7020 | 22 | G | Day |
| 8/2/2023 | 1015 | Mavic 3 | Patrol | 23-7445 | 20 | G | Day |
| 8/9/2023 | 843 | Mavic 3 Pro | Patrol | 23-7789 | 8 | G | Day |
| 8/12/2023 | 1009 | Mavic 3 Pro | ESU | 23-7928 | 269 | G | Day |
| 8/12/2023 | 1521 | Avata | ESU | 23-7928 | 16 | G | Day |
| 8/12/2023 | 1000 | Mavic 3 | ESU | 23-7953 | 300 | G | Day |
| 8/15/2023 | 1258 | Anafi2 | Patrol | 23-8052 | 20 | G | Day |
| 8/17/2023 | 1000 | Mavic 3 | ESU | Pre-event | 10 | G | Day |
| 8/21/2023 | 1350 | Maivc 3 | Patrol | 23-8255 | 1 | G | Day |
| 8/22/2023 | 454 | Mavic 3 Pro | ESU | 23-8279 | 40 | G | Day |
| 8/22/2023 | 523 | Avata | ESU | 23-8279 | 3 | G | Day |
| 8/22/2023 | 500 | Matrice 210 | ESU | 23-8279 | 30 | G | Night |
| 8/22/2023 | 500 | Mavic 3 | ESU | 23-8279 | 45 | G | Night |
| 8/29/2023 | 1311 | Mavic 3 Pro | Patrol | 23-8596 | 8 | G | Day |
| 8/29/2023 | 1257 | Mavic 3 | Patrol | 23-8596 | 10 | G | Day |
| 8/30/2023 | 1922 | Mavic 3 Pro | Traffic | 23-8650 | 17 | G | Day |
| 9/1/2023 | 907 | Mavic 3 Pro | Traffic | 23-8689 | 13 | G | Day |
| 9/6/2023 | 1108 | Mavic 3 Pro | ESU | 1200 | 10 | G | Day |
| 9/6/2023 | 1121 | Avata | ESU | 1200 | 2 | G | Day |
| 9/6/2023 | 1123 | FPV | ESU | 1200 | 3 | G | Day |
| 9/12/2023 | 1100 | Mavic 3 | Patrol | 23-9198 | 39 | G | Day |
| 9/24/2023 | 1654 | Mavic 3 Pro | Patrol | 23-9728 | 29 | G | Day |
| 9/25/2023 | 1200 | Mavic 3 | Investigations | Inv. | 60 | G | Day |
| 10/3/2023 | 822 | Mavic 3 Pro | Patrol | 23-10067 | 17 | G | Day |

| Date | Time | UAS | Mission | Case Number | Length (min) | Airspace | D/N |
|---|---|---|---|---|---|---|---|
| 10/3/2023 | 800 | Mavic 3 | Patrol | 23-10067 | 20 | G | Day |
| 10/7/2023 | 1821 | Mavic 3 Enterprise | Patrol | 23-10261 | 4 | G | Day |
| 10/8/2023 | 1643 | Mavic 3 Pro | Patrol | 23-10292 | 14 | G | Day |
| 10/9/2023 | 1600 | Maivc 3 | Patrol | 23-10310 | 20 | G | Day |
| 10/16/2023 | 1430 | Mavic 3 Pro | ESU | 23-10632 | 14 | G | Day |
| 10/18/2023 | 513 | Avata | ESU | 23-10632 | 6 | G | Day |
| 10/18/2023 | 430 | Mavic 3 Enterprise | ESU | 23-10632 | 60 | G | Night |
| 10/20/2023 | 2200 | Mavic 3 Enterprise | ESU | 23-10728 | 120 | G | Night |
| 11/3/2023 | 1700 | Mavic 3 | Patrol | TBD | 9 | G | Day |
| 11/5/2023 | 1700 | Mavic 3 | Patrol | TBD | 9 | G | Day |
| 11/20/2023 | 1317 | Mavic 3 Pro | Patrol | 23-11807 | 9 | G | Day |
| 11/20/2023 | 1320 | FPV | Patrol | 23-11807 | 7 | G | Day |
| 12/3/2023 | 900 | Mavic 3 | Patrol | TBD | 20 | G | Day |
| 12/7/2023 | 921 | Mavic 3 Pro | ESU | 23-12587 | 11 | G | Day |
| 12/11/2023 | 1442 | Mavic 3 Pro | ESU | 23-12587 | 26 | G | Day |
| 12/14/2023 | 536 | Avata | ESU | 23-12587 | 10 | G | Day |
| 12/15/2023 | 500 | Mavic 3 | Patrol | 23-12587 | 31 | G | Day |
| 12/28/2023 | 1313 | Mavic 3 Pro | Patrol | 23-13040 | 6 | G | Day |
| 12/31/2023 | 1441 | Mavic 3 Pro | Patrol | 23-13123 | 5 | G | Day |

