

1 Michael T. Risher (State Bar No. 191627)
2 LAW OFFICE OF MICHAEL T. RISCHER
2081 Center St. #154
3 Berkeley CA 94702
4 Email: michael@risherlaw.com
T: (510) 689-1657
F: (510) 225-0941

5 Stephanie J. Lacambra (State Bar No. 232517)
6 Lee Tien (State Bar No. 148216)
7 ELECTRONIC FRONTIER FOUNDATION
8 815 Eddy Street
9 San Francisco, California 94109
T: (415) 436-9333 x130
F: (415) 436-9993
Email: stephanie@eff.org

10 Attorneys for Plaintiff
11 Electronic Frontier Foundation

FILED
SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN BERNARDINO
SAN BERNARDINO CIVIL DIVISION

OCT 23 2018

BY 
VERONICA GONZALEZ, DEPUTY

12
13 SUPERIOR COURT OF CALIFORNIA
14 COUNTY OF SAN BERNARDINO

15 ELECTRONIC FRONTIER FOUNDATION,)
16)
17 Plaintiff,)
18 v.)
19 COUNTY OF SAN BERNARDINO,)
20 JOHN MCMAHON, SHERIFF-CORONER OF)
21 THE COUNTY OF SAN BERNARDINO,)
Defendants.)

Case No. CIVDS1827591
**Verified Petition for
Writ of Mandate to Enforce
California Public Records Act**
General civil—equity
Judge:
Department:

1 1. The 2015 California Electronic Communications Privacy Act requires California law-
2 enforcement agencies to provide the California Department of Justice with certain information about
3 search warrants they obtain for electronic information. It also requires the Department of Justice to
4 publish information about these warrants on its website. Plaintiff Electronic Frontier Foundation
5 (“EFF”) requested copies of six of these search warrants that Defendants obtained in 2017, along with
6 their supporting affidavits.

7
8 2. Each of these warrants authorized Defendants’ personnel to use cell site simulator
9 devices as part of a criminal investigation. These devices, commonly known as Stingrays (a brand
10 name), masquerade as cell-phone towers and allow law enforcement to locate specific cell phones by
11 diverting these phones’ signals to the simulator, rather than to the carrier’s real tower. They can also be
12 used to determine the unique international mobile subscriber identifiers of unknown devices.

13 3. The Legislature recognized that the use of these devices can have profound civil liberties
14 implications. And as Defendants’ own use policy explains, a cell site simulator collects identifying and
15 location information and may cause a “temporary disruption of service” not only of the target device,
16 but of all other cell-phones within range. The Legislature has therefore imposed a number of
17 limitations and transparency requirements on their use, as discussed below.

18 4. In an attempt to learn about Defendants’ use of these devices, EFF sent a request for
19 records relating to six cell site simulator warrants that precisely identified each warrant using the
20 information on the Department of Justice’s OpenJustice website, including the date range of the
21 authorized search, the nature of the investigation, the items to be searched for, and the exact date and
22 time Defendants electronically provided information about them to the Department of Justice.

23
24 5. Defendants refused to comply with the request, claiming that it failed to reasonably
25 describe the records at issue and that the records are exempt from disclosure as records of an
26 investigation under Government Code § 6254(f).

27 6. Neither of these is a legitimate justification for failing to provide the records:
28

1 7. The request more than reasonably described the target records. In fact, it uniquely
2 identified the warrants in question, providing the exact time frame covered by the warrant, the exact
3 date and time the Defendants provided information about the warrants to the Department of Justice,
4 and other identifying information. Defendants' claim in this regard is particularly weak because their
5 own policy – which state law requires them to adopt and make public – requires their personnel to
6 obtain high-level approval for, and then maintain a log of, all warrants like those here at issue. This log
7 must contain the dates that the cell site simulator was used, which would mirror or be contained within
8 the time frame covered by the warrant, and so would allow Defendants to easily identify and locate the
9 requested warrants.

10
11 8. Search warrants, which are issued by the Court, are public records, as are the supporting
12 affidavits. Penal Code § 1534 (a). In fact, the California Department of Justice has informed EFF that it
13 could, and should, obtain copies of warrants included in its website directly from the agency that
14 obtained them. Although the statutory scheme allows the issuing court to seal this type of warrant for
15 limited time periods under certain conditions, there is no indication that the requested warrants are
16 sealed (Defendants do not suggest that they are, and they appear to claim that they cannot even identify
17 the warrants at issue).

18
19 9. The Court should therefore order Defendants to disclose the requested records under the
20 Public Records Act.

21 **Parties¹**

22 10. Plaintiff Electronic Frontier Foundation ("EFF") is a San Francisco-based, donor-
23 supported, non-profit civil liberties organization working to protect and promote fundamental liberties
24 in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's
25 team of attorneys, activists, and technologists encourage and challenge industry, government, and
26

27 ¹ This Complaint refers to the parties as Plaintiffs and Defendants as authorized by Code of Civil
28 Procedure § 1063.

