Case Info

JUDGE
Mary H. Strobel

CASE NO.
BS158621

HEARING DATE
September 7, 2017

COUNTY
Los Angeles County, CA

DEPARTMENT
82

FILED
September 7, 2017

CATEGORY
Civil

TYPE
Writ - Administrative Mandamus (General Jurisdiction)

STATUS
Pending

MICHELLE OLSON VS THE CITY OF LONG BEACH ET AL

Case No.: BS158621

Michelle Olson, v. The City of Long Beach, et al.

Judge Mary Strobel

Hearing: September 7, 2017

BS158621

Tentative Decision on Petition for Writ of Mandate

Petitioner Michelle Olson ("Petitioner") seeks a writ of mandate compelling Respondents City of Long Beach ("City"), Larry Herrera, and Theressa Graham (collectively "Respondents") to provide unredacted records under the California Public Records Act ("CPRA") in response to a document request dated May 12, 2015 which sought information about cellphone tracking and surveillance devices used by City.

Request to Seal Declaration

With her reply brief, Petitioner submits a request to seal a declaration of a confidential informant referred to as "S." There is an overriding interest in maintaining the confidentiality of S's identity as an informant and the contents of her declaration, which discusses her work as an informant. The court concludes that (1) There exists an overriding interest in sealing S's declaration that overcomes the right of public access to the record; (2) The overriding interest supports sealing the record; (3) A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed; (4) The proposed sealing is narrowly tailored; and (5) No less restrictive means exist to achieve the overriding interest. (CRC 2.550(d).)

Statement of the Case

Petitioner's Public Records Act Request

On May 12, 2015, Petitioner sent a CPRA request to Respondent, which stated the following:

I would like to obtain any documents - such as contracts or agreements -that require or speak to maintaining secrecy about the products, their capabilities, and their use, that police use to observe, conduct surveillance, or analyze information about, people including, as an example, their communications, their lifestyle including associations, and movement. By "analyze information" I mean any computer program that collects or analyzes data that has been collected.

So, specifically, I would like:

A: Agreements about Stingray products and/or with its manufacturer. (Evidently,

StingRay and similar Harris Corporation products can be used to intercept cell

communications content transmitted over-the-air between a target cellular- device and a legitimate service provider cell site. I learned this from Wikipedia.) (Harris Corporation is an American Florida-based international telecommunications equipment company that produces wireless equipment, electronic systems, and antennas for use in the government, defense, and commercial sectors. Headquartered in Melbourne, Florida. Also from Wiki.)

B: Any agreement entered into by the City of Long Beach for surveillance equipment or data collection tools or analysis programs that requires the City of Long Beach to maintain secrets or confidences about the capability or use of the product. (Olson Decl. ¶ 3; Exh. 3.)

Respondent did not respond to the May 12, 2015 request until after this action was filed. On October 21, 2015, Petitioner filed her petition for writ of mandate.[1] 1 On November 16, 2015, Respondent informed Petitioner's counsel that, after diligent search, it was unable to locate any record that it had received the May 12, 2015 request. On January 19, 2016, Respondent mailed to Petitioner approximately 170 pages of documents responsive to her May 12, 2015 request. The documents are, in some cases, heavily redacted. (See Corry Decl. ¶¶ 4-11; Olson Decl. ¶¶ 9-13 and Exh. 5.)

Respondent's January 19, 2016 production of documents apparently did not include a cover letter explaining the reasons for the redactions as required by the CPRA. (Olson Decl. Exh. 5; see Gov. Code § 6253(c); see Gov. Code § 6255(b) [" A response to a written request for inspection or copies of public records that includes a determination that the request is denied, in whole or in part, shall be in writing."].)

Opposition Evidence

In support of the supplemental opposition, Respondents submit the declarations of Lloyd Cox, a lieutenant assigned to the Investigation Bureau of the Long Beach Police Department (LBPD), and of Russell D. Hansen, a supervisory special agent with the Federal Bureau of Investigation (FBI) assigned as Chief, Tracking Technology Unit, Operational Technology Division. Respondents also submit a declaration of Eric Trew, senior counsel for vendor Harris Corporation, and a "List of Exemptions and Justifications re: Redactions." The court summarizes the Cox and Hansen declarations here, and refers to other opposition evidence where relevant in the Analysis section below.