DELL CAMERON DHRUV MEHROTRA SECURITY NOV 20, 2023 1:25 PM

# Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records

**A WIRED analysis of leaked police documents verifies that a secretive government program is allowing federal, state, and local law enforcement to access phone records of Americans who are not suspected of a crime.**



PHOTOGRAPH: PANITHAN PHOLPANICHRASSAMEE/GETTY IMAGES

SAVE

A little-known surveillance program tracks more than a trillion domestic phone records within the United States each year, according to a letter WIRED obtained that was sent by US senator Ron Wyden to the Department of Justice (DOJ) on Sunday, challenging the program's legality.

According to the letter, a surveillance program now known as Data Analytical Services (DAS) has for more than a decade allowed federal, state, and local law enforcement agencies to mine the details of Americans' calls, analyzing the phone records of countless people who are not suspected of any crime, including victims. Using a technique known as chain analysis, the program targets not only those in direct phone contact with a criminal suspect but anyone with whom those individuals have been in contact as well.

The DAS program, formerly known as Hemisphere, is run in coordination with the telecom giant AT&T, which captures and conducts analysis of US call records for law enforcement agencies, from local police and sheriffs' departments to US customs offices and postal inspectors across the country, according to a White House memo reviewed by WIRED. Records show that the White House has provided more than $6 million to the program, which allows the targeting of the records of any calls that use AT&T's infrastructure—a maze of routers and switches that crisscross the United States.

In a letter to US attorney general Merrick Garland on Sunday, Wyden wrote that he had "serious concerns about the legality" of the DAS program, adding that "troubling information" he'd received "would justifiably outrage many Americans and other members of Congress." That information, which Wyden says the DOJ confidentially provided to him, is considered "sensitive but unclassified" by the US government, meaning that while it poses no risk to national security, federal officials, like Wyden, are forbidden from disclosing it to the public, according to the senator's letter.

AT&T spokesperson Kim Hart Jonson declined WIRED's request to comment on the DAS program, saying only that the company is required by law to comply with a

lawful subpoena.

There is no law requiring AT&T to store decades' worth of Americans' call records for law enforcement purposes. Documents reviewed by WIRED show that AT&T officials have attended law enforcement conferences in Texas as recently as 2018 to train police officials on how best to utilize AT&T's voluntary, albeit revenue-generating, assistance.

In 2020, the transparency collective Distributed Denial of Secrets published hundreds of gigabytes of law enforcement data stolen from agencies around the US. A WIRED review of the files unearths extraordinary detail regarding the processes and justifications that agencies use to monitor the call records of not only criminal suspects, but of their spouses, children, parents, and friends. While DAS is managed under a program devoted to drug trafficking, a leaked file from the Northern California Regional Intelligence Center (NCRIC) shows that local police agencies, such as those in Daly City and Oakland, requested DAS data for unsolved cases seemingly unrelated to drugs.

In one instance, an officer with the Oakland Police Department asked for a "Hemisphere analysis" to identify the phone number of a suspect by analyzing the calls of the suspect's close friends. In another, a San Jose law enforcement officer asked the Northern California Regional Intelligence Center to identify a victim and material witness in an unspecified case. One officer, soliciting information from AT&T under the program, wrote: "We obtained six months of call data for [suspect]'s phone, as well as several close associations (his girlfriend, father, sister, mother)." The records do not indicate how AT&T responds to every request.

Leaked law enforcement files further show that a range of officials—from a US Postal Service inspector to a New York Department of Corrections parole officer—participated in DAS training sessions. Other participants include port authorities and members of US Immigration & Customs Enforcement, National Guard, and California Highway Patrol, alongside scores of smaller agencies.

First disclosed by *The New York Times* in September 2013 as Hemisphere, the DAS program—renamed in 2013—has since flown largely under the radar. Internal records concerning the program's secrecy that were obtained by the newspaper at

the time show that law enforcement had long been instructed to never "refer to Hemisphere in any official document."

Following the *Times*' story, former US president Barack Obama reportedly suspended funding for the Hemisphere program in 2013. And while discretionary funding was withheld over the following three years, a White House memo obtained by WIRED shows that individual law enforcement organizations across the US were permitted to continue contracting with AT&T directly in order to maintain access to its data-mining service. Funding resumed under former president Donald Trump but was halted again in 2021, according to the White House memo. Last year, under president Joe Biden, the funding resumed once more, the memo says.
The White House acknowledged an inquiry from WIRED but has yet to provide a comment.