1 courts to support free expression, privacy, and transparency in the information society. EFF has over
2 37,000 dues-paying members and represents the interests of everyday users of the Internet. EFF was a
3 prominent supporter of the passage of the California Electronic Communications Privacy Act and
4 served as a key advisor to the law's authors, Senators Mark Leno and Joel Anderson, throughout the
5 legislative process.

6 11. EFF is a member of the public under Government Code §§ 6252 (b) and (c) and is
7 beneficially interested in the outcome of these proceedings; it has a clear, present and substantial right
8 to the relief sought herein and no plain, speedy and adequate remedy at law other than that sought
9 herein.
10

11 12. Defendant County of San Bernardino is a public agency within the meaning of
12 Government Code § 6252(d) and is the parent entity of the San Bernardino Sheriff's Department.

13 13. Defendant John McMahon is the Sheriff-Coroner of San Bernardino County and the head
14 of the San Bernardino Sheriff's Department. Plaintiffs name him in his official capacity only.

15 14. Defendants are in possession of the records sought by this Petition.

16 **Jurisdiction and Venue**

17 15. This Court has jurisdiction under Government Code §§ 6258, 6259, Code of Civil
18 Procedure §§ 1060 and 1085, and Article VI section 10 of the California Constitution.

19 16. Venue is proper in this Court: The records in question, or some portion of them, are
20 situated in the County of San Bernardino. *See* Gov. Code § 6259 (a); Code Civ. Proc. § 401(1). In
21 addition, the Defendants reside in, and the acts and omissions complained of herein occurred in, that
22 County. *See* Code Civ. Proc. §§ 393, 395(a).

23 **The California Public Records Act**

24 17. Under the California Public Records Act, Government Code §§ 6250 *et seq.* ("PRA"), all
25 records that are prepared, owned, used, or retained by any public agency must be made publicly
26
27

1 available for inspection and copying upon request, unless they are exempt from disclosure. Gov. Code
2 §§ 6253(a) and (b); 6252(e).

3 18. An agency that receives a request must also “[p]rovide suggestions for overcoming any
4 practical basis for denying access to the records or information sought.” *Id.* § 6253.1. If documents
5 contain both exempt and non-exempt material, the government must disclose all non-exempt material.
6 *Id.* § 6253(a).

7
8 19. “Whenever it is made to appear by verified petition to the superior court of the county
9 where the records or some part thereof are situated that certain public records are being improperly
10 withheld from a member of the public, the court shall order the officer or person charged with
11 withholding the records to disclose the public record or show cause why he or she should not do so.”
12 *Id.* § 6259(a). The government has the burden to justify non-disclosure of any record with specific
13 evidence. “The court shall decide the case after examining the record in camera, [if permitted by the
14 Evidence Code], papers filed by the parties and any oral argument and additional evidence as the court
15 may allow.” *Id.* § 6259(a).

16 20. If the Court finds that the failure to disclose is not justified, it shall order the public
17 official to make the record public. *Id.* § 6259(b).

18 21. The California Constitution provides an additional, independent right of access to
19 government records: “The people have the right of access to information concerning the conduct of the
20 people’s business, and, therefore, the meetings of public bodies and the writings of public officials and
21 agencies shall be open to public scrutiny.” CAL. CONST., ART. 1 § 3(b)(1).

22 22. Mandate lies to compel the government to comply with the PRA and with the California
23 Constitution. *See* Code Civ. Proc. § 1085; Gov. Code § 6258.

24 **Defendants’ Policy on Using Cell Site Simulators**

25
26 23. California law requires law enforcement agencies, including sheriff’s departments, that
27 use cell site simulators to “[i]mplement a usage and privacy policy to ensure that the collection, use,
28

1 maintenance, sharing, and dissemination of information gathered through the use of cellular
2 communications interception technology complies with all applicable law and is consistent with
3 respect for an individual’s privacy and civil liberties.” Gov. Code § 53166(b)(2). Any department that
4 has a website must post this policy on it. *Id.* The local legislative body must authorize that policy
5 before the agency acquires the equipment. *Id.* § 53166(c)(2). A violation subjects the agency to suit. *Id.*
6 § 53166(d).

7
8 24. A true and correct copy of Defendants’ cell site simulator use policy, posted on its
9 website at [http://wp.sbcounty.gov/sheriff/wp-content/uploads/sites/17/2017/07/cell-site-sims-](http://wp.sbcounty.gov/sheriff/wp-content/uploads/sites/17/2017/07/cell-site-sims-04122016.pdf)
10 [04122016.pdf](http://wp.sbcounty.gov/sheriff/wp-content/uploads/sites/17/2017/07/cell-site-sims-04122016.pdf), is attached to this Petition as Exhibit A.²

11 25. This policy summarizes some of the uses of cell site simulators and how the technology
12 works, as follows:

13 26. “Cell site simulator technology may be used to gather information leading to the identity
14 or whereabouts of fugitives, suspects, victims, or missing persons. Authorized Department operators
15 can use cell site simulators to help locate cellular devices whose unique identifiers are already known
16 to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited
17 signaling information from devices in the simulator user's vicinity.” See Exh. A.