Declaration of Lloyd Cox

In his declaration, Lieutenant Cox discusses the process by which he gathered responsive documents and made redactions about a prior CPRA request that sought information from LBPD about the Stingray technology. For that prior CPRA case, Cox redacted information to protect the technology, information about the vendor (Harris Corporation), and unit pricing, among other information, to prevent potential criminal targets from compiling information to defeat the Stingray technology. Cox redacted information about the identities of undercover detectives and vehicles used. (Cox Decl. ¶¶ 3-6.) Cox also notified the FBI of the first CPRA request about Stingray (not the one in this case) so that the FBI could make redactions to comply with a non-disclosure agreement executed by LBPD and the FBI regarding the Stingray technology. (Id. ¶¶ 7-8.) Finally, for that prior CPRA request, Cox contacted Harris about any specific information that Harris believed was confidential and should be redacted. (Id. ¶ 9.) Cox believes that LBPD kept copies of the previously redacted documents from the prior CPRA case, and used those copies to produce responsive records to Petitioner. (Id. ¶ 11.)

Declaration of Russell D. Hansen

As Chief of the FBI's Tracking Technology Unit, Hansen is responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of FBI investigations. (Hansen Decl. ¶ 1.)

Cell Site Simulators

Hansen states the following about cell site simulator technologies, which include the Stingray products at issue in Petitioner's CPRA request.[2] 2

"Law enforcement agents 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 operator's vicinity." (Hansen Decl. ¶ 4.) "In general, cell site simulators function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower." (Id. ¶ 5.)

"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." (Id. ¶ 6.)

“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 Federal, state, and local law enforcement agencies must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself. The cell site simulator does not remotely capture e-mails, texts, contact lists, images, or other data from the phone, nor does it, as configured, provide subscriber account information (such as an account holder's name, address, or telephone number).” (¶ 7.)

“Use of cell site simulators is predicated on obtaining a search warrant supported by probable cause … unless an exception exists.” (Id. ¶ 8; see Ibid. fn. 3 [exceptions for exigent and exceptional circumstances].)

Non-Disclosure Agreement with LBPD

“Cell site simulator/pen register technology was originally developed under contract with the Federal Government. The United States has authorized two private companies (Digital Receiver Technology (‘DRT’) and Harris Corporation) to manufacture this equipment and since 2010 has expressly conditioned their ability to sell the equipment to state and local law enforcement agencies on specific and controlled terms reflecting its sensitive nature.” (¶ 9.)

“The FCC has issued authorization for manufacturers to sell their equipment to state and local law enforcement agencies with two conditions: (1) the marketing and sale of cell site simulator devices is limited to Federal, state, and local public safety and law enforcement agencies; and (2) state and local agencies must coordinate with the FBI in advance of their acquisition and use of the equipment.” (¶ 10.) “This advance coordination is accomplished through and documented by a Non-Disclosure Agreement (‘NDA’) executed between the state or local law enforcement agency and the FBI.” (¶ 11.)

“The City of Long Beach, via the Long Beach Police Department (‘LBPD’), signed an NDA with the FBI as a prerequisite to purchasing cell site simulator systems from Harris Corp. in 2013.” (¶ 13.) The NDA provides in part:

Disclosing the existence of and the capabilities provided by [cell site simulator equipment and technology] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that [cell site simulator equipment and technology] continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the

public…. (Id., Exh. B.)

LBPD agreed to notify FBI immediately if it received a CPRA request to disclose information concerning the Harris cell site simulator technology so that FBI could seek to prevent disclosure. (Ibid.)

Petitioner’s CPRA Requests

Hansen describes the FBI’s review of Petitioner CPRA request and the reasons the FBI asked LBPD to redact certain information. “Consistent with its practice in similar cases throughout the country, the information the FBI asked LBPD to protect in this matter falls within three general categories: (1) technical specifications and capabilities of cell site simulator systems; (2) techniques and tradecraft employed in operating cell site simulator equipment; and (3) makes and models of cell site simulator systems.” (Id. ¶ 16.) Hansen goes on to explain in broad terms why disclosure of these categories of information could allow criminals and other persons to ascertain law enforcement’s capabilities and limitations with the use of cell site simulators, and to develop countermeasures. (Id. ¶¶ 18-22.)