**THE DAS PROGRAM** is maintained under an affiliated program called HIDTA, funded by the White House's Office of National Drug Control Policy (ONDCP). HIDTA, or "high-intensity drug trafficking area," is a designation assigned to 33 different regions of the US, according to the White House. The first five regions, mapped out in 1990, included areas around Los Angeles, Houston, Miami, New York, and the entire US-Mexico border, some of the nation's most active drug trafficking areas.

The collection of call record data under DAS is not wiretapping, which on US soil requires a warrant based on probable cause. Call records stored by AT&T do not include recordings of any conversations. Instead, the records include a range of identifying information, such as the caller and recipient's names, phone numbers, and the dates and times they placed calls, for six months or more at a time. Documents released under public records laws show the DAS program has been used to produce location information on criminal suspects and their known associates, a practice deemed unconstitutional without a warrant in 2018.

"Requests concerning location information require the highest level of legal demand, which is a court-issued warrant, except in emergency situations," AT&T's Hart Jonson says.

Orders targeting a nexus of individuals are sometimes called "community of interest" subpoenas, a phrase that among privacy advocates is synonymous with dragnet surveillance.

"The scale of the data available to and routinely searched for the benefit of law enforcement under the Hemisphere Project is stunning in its scope," Wyden's letter to Garland says.

The White House has provided at least $6.1 million in discretionary funding to the DAS program since 2013, according to a two-page memo authored last year by White House officials. An internal HIDTA "participant guide" reviewed by WIRED shows that HIDTA funding exceeded $280 million in 2020 alone. It remains unclear how much HIDTA funding is spent to support AT&T's vast collection of American call records.

It is not currently known how far back the call records accessible under DAS go. A slide deck released under the Freedom of Information Act in 2014 states that up to 10 years' worth of records can be queried under the program, a statistic that contrasts with other internal documents that claimed AT&T could reach decades into the past. AT&T's competitors, meanwhile, typically retain call records for no more than two years. (The necessity for phone companies to track call records for extended periods of time has gradually decreased with the disappearance of long-distance charges.)

**THE DAS PROGRAM** echoes multiple dragnet surveillance programs dating back decades, including a Drug Enforcement Agency program launched in 1992 that forced phone companies to surrender records of virtually all calls going to and from over 100 other countries; the National Security Agency's bulk metadata collection program, which the US Second Circuit Court of Appeals deemed illegal in 2014; and the Call Details Records program, which suffered from "technical irregularities" leading the NSA to collect millions of calls it was "not authorized to receive."

Unlike these past programs, which were subject to congressional oversight, DAS is not. A senior Wyden aide tells WIRED the program takes advantage of numerous "loopholes" in federal privacy law. The fact that it's effectively run out of the White House, for example, means it is exempt from rules requiring assessments of its

privacy impacts. The White House is also exempt from the Freedom of Information Act, reducing the public's overall ability to shed light on the program.

Because AT&T's call record collection occurs along a telecommunications "backbone," protections enshrined under the Electronic Communications Privacy Act may not apply to the program.

Earlier this month, Wyden and other lawmakers in the House and Senate introduced comprehensive privacy legislation known as the Government Surveillance Reform Act. The bill contains numerous provisions that, if enacted, would patch most if not all of these loopholes, effectively rendering the DAS program, in its current form, explicitly illegal.

**READ WYDEN'S FULL** letter to the US Department of Justice below:



*The Honorable Merrick B. Garland*
*Attorney General*
*U.S. Department of Justice*
*950 Pennsylvania Avenue, NW*
*Washington, DC 20530-0001*

*Dear Attorney General Garland:*

*I write to request that you clear for public release additional information about the Hemisphere Project. This is a long-running dragnet surveillance program in which the White House pays AT&T to provide all federal, state, local, and Tribal law enforcement agencies the ability to request often-warrantless searches of trillions of domestic phone records.*