18 27. “A cell site simulator receives and uses an industry standard unique identifying number
19 assigned by a device manufacturer or cellular network provider. When used to locate a known cellular
20 device, a cell site simulator initially receives the unique identifying number from multiple devices in
21 the vicinity of the simulator. Once the cell site simulator identifies the specific cellular device for
22 which it is looking, it will obtain the signaling information relating only to that particular phone. When
23 used to identify an unknown device, the cell site simulator obtains signaling information from non-
24

25
26
27 ² This document is archived at <https://web.archive.org/web/20181019180623/http://wp.sbcounty.gov/sheriff/wp-content/uploads/sites/17/2017/07/cell-site-sims-04122016.pdf>.

1 target devices in the target's vicinity for the limited purpose of distinguishing the target device.” See
2 Exh. A.

3 28. This policy states that “Whenever possible, a search warrant supported by probable cause
4 shall be obtained prior to use of a cell site simulator.” See Exh. A. Warrant applications must inform
5 the court about the technology, including the fact that use of a cell site simulator may disrupt cell-
6 phone service to devices in the area that have nothing to do with the investigation. See Exh. A.

7 29. The policy allows only authorized personnel to use these devices: “Cell site simulators
8 may be operated only by trained personnel who have been authorized by the Department to use the
9 technology and whose training has been administered by a qualified Department component or expert.”
10 See Exh. A.

11 30. The policy also requires that “[d]eployment of a cell site simulator by the Department
12 must be approved by a Gang/Narcotics Division supervisor. Any emergency/warrantless use of a cell
13 site simulator must be approved by a Gang/Narcotics Division supervisor, and notice shall be given to
14 the lieutenant of the Gang/Narcotics Division. The Gang/Narcotics supervisor shall be responsible for
15 reviewing all court paper work, or any facts giving rise to an emergency situation, to insure compliance
16 with this policy and the law.” See Exh. A.

17 31. The policy also requires that “[a] cell site simulator log shall be maintained tracking
18 every use of a cell site simulator by the Department. See Exh. A. The log shall contain:

- 19 • Date(s)/time(s) of use
- 20 • Suspected crime(s), if applicable
- 21 • Location(s) used
- 22 • Associated DR numbers, if applicable
- 23 • Phone # and/or device ID
- 24 • If use of the device was at the request of an outside agency, the outside agency and
25 case agent

- Whether a phone was successfully located or identified.”

32. This policy was in place at the time the warrants at issue were obtained.

CalECPA and the Records at Issue

33. In 2015, the California Legislature passed the Electronic Communications Privacy Act (CalECPA), SB 178, codified at Penal Code § 1546 *et seq.*

34. As the Legislative Counsel’s Digest to the law explains, CalECPA is meant to “prohibit a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions, except for emergency situations, as defined.”

35. The law therefore generally requires law-enforcement agencies to obtain a warrant or wiretap order before they “[a]ccess electronic device information by means of physical interaction or electronic communication with the electronic device,” unless one of the enumerated exceptions applies. Penal Code § 1546.1(a)(3), (c).

36. Warrants issued under this provision must comply with all statutory and constitutional warrant requirements, and must additionally comply with a number of special requirements intended to protect privacy. *Id.* § 1546.1(d)(1)-(3).

37. In addition, agencies that execute these warrants must provide notice to the person searched, if known. *Id.* § 1546.2(a). This notice must generally occur when the information is obtained or, in an emergency, within 3 days. *Id.*

38. If the agency believes that providing this notice will create an “adverse result” – for example, that it may lead to the destruction of evidence or the suspect’s flight – it may apply to the court for an order allowing it to delay notice. *Id.* § 1546.2(b); *see id.* § 1546(a) (defining “adverse result”). If the court finds that providing notice will have an adverse result, it may allow the agency to

1 delay notice for up to 90 days. *Id.* The agency may apply for, and the court may grant, multiple
2 extensions. *Id.*

3 39. If the agency does not know the identity of the person whose information has been
4 obtained – as is the case with the warrants here at issue – it must provide information about the warrant
5 to the Department of Justice within 3 days of executing the warrant. *Id.* § 1546.2(c). Again, if it
6 believes that release of the information could compromise the investigation, it may apply to the court
7 for 90-day delay in notice. *Id.* It must then provide the required information to the Department of
8 Justice. *Id.*

9
10 40. Agencies provide this information through an online portal, the Department of Justice’s
11 California Law Enforcement Website. In addition to the information discussed above, they must
12 provide the date the warrant was signed and upload the warrant itself.

13 41. Once the Department of Justice receives this information, it must publish information
14 about the warrants on its website. *Id.*

15 42. The Department of Justice publishes this information on its OpenJustice Data Portal,
16 under Electronic Search Warrant Notifications, at <https://openjustice.doj.ca.gov/data>.³ The published
17 information for 2017 includes the name of the agency that sought and executed the warrant, the issuing
18 court, the date and time the agency submitted the information electronically to the Department of
19 Justice, the nature of the investigation, the start and end date of the information sought, the grounds for
20 issuance of the warrant, the reasons for any delay in providing notice, and whether or not the search
21 involved an emergency.

22
23 43. A true and correct copy of EFF’s initial PRA request (“Request”) is attached to this
24 Petition as Exhibit B and shows the information fields that the Department of Justice OpenJustice
25 website provides.

26
27 ³ This webpage is archived at
<https://web.archive.org/web/20181019183126/https://openjustice.doj.ca.gov/data>.

1 44. Researchers and journalists use the information on this website to inform the public about
2 law-enforcement implementation of and compliance with CalECPA and departmental policies.

3 45. For example, in July 2018 the Palm Springs Desert Sun reported that this information
4 indicated that “San Bernardino County’s law enforcement agencies were granted the most electronic
5 warrants to search digital property per resident in the state, according to the data. The San Bernardino
6 County Sheriff’s Department accounts for almost all of the electronic search warrants reported to the
7 California Department of Justice for the county. And the department is carrying out the electronic
8 searches at an increasing rate.” Christopher Damien and Evan Wyloge, *In San Bernardino County,*
9 *you’re 20 times more likely to have your Facebook, iPhone secretly probed by police*, Palm Springs
10 Desert Sun, July 23 and 24, 2018, available at [https://www.desertsun.com/story/news/2018/07/23/san-](https://www.desertsun.com/story/news/2018/07/23/san-bernardino-countys-electronic-records-probed-most-california/820052002/)
11 [bernardino-countys-electronic-records-probed-most-california/820052002/](https://www.desertsun.com/story/news/2018/07/23/san-bernardino-countys-electronic-records-probed-most-california/820052002/) The article noted that 93%
12 of the CalECPA warrants reported to the state by the San Bernardino Sheriff’s Department “were
13 granted to investigate people whose identity was unknown to the department,” and that privacy
14 advocates found this “surprising.” *Id.*

15
16 46. The article also stated that the sheriff’s “department did not provide an explanation for
17 why they are investigating the digital property of so many people before identifying them,” calling the
18 department’s “lack of transparency” a “concern for privacy watchdogs” and stating that advocates
19 “wonder whether the San Bernardino County Sheriff’s Department’s high rate is related to the
20 agency’s controversial history with digital surveillance.” *Id.*

21
22 47. However, the Department of Justice OpenJustice website does not provide sufficient
23 detail about the warrants to allow a full evaluation of how they are being used.

24 48. In particular, that website does not contain the warrants themselves or the warrant
25 numbers, at least not for the warrants here at issue. Having the warrant number would allow a member
26 of the public to obtain the warrant, the supporting affidavit, and related documents from the issuing
27 court. Without these numbers, it is not practicable to obtain these documents from the court. These

1 documents would allow additional assessment of whether the requesting agency was following the law
2 and its own policies relating to obtaining these warrants and any orders delaying disclosure.

3 **Plaintiff's Records Request and Defendants' Response**

4 49. In August 2018, EFF Senior Investigative Researcher David Maass emailed a written
5 request on behalf of Plaintiff EFF to Defendant San Bernardino County Sheriff's Department for
6 records under the Public Records Act. See Exh B (references in this Complaint to "Request" are to this
7 Exhibit).

8
9 50. This Request asked for search warrants related to six specific searches, as well as the
10 search warrant numbers associated with these specific warrants, that appeared on the Department of
11 Justice's OpenJustice website. See Exh B.

12 51. The Request identified each warrant by providing all of the information about each
13 warrant that appears on the Department of Justice's OpenJustice website, information that Defendant
14 Department had provided to the Department of Justice and that the Department of Justice had then
15 posted verbatim on its website, with possible redactions as allowed by statute.

16 52. The Request indicated that the "primary nature" of each warrant/investigation was listed
17 on the website as homicide.

18 53. The Request indicated that the "secondary nature" of each warrant/investigation was
19 listed on the website as "gang related."

20 54. The Request indicated that the "items to be searched for" relating to each
21 warrant/investigation was listed on the website as including "Cell Site Stimulator [sic]," in addition to
22 other identifying information. The erroneous substitution of "stimulator" for "simulator" on the website
23 appears only in information provided by Defendants, indicating that the error originated with
24 Defendants.
25
26
27

1 55. The Request indicated the precise start and end dates for each warrant. This information
2 should correspond with the date-of-use information that the Defendant’s policy requires its personnel
3 to record.

4 56. The Request quoted verbatim the grounds for issuance of each warrant.

5 57. The Request quoted verbatim the cause for delay in providing notification given for each
6 warrant.

7 58. The Request also listed the precise date and time that the Department had electronically
8 submitted the information about each warrant to the Department of Justice. This information is
9 automatically generated by the electronic submission system.