*In 2013, the New York Times revealed the existence of a surveillance program in which the White House Office of National Drug Control Policy (ONDCP) pays AT&T to mine its customers' records for the benefit of federal, state, local, and Tribal law enforcement agencies. According to an ONDCP slide deck, AT&T has kept and queries as part of the Hemisphere Project call records going back to 1987, with 4 billion new records being added every day. That slide deck was apparently disclosed by a local law enforcement agency in response to a public information request and was published by the New York Times in 2013.*
*The scale of the data available to and routinely searched for the benefit of law enforcement under the Hemisphere Project is stunning in its scope. One law enforcement official described the Hemisphere Project as "AT&T's Super Search Engine" and ... "Google on Steroids," according to emails released by the Drug Enforcement Administration (DEA) under the Freedom of Information Act. The ONDCP slide deck and an email released by the DEA also reveal that AT&T searches records kept by its wholesale division, which carries communications on behalf of other communications companies and their customers. Another slide deck released by ONDCP and published by the press in 2014 describes the specific capabilities of Hemisphere, including that it can be used to identify alternate numbers used by a target, obtain location data and "two levels of call detail records for one target number" (meaning the phone records of everyone who communicated with the target).*

*The Hemisphere Project has been supported by regular funding from the White House ONDCP since 2009, according to the attached undated white paper that ONDCP provided to my office on October 27, 2022 (Appendix A). That same document reveals that White House funding for this program was suspended by the Obama Administration in 2013, the same year the program was exposed by the press, but continued with other federal funding under a new generic sounding program name, "Data Analytical Services." ONDCP funding for this surveillance*

*program was quietly resumed by the Trump Administration in 2017, paused again in 2021, the first year of the Biden Administration, and then quietly restarted again in 2022.*

*Although the Hemisphere Project is paid for with federal funds, they are delivered to AT&T through an obscure grant program, enabling the program to skip an otherwise mandatory federal privacy review. If the funds came directly from a federal agency, such as the DEA, Hemisphere would have been subjected to a mandatory Privacy Impact Assessment conducted by the Department of Justice (DOJ) Office of Privacy and Civil Liberties, the findings of which would be made public. Instead, ONDCP provides funding for the program through the Houston High Intensity Drug Trafficking Area (HIDTA), one of 33 regional funding organizations as a part of a grant program created by Congress and administered by ONDCP. The HIDTAs distribute federal anti-drug law enforcement grants to state and local agencies, and are governed by a board made up entirely of federal, state and local law enforcement officials.*
*ONDCP provided my staff with an undated white paper describing the program and its historical funding levels, but ONDCP directed all questions about Hemisphere to the Houston HIDTA. Officials at the Houston HIDTA provided my office with a briefing on November 7, 2022, and spoke again with my staff again by phone on December 1, 2022. The Houston HIDTA officials told my staff that all Hemisphere requests are sent to a single AT&T analyst located in Atlanta, Georgia, and that any law enforcement officer working for one of the federal, state, local and Tribal law enforcement agencies in the U.S. can contact the AT&T Hemisphere analyst directly to request they run a query, with varying authorization requirements. The Houston HIDTA officials confirmed that Federal and state law enforcement agencies can request a Hemisphere search with a subpoena, which is a directive that many law enforcement agencies can issue themselves (except in California and Texas, where a court order is required by state law). They also explained that Hemisphere searches are not required to be in support of drug-related investigations.*

*For the past year, I have urged the DOJ to release dozens of pages of material related to the Hemisphere Project, which it first provided to my office in 2019. This information has been designated "Law Enforcement Sensitive," which is meant to restrict its public release. I have serious concerns about the legality of this*

*surveillance program, and the materials provided by the DOJ contain troubling information that would justifiably outrage many Americans and other members of Congress. While I have long defended the government's need to protect classified sources and methods, this surveillance program is not classified and its existence has already been acknowledged by the DOJ in federal court. The public interest in an informed debate about government surveillance far outweighs the need to keep this information secret. To that end, I urge you to promptly clear for public release the material described in Appendix B.*

*Thank you for your attention to this important matter.*

*Sincerely,*

*Ron Wyden*
*United States Senator*

---

## You Might Also Like ...



---

Dell Cameron is an investigative journalist in Texas covering national security and tech policy. He's a recipient of multiple Society of Professional Journalists awards and co-recipient of an Edward R. Murrow Award for Investigative Reporting. Previously, he was a senior reporter at Gizmodo and staff writer for the Daily Dot.

SENIOR REPORTER, NATIONAL SECURITY

Dhruv Mehrotra (he/him) is an investigative data reporter for WIRED. He uses technology to find, build, and analyze datasets for storytelling. Before joining WIRED, he worked for the Center for Investigative Reporting and was a researcher at New York University's Courant Institute of Mathematical Sciences. At Gizmodo, he was on... Read more

STAFF WRITER

TOPICS PRIVACY SURVEILLANCE NSA JOE BIDEN WHITE HOUSE

MORE FROM WIRED

## Senate Leaders Plan to Prolong NSA Surveillance Using a Must-Pass Bill

Top senate officials are planning to save the Section 702 surveillance program by attaching it to a crucial piece of legislation. Critics worry a chance to pass privacy reforms will be missed.