10 59. This information is sufficient to allow Defendants to identify and locate the requested
11 records.

12 60. On August 31, 2018, Defendant County responded to the Request by confirming receipt,
13 but refusing to release any records. A true and correct copy of Defendant’s Response (“Response”),
14 dated August 30 but emailed on August 31, 2018 is attached as Exhibit C to this Petition.

15 61. This Response asserted that the Request was “vague, overly broad, and does not
16 reasonably describe an identifiable record.” See Exh. C. It additionally asserted that the requested
17 records were exempt from disclosure under the PRA, including the exemption for records of
18 investigation and official information.

19 62. The County’s Response also claimed that the records would be withheld because “there is
20 a necessity for preserving the confidentiality of the information that outweighs the necessity for
21 disclosure,” even as it simultaneously claimed that the “information provided [in the Request] does not
22 contain sufficient information to allow the Department to conduct a search of its records.”

23 63. On September 7, 2018, Mr. Maass sent an email to Defendant County explaining that the
24 Department of Justice had specifically informed him that he should (and could) obtain search warrant
25 numbers for warrants listed on the OpenJustice website directly from the agency that had obtained the
26

1 warrant. This email also explained why the County should release the records. When he did not
2 receive a response, he sent an additional email on September 10, 2018, requesting a telephone call to
3 discuss the issue. A true and correct copy of this email string (“Email”) is attached as Exhibit D to this
4 Petition.

5 64. Neither Mr. Maass nor EFF itself received a response to these emails; nor did either of
6 them receive any of the requested records.

7 **List of Exhibits**

8 65. Exhibit A to this Petition is a true copy of Defendants’ cell site simulator use policy,
9 downloaded from its website.

10 66. Exhibit B to this Petition is a true copy of Plaintiff’s PRA request to Defendants.

11 67. Exhibit C to this Petition is a true copy of Defendants’ response to Plaintiffs’ PRA
12 request.

13 68. Exhibit D to this Petition is a true copy of an email exchange between EFF Senior
14 Investigative Researcher David Maass and Defendants agent regarding EFF’s PRA request.

15 **FIRST CAUSE OF ACTION** 16 **For Writ of Mandate to Enforce the California Public Records Act and** 17 **Article I, § 3 of the California Constitution**

18 (Plaintiff EFF v. Both Defendants)

19 69. Plaintiff incorporates herein by reference the above allegations, as if set forth in full.

20 70. The PRA requires the disclosure of the requested records in whole or in part.

21 71. Defendants’ failure to provide the requested records violates the PRA and Article I, § 3 of
22 the California Constitution.

23 **Wherefore**, Plaintiff requests the following:

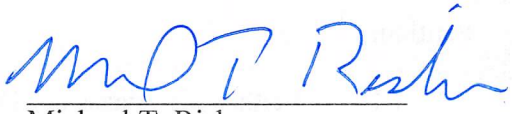
- 24 1. That the Court issue a writ of mandate directing Defendants to provide
25 Plaintiff EFF with all requested records except those records or parts thereof that the
26 Court determines may lawfully be withheld;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

2. That Plaintiff be awarded attorneys' fees and costs under Gov. Code § 6259 and any other applicable statutes or basis;

3. For such other and further relief as the Court deems proper and just.

Dated: 10/22/2018

By: 
Michael T. Risher
Attorney for Plaintiff EFF

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Verification

I, Corynne McSherry, am the Legal Director of the Electronic Frontier Foundation and authorized to verify this Petition as an officer. I have read this Verified Petition for Writ of Mandate in *Electronic Frontier Foundation v. County of San Bernardino* and am informed, and do believe, that the matters herein are true. On that ground I allege that the matters stated herein are true.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATED: 10/22/18 at San Francisco, CA



Corynne McSherry

1 **Verification**

2 I, David Maass, am a Senior Investigative Researcher at the Electronic Frontier Foundation. I
3 have read paragraphs 4, 5, 10, 11, 24-31, 40, 42-58, 60-68 of the foregoing Verified Petition for Writ
4 of Mandate in *Electronic Frontier Foundation v. County of San Bernardino*. The facts alleged in those
5 paragraphs are within my own knowledge and I know these facts to be true.

6 I declare under penalty of perjury under the laws of the State of California that the foregoing
7 is true and correct.

8
9 DATED: 10/22/18 at San Francisco, CA

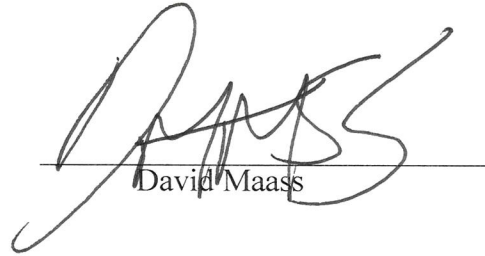
10 
David Maass

Exhibit A



Interoffice Memo

DATE: April 12, 2016

PHONE:

FROM: Dave Williams, Assistant Sheriff

TO: All Personnel,
Gang/Narcotics Division

SUBJECT	Temporary Order: Use of Cell-Site Simulators
----------------	---

Effective immediately, the following policies shall guide members in their usage of cell site simulators.

Cell-Site Simulator Policy: Introduction

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell-site simulators fulfill critical operational needs. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and public safety missions, as well as the Department's commitments to accord appropriate respect for individuals' privacy and civil liberties. This policy provides guidance and establishes common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way. The Department's individual divisions may issue additional specific guidance consistent with this policy.

Authorized Purposes and Use of Cell-Site Simulator

Cell site simulator technology may be used to gather information leading to the identity or whereabouts of fugitives, suspects, victims, or missing persons. Authorized Department operators can use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-

site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department cannot, and shall not be used to collect the contents of any communication or any data contained on the phone itself, such as emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

Authorized Cell-Site Simulator Operators and Training Requirements

Cell-site simulators require training and practice to operate correctly. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by the Department to use the technology and whose training has been administered by a qualified Department component or expert. This training shall include laws and concerns related to privacy and civil liberties, and, when available, training from the product manufacturer.

Legal Process and Court Orders for Use of Cell-Site Simulator

Whenever possible, a search warrant supported by probable cause shall be obtained prior to use of a cell-site simulator. When making any application to a court, a deputy must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.

Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.

An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

In the case of an emergency involving danger of death or serious physical injury to any person requiring use of cell-site simulator technology without delay, the technology may be deployed prior to obtaining a warrant. In every case of a warrantless use of a cell-site simulator, the authorized operator shall insure that, within three days after the use, an application for a warrant or order authorizing the emergency use of the cell-site simulator is filed with the appropriate court. The application shall set forth the facts giving rise to the emergency and probable cause.

Department Monitoring of Use of Cell-Site Simulators

Deployment of a cell-site simulator by the Department must be approved by a Gang/Narcotics Division supervisor. Any emergency/warrantless use of a cell-site simulator must be approved by a Gang/Narcotics Division supervisor, and notice shall be given to the lieutenant of the Gang/Narcotics Division. The Gang/Narcotics supervisor shall be responsible for reviewing all court paper work, or any facts giving rise to an emergency situation, to insure compliance with this policy and the law.

A cell-site simulator log shall be maintained tracking every use of a cell-site simulator by the Department. The log shall contain:

- Date(s)/time(s) of use
- Suspected crime(s), if applicable
- Location(s) used
- Associated DR numbers, if applicable
- Phone # and/or device ID
- If use of the device was at the request of an outside agency, the outside agency and case agent
- Whether a phone was successfully located or identified

A Gang/Narcotics Division supervisor shall routinely inspect the technology to insure any and all data from any completed operation has been successfully erased. Quarterly random audits of the cell-site simulator use log and corresponding search warrants will be conducted by a Gang/Narcotics Division supervisor.

An annual report shall be made to the Board of Chiefs reflecting:

- The total number of times a cell-site simulator was deployed by the Department;
- The number of deployments at the request of other agencies, including State or Local law enforcement; and
- The number of times the technology was deployed in emergency circumstances.

Sharing of Information Gathered by Cell-Site Simulators

A request from an outside agency for investigative assistance from the Department involving the use of a cell-site simulator may be honored upon approval of the Gang/Narcotics Division supervisor.

A cell-site simulator shall only be deployed at the request of an outside agency subject to the following limitations:

- Requested deployment must be for an approved purpose pursuant to this policy.
- If a warrant has been obtained by the outside agency, the warrant application must include sufficient information to ensure that the court was aware of, and authorized the use of, the technology.
- If a warrantless use is requested, the case must involve an emergency involving danger of death or serious physical injury to any person requiring use of cell-site simulator technology without delay.
- No personnel from the outside agency shall use, or observe the use of a cell-site simulator.
- Only location and/or device ID # shall be provided to the outside agency; all data unrelated to the outside agency's investigation shall not be shared, and will be destroyed by the Department.

Retention/Destruction of Information Gathered by Cell-Site Simulators

All information gathered during an approved deployment must be deleted at the conclusion of the operation. The Department's use of cell-site simulators shall include the following practices:

- When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.
- When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.
- Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent investigators know or have reason to believe that information is exculpatory or impeaching they have a duty to memorialize that information.