DELL CAMERON

## A New US Privacy Bill Seeks to End Warrantless Police and FBI Spying

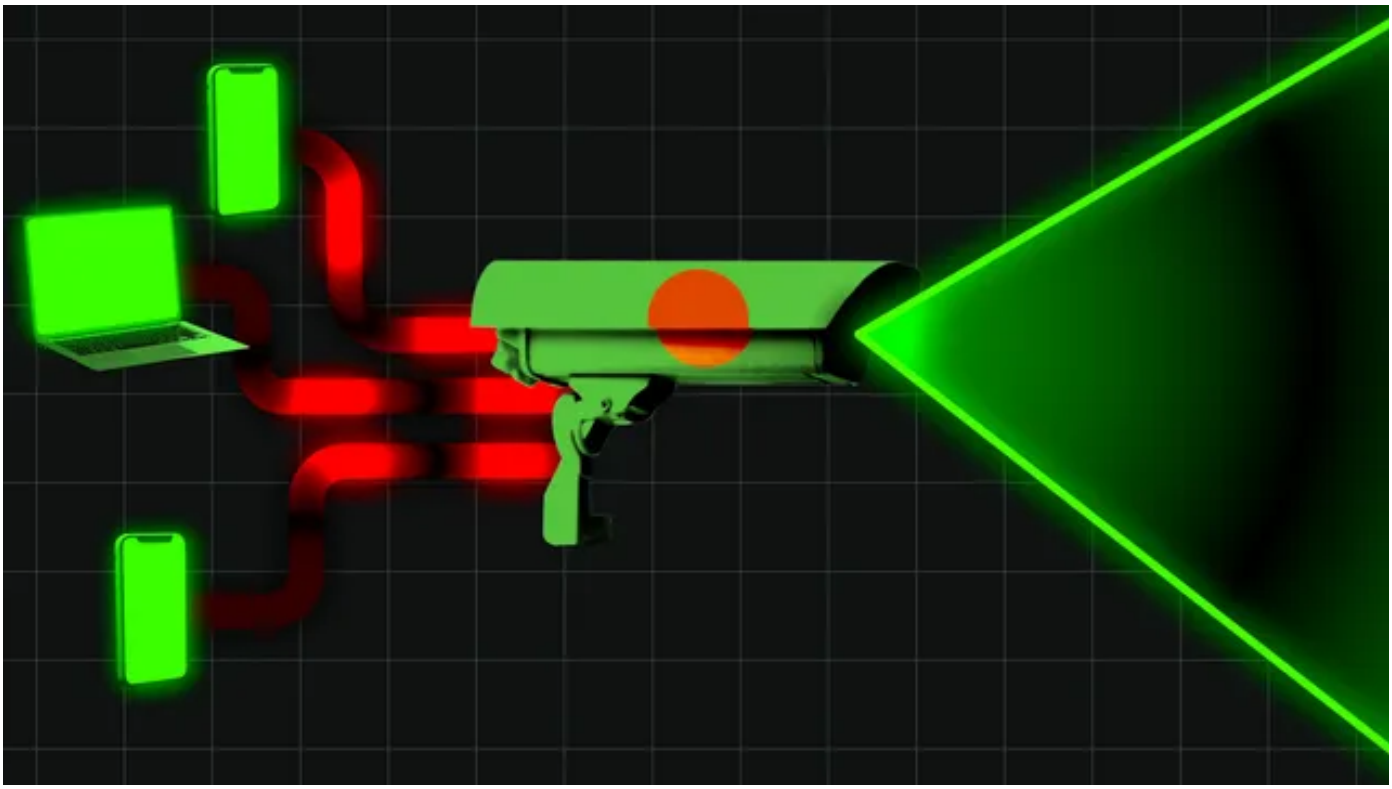
The Government Surveillance Reform Act of 2023 pulls from past privacy bills to overhaul how police and the feds access Americans' data and communications.

DELL CAMERON

## US Congress Report Calls for Privacy Reforms After FBI Surveillance 'Abuses'

A new report by an oversight committee in the US House of Representatives says the FBI has routinely violated rules governing FISA's Section 702 surveillance program and must be reined in.

DELL CAMERON



## A Spy Agency Leaked People's Data Online—Then the Data Was Stolen

The National Telecommunication Monitoring Center in Bangladesh exposed a database to the open web. The types of data leaked online are extensive.

MATT BURGESS

## Asian Americans Raise Alarm Over 'Chilling Effects' of Section 702 Surveillance Program

More than 60 groups advocating for Asian American and Pacific Islander communities are pushing the US Congress to reform the Section 702 surveillance program as Senate leaders move to renew it.