Exhibit B



August 22, 2018

VIA EMAIL

San Bernardino County Sheriff's Department
 Miles Kowalski, General Legal Counsel
 655 East Third Street
 San Bernardino, California
 92415-0061
 Email: mkowalski@sbcasd.org

RE: California Public Records Act Request

Dear Mr. Kowalski,

This letter serves as a formal request for records under the California Public Records Act (CPRA) from the Electronic Frontier Foundation (EFF). We are seeking the following records:

- 1) Search warrant numbers for these six electronic searches that were disclosed to the California Department of Justice and published at <https://openjustice.doj.ca.gov/>

Agency Name:	County of Court	Submitted	Nature of the investigation	Primary Nature	Crime of Violence Options	Secondary Nature	Order Served on	Business Name	Items to be searched for:	Start Date for Info	End Date for Info	Grounds for Issuance	Reasons for Delay (if any)	Emergency?	Facts giving rise to the emergency
San Bernardino County Sheriffs	San Bernardino	03/30/2018 - 12:16		Homicide		Gang Related	Device Only		Basic subscriber information from a service provider Other transactional and account records from a service provider Addressing information (pen register or trap and trace) Cell Site Stimulator	2017-03-14	2017-04-13	Assist in locating individual		No	
San Bernardino County Sheriffs	San Bernardino	03/30/2018 - 12:24		Homicide		Gang Related	Device Only		Basic subscriber information from a service provider Other transactional and account records from a service provider Addressing information (pen register or trap and trace) Cell Site Stimulator	2017-03-14	2017-04-13	tends to show that a felony has been committed or that a particular person has committed a felony Assist in locating individual	lead to flight from prosecution lead to destruction of or tampering with evidence lead to intimidation of potential witnesses otherwise seriously jeopardize an investigation or unduly delay a trial	No	
San Bernardino County Sheriffs	San Bernardino	03/30/2018 - 12:31		Homicide		Gang Related	Device Only		Location information Cell site stimulator	2017-03-02	2017-04-01	tends to show that a felony has been committed	lead to flight from prosecution lead to destruction of	No	

California Public Records Act Request
 August 22, 2018
 Page 2 of 3

												or that a particular person has committed a felony Assist in locating individual	or tampering with evidence lead to intimidation of potential witnesses otherwise seriously jeopardize an investigation or unduly delay a trial		
San Bernardino County Sheriff's	San Bernardino	03/30/2018 - 12:36	Homicide		Gang Related	Device Only	Basic subscriber information from a service provider Other transactional and account records from a service provider Addressing information (pen register or trap and trace) Cell site stimulator	2017-03-21	2017-04-20	tends to show that a felony has been committed or that a particular person has committed a felony Assist in locating individual	lead to flight from prosecution lead to destruction of or tampering with evidence lead to intimidation of potential witnesses otherwise seriously jeopardize an investigation or unduly delay a trial	No			
San Bernardino County Sheriff's	San Bernardino	03/30/2018 - 12:43	Homicide		Gang Related	Device Only	Location information Cell site stimulator	2017-03-02	2017-04-01	tends to show that a felony has been committed or that a particular person has committed a felony Assist in locating individual	lead to flight from prosecution lead to destruction of or tampering with evidence lead to intimidation of potential witnesses otherwise seriously jeopardize an investigation or unduly delay a trial	No			
San Bernardino County Sheriff's	San Bernardino	03/30/2018 - 12:46	Homicide		Gang Related	Device Only	Location information Cell Site Stimulator	2017-03-02	2017-04-01	tends to show that a felony has been committed or that a particular person has committed a felony Assist in locating individual	lead to flight from prosecution lead to destruction of or tampering with evidence lead to intimidation of potential witnesses otherwise seriously jeopardize an investigation or unduly delay a trial	No			

2) Copies of the search warrants and affidavits associated with the six searches identified above.

We ask that you please respond to this request within 10 days either by providing all the requested records, stating when the records will be made available, or by providing a written response setting forth the legal authority on which you rely in withholding or redacting any records. If your agency invokes an extension, please specify the need for the extension.

We further request the records be provided in an electronic format via email or download in order to save postage and natural resources. Should you be unable to avoid incurring copying costs, EFF will reimburse you for the direct costs of copying these records (if you elect to charge for copying) plus postage. If you anticipate that these costs will exceed \$25.00, or that the time needed to copy the records will delay their release, please

California Public Records Act Request
August 22, 2018
Page 3 of 3

contact me so that I can arrange to inspect the documents or decide which documents I wish to have copied. Otherwise, please copy and send them as soon as possible, and we will promptly pay the required costs.

If you have any questions or concerns, or if I can provide any clarification that will help identify responsive records or focus this request, please do not hesitate to contact me at (415) 436-9333 x151 or dm@eff.org.

Best regards,

Dave Maass
Senior Investigative Researcher
Electronic Frontier Foundation

Exhibit C



JOHN McMAHON, SHERIFF-CORONER

August 30, 2018

Electronic Frontier Foundation
Attn: Dave Maass
Via E-mail Only: dm@eff.org

Re: Public Records Act request – *Electronic Search Warrants*

Dear Mr. Maass:

The San Bernardino County Sheriff's Department ("Department") has concluded its review of the Public Records Act request, wherein you seek: 1) electronic search warrants for six searches that were disclosed to the California Department of Justice, and 2) copies of search warrants and affidavits associated with the six searches attached herewith.