DELL CAMERON

## The Startup That Transformed the Hack-for-Hire Industry

Plus: The FBI's baffling inaction on a ransomware group, a massive breach of Danish electric utilities, and more.

ANDY GREENBERG

## This Is the Ops Manual for the Most Tech-Savvy Animal Liberation Group in the US

For the first time, guerrilla animal rights group Direct Action Everywhere reveals a guide to its investigative tactics and toolkit, from spy cams to night vision and drones.

ANDY GREENBERG

# Electronic Communications Searches The New California Law

*A new law in California ensures that law enforcement can't snoop around your digital data without first obtaining a warrant.*[1]

Effective January first, California's comprehensive Electronic Communications Privacy Act (CalECPA) became law. As the result, a search warrant is now ordinarily required to obtain copies of any electronic communication content or related data that was sent to or received by a suspect or anyone else.[2] This includes email, voicemail, text messages, subscriber information, and cell site tracking data. CalECPA also changed the required form and notice requirements of electronic communications search warrants. It accomplished all of this by adding, deleting, or modifying several sections of the Penal Code.

The consequences of these changes for law enforcement are enormous because they restrict when and how officers can obtain an entire class of information which has become crucial in many criminal investigations. They do, however, provide clarity to this important area of the law which, until now, was regulated by the federal government's disordered hodgepodge known as the Electronic Communications Privacy Act (ECPA).

One of the problems with the ECPA is that it went into effect in 1986, which was several years before electronic communications became the dominant means of personal and business contact in the United States and virtually everywhere else. As the result, it enabled officers to obtain this content and data without too much difficulty. And few people complained because most people had not yet come to view electronic communications as highly private. They do now.

As these changes were occurring, the providers of electronic communications services (especially their attorneys) were becoming more and more nervous about privacy lawsuits that might result if they continued to release this information without a search warrant. So, many of them took the position that officers must obtain a warrant for almost everything, even if the ECPA might have required only a low-level court order known as a D-Order. Moreover, many judges in California were refusing to sign D-Orders because California law did not expressly authorize them to do so. And then the Sixth and Ninth Circuits issued persuasive opinions in which they ruled that, even if the ECPA did not require a search warrant, the Fourth Amendment *did*.

Congress did, however, occasionally attempt to update the ECPA by enacting legislation such as the Stored Communications Act, the Communications Assistance for Law Enforcement Act, the Patriot Act in 2001, and the Foreign Intelligence Surveillance Amendments Act in 2008. But this legislation did not satisfactorily address the general public's concern about the privacy. So the California Legislature took the initiative and, as reported by the national news media, passed CalECPA. (It has been reported that Congress may be using CalECPA as the blueprint for a new federal privacy bill.)

In this article, we will explain the fundamentals of the new law. But first, it is important to note that it was passed by a two-thirds majority of the Legislature which means that any evidence obtained in violation of the law may be suppressed.[4] Also note that because CalECPA is more strict than ECPA, officers who comply with the California law will be in compliance with federal law.

---

[1] FindLaw.com, "Digital Searches Now Require Warrants in California" (October 14, 2015) www.findlaw.com/technologist.
[2] See Pen. Code § 1546 et seq. Also see Pen. Code § 1524.3.
[3] See Pen. Code § 638.50 et seq.
[4] See Pen. Code § 1546.4; *People v. Hull* (1995) 34 Cal.App.4th 1448, 1455; *In re Lance W.* (1985) 37 Cal.3d 873.

One other thing: the information we will discuss in this introductory article is based on our understanding of CalECPA at the time we went to press. It will take a while before the Legislature and our appellate courts resolve some of the uncertainties and dubious provisions in the law. We will, of course, report on these developments as they occur.

## The New Regulations

CalECPA covers nearly every form of stored electronic communications and data about such communications that might be relevant in a criminal investigation. This includes communications and data that were stored in a physical device to which officers made a physical or electronic contact (e.g., the suspect's cell phone), and information stored in equipment owned or operated by a provider(e.g., voicemail, subscriber records).[5] It also includes real time interception of cell site location information and pen register/phone trap information.

**ELECTRONIC COMMUNICATION INFORMATION**: As used in CalECPA, the term "electronic communication information" includes any information *about* a communication (a.k.a. "metadata.") Examples include the names of the sender and recipient of an email or text message; the time or date the communication was created, sent, or received; the IP address of a person's computer and the websites visited by that computer including the date and time of the visit.[6] The term also includes the message and cell site location information, but these subjects will be discussed separately.