The Department respectfully objects to your request on the grounds that it is vague, overly broad, and does not reasonably describe an identifiable record as required by Government Code section 6253(b). (*Rogers v. Superior Court* (1993) 19 Cal.App.4th 469, 481.) The information provided does not contain sufficient to allow the Department to conduct a search of its records.

Furthermore, records of the kind you describe are investigative records, and/or are contained within confidential investigative files. The Public Records Act "does not require the disclosure of ... [r]ecords of ... investigations conducted by, or records of intelligence information or security procedures of, ... any state or local police agency, or any investigatory or security files compiled by any other state or local police agency..." (Gov. Code, § 6254, subd. (f).) These records are exempt from disclosure whether or not the prospect of enforcement proceedings is concrete and definite (*Haynie v. Superior Court* (2001) 26 Cal. 4th 1061, 1069; *Black Panther Party v. Kehoe* (1974) 42 Cal.App.3d 645, 654; *Younger v. Berkeley City Council* (1st Dist. 1975) 45 Cal.App.3d 825, 833; *American Civil Liberties Union Foundation v. Deukmejian* (1982) 32 Cal.3d 440), and remain protected from disclosure, even after an investigation has concluded. (*Williams v. Superior Court* (1933) 5 Cal. 4th 337, 355-362.) Additionally, "information acquired in confidence by a public employee in the course of his or her duty and not open, or officially disclosed, to the public" is protected by the official information privilege whenever "disclosure of the information is against the public interest because there is a necessity for preserving the confidentiality of the information that outweighs the necessity for disclosure in the interest of justice." (Evid. Code, § 1040; Gov. Code, § 6254, subd. (k).)

For the reasons outlined above, your request is respectfully denied. If you have any questions or concerns, or would like to discuss this matter further, please contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Miles A. Kowalski".

MILES A. KOWALSKI
General Legal Counsel
San Bernardino County Sheriff's Department

MAK/ct

Exhibit D

Subject: Re: Immediate Response Requested: Public Records Act request – Electronic Search Warrants

From: Dave Maass <dm@eff.org>

Date: 9/10/18, 10:30 AM

To: "Kowalski, Miles" <mkowalski@SBCSD.ORG>

CC: "Torres, Cesia" <ctorres@SBCSD.ORG>, Robert Morgester <Robert.Morgester@doj.ca.gov>

Mr. Kowalski,

Dave Maass from the Electronic Frontier Foundation writing again. Are you available for a phone call to discuss this issue further?

On 9/7/18 9:15 AM, Dave Maass wrote:

Good Morning Mr. Kowalski,

In reading your response to my CPRA request, it seems that you misread the request. In your response you indicate that for Item 1, you write that I was seeking the search warrants. This is incorrect: in that item, I was seeking the search warrant numbers.

I am including Robert Morgester of the California Attorney General's office in this response. In August, Mr. Morgester recommended I file requests for warrants/warrant numbers with the individual agencies. He wrote (bolding added):

"The originating agency is always the best source of information as to the search warrant number – they will have the most complete record. **As an example a CPRA request on a originating agency will get you all search warrant numbers.**"

It is surprising that your office claims that our request is "vague, overly broad, and does not reasonably describe an identifiable record" when we filed the request on the recommendation of the California Attorney General. Rather than request all search warrant numbers, we filed a narrow request for only a handful of cases and provided you with granular detail on each one (the same information your agency provided to the Attorney General).

Furthermore, when we filed for substantially similar records with the San Francisco Police Department, they had little issue providing the records requests.

Would it be possible to arrange a call with you as soon as possible, and if necessary with the California Department of Justice? I make this request for assistance pursuant to 6253.1 of the California Public Records Act, which requires your agency to do all of the following:

- (1) Assist the member of the public to identify records and information that are responsive to the request or to the purpose of the request, if stated.*
- (2) Describe the information technology and physical location in which the records exist.*

(3) Provide suggestions for overcoming any practical basis for denying access to the records or information sought.

I should note that I do intend to follow up with further CPRA requests for warrant numbers (and potentially the warrants themselves) associated with electronic searches disclosed to the California Attorney General. Before doing so, it would be best for all sides if we discuss the best way of going about handling these records.

I may be reached at this email address or by phone at 415-436-9333 x151.

Thank you,

Dave Maass

On 8/31/18 3:56 PM, Torres, Cesia wrote:

Please see attached.

Cesia Torres
County Counsel Paralegal to Sheriff's Department
ctorres@sbcisd.org

CONFIDENTIALITY NOTICE: This communication contains legally privileged and confidential information sent solely for the use of the intended recipient. If you are not the intended recipient of this communication, you are not authorized to use it in any manner, except to immediately destroy it and notify the sender.

Sincerely,

--

Dave Maass
Senior Investigative Researcher
Electronic Frontier Foundation
Phone: +1 415-436-9333 x151
Email: dm@eff.org
Twitter: @maassive

--

Dave Maass
Senior Investigative Researcher
Electronic Frontier Foundation
Phone: +1 415-436-9333 x151
Email: dm@eff.org
Twitter: @maassive