It is easy to remember the requirements for obtaining electronic communication information. That's because there is only one: Officers must obtain a search warrant.[7] (It is noteworthy, and disturbing, that the Legislature decided not to permit the warrantless release of this information when it could save a life or prevent great bodily injury.)

**SUBSCRIBER INFORMATION**: The term "subscriber information" means general information which the subscriber submitted to the provider in order to open or maintain an account. This includes the subscriber's name, address, phone number, email address, and "similar contact information" It also includes the length of service and the types of services utilized by the subscriber.[8]

Although CalECPA provides a definition of "subscriber information," it exempted this information from its definition of "electronic communication information."[9] So we do not know for sure what officers must do to obtain it. One possibility is that providers may release it without a warrant if it is relevant to an investigation.[10] But until this is clarified, they may require a warrant.

**ELECTRONIC COMMUNICATIONS**: The term "electronic communication information" also includes the spoken and written words in a communication that has been stored in an electronic communications device or in equipment owned or operated by a service provider. Because "content" was included in the definition of "electronic communication information," it can only be obtained by means of a search warrant.[11] But if officers believe they have probable cause to search for communications or data stored in a device in their custody, they may seize it and promptly seek a warrant.[12]

**CELL SITE LOCATION INFORMATION**: "Cell Site Location Information" (CSLI) is information that identifies the physical locations of cell towers or other sites that were utilized by a provider in transmitting information to or from a particular cell phone or other device which utilized cell sites. CSLI has become useful to law enforcement because, by knowing the locations of the cell sites which carry a suspect's messages and transmission data, officers can essentially "follow" the suspect's phone and, thereby, the suspect.

---

[5] See Pen. Code § 1546.1(a)(3).
[6] See Pen. Code § 1546(d). Also see Pen. Code § 1524.3.
[7] See Pen. Code § 1546.1(b)(1); Pen. Code § 1546(b)(2).
[8] Pen. Code § 1546(l).
[9] See Pen. Code § 1546(d) [electronic communication information "does not include subscriber information"].
[10] See Pen. Code § 1546.1(f).
[11] See Pen. Code § 1546(d) ["contents"]; Pen. Code § 1546.1(b).
[12] See *Riley v. California* (2014) __ U.S. __ [134 S.Ct. 2473, 2486].

For no apparent reason, CSLI falls into three categories: "electronic communication," "electronic communication information," and "electronic device information.[13] This seems to mean it can be obtained by means of a search warrant, exigent circumstances, or "specific consent."[14] We will discuss the term "specific consent" below in the section "Consent, probation and parole searches."

There are two types of CSLI: historical and prospective. "Historical" CSLI consists of records pertaining to cell transmissions that occurred in the past.[15] For example, if officers wanted to know if a murder suspect had been near the location where the victim's body had been found, they would seek historical data for the relevant time period.

The other type of CSLI—"prospective" information—consists of cell site data that will be obtained *after* a court issues a search warrant, or *after* officers determined that CSLI was needed because of exigent circumstances. Prospective information is usually obtained in real time, meaning it is sent directly from the provider's equipment to an investigator's computer, tablet, or cell phone. For example, if officers wanted to follow a suspect by means of cell tower transmissions (or GPS) they would seek prospective data.

One method of obtaining prospective CSLI is through equipment owned or operated by a cell phone provider. This can be accomplished by having the provider "ping" the target's phone, which means transmitting an electronic signal that instructs the phone to disclose its current location. This information is then disseminated to officers in real time or through periodic reports.[16]

CSLI can also be obtained by means of a "cell site simulator." These are mobile devices that, when near the target's phone, essentially trick it into believing that the simulator is a cell site, and that it is the closest and most powerful cell site in its vicinity. This causes the cell phone to send the phone's current location It may also do a variety of more intrustive things. For example, when we went to press, cell site simulators were a hot topic in the news media because it was alleged in a privacy lawsuit that they can intercept communications as well as data.

**PEN REGISTERS AND PHONE TRAPS**: A "pen register" is a device or software application that records or decodes the phone numbers that are dialed on the target's phone over a particular period of time.[16] A "phone trap" or "trap and trace device" functions like a pen register but, instead of obtaining phone numbers dialed on the target's phone, it identifies the phone numbers of devices from which calls to the phone were made.[18]

Although pen registers and phone traps serve important functions in law enforcement, it is uncertain whether officers may obtain authorization to install and monitor them via a court order, or whether a search warrant is required. That is because the Legislature passed two bills in 2015—Senate Bill 178 and Assembly Bill 929—which establish different requirements for utilizing these devices. Specifically, SB 178 requires a warrant, while AB 929 requires a court order that does not require probable cause. In fact, AB 929 requires only a officer's declaration that the data which is likely to be obtained via the pen register and/or phone trap is relevant to an ongoing criminal investigation.

Based on its analysis of these two bills, the California Department of Justice concluded that AB 929 was superseded by SB 178 which would mean that a search warrant would be required. It appears that one reason for this conclusion is that SB 178 was the bill that established the comprehensive change in the law which we discussed earlier in this article,

[13] See Pen. Code §§ 1546(c); 1546(d); Pen. Code § 1546(g).
[14] See Pen. Code § 1546.1(b); Pen. Code § 1546.1(c).
[15] See *U.S. v. Graham* (4th Cir. 2015) __ F.3d __ [2015 WL 4637931]
[16] See *People v. Barnes* (2013) 216 Cal.App.4th 1508, 1511; *U.S. v. Skinner* (6th Cir. 2012) 690 F.3d 772, 778.
[17] See Pen. Code § 638.50(b).
[18] See Pen. Code § 638.50(c).
[19] See Pen. Code § 638.52.
[20] See Pen. Code § 638.52.
[21] See Pen. Code § 638.52(d); Pen. Code § 638.52(e).

while AB 929 pertained only to pen registers and phone traps. Although the Legislature is expected to correct this oversight, it usually takes some time which means that, until then, officers may need a search warrant.

## Consent, probation and parole searches

**CONSENT SEARCHES**: Per CalECPA, the only type of search that can be conducted pursuant to the suspect's consent is a search for "electronic device information" which is defined as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device" (i.e., CSLI).[24] But such consent must constitute "specific consent," a new type of consent discussed next under "Probation searches."

**PROBATION SEARCHES**: It is not clear whether officers may search a probationer's cell phone or other electronic communications device pursuant to a probation search condition that authorizes warrantless searches of property under the control of the probationer. Although the legal basis for probation searches is "consent,"[25] CalECPA requires something it calls "specific consent," which it defines as "consent provided directly to the government entity seeking information."[26] What does this mean?

It seems to mean that searches of electronic communications devices are not covered under the scope of a probation search. That is because such consent is not given "directly" to officers—it is given directly to the sentencing judge in exchange for the judge's agreement not to send the probationer directly to jail or prison. Assuming that's what "specific consent" means, it admittedly represents irrational legislative overreaching. After all, it would mean that officers may search the probationer's entire home and its contents—including documents and personal property—but not his cell phone. Why should a person's cell phone be entitled to more privacy than his home? This is a question the Legislature should be required to address.

**PAROLE SEARCHES**: Unlike probation searches, parole and postrelease community supervision (PRCS) searches are mandated by statute,[27] which means that officers will need a search warrant. (Again, it seems strange that, as with probationers, officers may search the parolee's entire home pursuant to the terms of parole but not his cell phone.)

## Warrantless searches permitted

Although a warrant is ordinarily required to search electronics communications devices and records, CalECPA expressly authorizes the following warrantless searches:

**ABANDONED DEVICES**: Officers may search a cell phone if they have a good faith belief that it is lost, stolen, or abandoned. However, they must limit the search to files or other information that may help "identify, verify, or contact the owner or authorized possessor of the device."[28]

**INFORMATION VOLUNTARILY DISCLOSED**: Neither a search warrant nor other authorization is required to search or seize information that is voluntarily disclosed to an officer by the intended recipient of the information.[29]

**CELL PHONES IN PRISONS**: Although it sounds obvious, a warrant is not ordinarily required to search for records stored in a cell phone that was apparently abandoned in a state prison.[30] POV

***Note:*** *We have three new search warrant forms that may be used to obtain electronic communications and data from the following: a communications provider, a device in police custody, and a device not in police custody; e.g., the suspect's cell phone. To obtain these forms in Microsoft Word format, send an email from a departmental email address to pov.alcoda.org.*

---

[22] See Pen. Code § 638.53(a).
[23] See Pen. Code § 638.53(b).
[24] See Pen. Code § 1546.1(c)(3).
[25] See *People v. Bravo* (1987) 43 Cal.3d 600, 608; *People v. Medina* (2008) 158 Cal.App.4th 1571, 1575.
[26] See Pen. Code § 1546(k); Pen. Code § 1546.1(c)(3).
[27] See Pen. Code § 3067(a) [standard parole]; Pen. Code § 3453(f) [PRCS].
[28] See Pen. Code § 1546.1(c)(6).
[29] See Pen. Code § 1546.1(a)(3).
[30] See Pen. Code § 1546.1(c)(7).