Procedural History

On October 21, 2015, Petitioner filed her petition for writ of mandate. On January 26, 2016, the court set the petition for hearing on August 30, 2016. The court ordered Petitioner to file and serve her opening brief 60 days before the hearing, Respondent to file and serve its opposition 30 days before the hearing, and Petitioner to file and serve her reply 15 days before the hearing. Petitioner timely filed and served her opening brief on July 1, 2016. Respondent untimely filed and served its opposition on August 5, 2016. Petitioner untimely filed and served a reply on August 17, 2016.

On August 29, 2016, the court granted Respondents’ ex parte application to continue the hearing date on the petition. The court permitted Respondents to submit a supplemental opposition, and Petitioner a supplemental reply. The hearing on the writ petition was subsequently continued to September 7, 2017.

On November 7, 2016, Respondents filed their supplemental opposition to the petition. That same date, the United States filed a statement of interest pursuant to 28 U.S.C. § 517.[3] 3 The United States has not moved to intervene in this action, and has therefore filed its statement of interest as amicus curiae. On January 20, 2017, Petitioner filed a supplemental reply to Respondents’ supplemental opposition and to the United States’ briefing.

Summary of Applicable Law

Pursuant to the CPRA (Gov. Code § 6250, et seq.), individual citizens have a right to access government records. In enacting the CPRA, the California Legislature declared that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state." (Gov. Code, § 6250; see also County of Los Angeles v. Superior Court (2012) 211 Cal.App.4th 57, 63.) To facilitate the public's access to this information, the CPRA mandates, in part, that:

[E]ach state or local agency, upon a request for a copy of records that reasonably describes an identifiable record or records, shall make the records promptly available . . ." (Gov. Code § 6253(b).)

The CPRA defines "public records" submit to its provisions as follows:

(e) "Public records" includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. "Public records" in the custody of, or maintained by, the Governor's office means any writing prepared on or after January 6, 1975. (Gov. Code § 6252(e).)

While the CPRA provides express exemptions to its disclosure requirements, these exemptions must be narrowly construed and the agency bears the burden of showing that a specific exemption applies. (Sacramento County Employees' Retirement System v. Superior Court (2013) 195 Cal.App.4th 440, 453.)

Analysis

The parties do not dispute that the Stingray documents requested by Petitioner are public records. The legal issue is whether Respondents properly redacted certain information as exempt from disclosure under the CPRA.[4] 4

In their supplemental opposition filed November 7, 2016, Respondents argue that the redactions were justified based on three exemptions. First, Respondents contend that redactions were properly made under Government Code section 6254(f) for "records of intelligence information and security procedures." Second, Respondents contend that redacted information about cell site simulator technology was obtained by City in confidence from the FBI pursuant to a NDA, and therefore is exempt under section 6254(k) and Evidence Code section 1040. Finally, Respondents contend the public interest balancing exemption in section 6255 also supports the redactions.

In its statement of interest ("SOI"), the United States relies on the same general exemptions asserted by Respondents.[5] 5

Respondents bear the burden of showing that the redacted information is exempt from disclosure. (Sacramento County Employees' Retirement System v. Superior Court (2013) 195 Cal.App.4th 440, 453.)

Government Code Section 6255

Section 6255 "allows a government agency to withhold records if it can demonstrate that, on the facts of a particular case, the public interest served by withholding the records clearly outweighs the public interest served by disclosure." (City of San Jose v. Sup. Ct. (1999) 74 Cal.App.4th 1008, 1017.) "The burden of proof is on the proponent of nondisclosure, who must demonstrate a 'clear overbalance' on the side of confidentiality." (Id. at 1018.)

"In assigning weight to the general public interest in disclosure, courts should look to the 'nature of the information' and how disclosure of that information contributes to the public's understanding of government." (Humane Society of the United States v. Sup. Ct. (2013) 214 Cal.App.4th 1233, 1268.) "[W]here the requester has alternative, less intrusive means of obtaining the information sought," the public interest in disclosure is lessened. (City of San Jose v. Sup. Ct. (1999) 74 Cal.App.4th 1008, 1020.)

""This catchall exemption 'contemplates a case-by-case balancing process.'" (American Civil Liberties Union of Northern Cal. V. Sup. Ct. (2011) 202 Cal.App.4th 55, 68 (**ACLU**).) In **ACLU**, the court held that an agency must produce evidence, and cannot rely on speculation, to establish a potential threat to security warranting an exemption from disclosure under the CPRA. Citing the California Supreme Court, the court stated that "a mere assertion of possible endangerment is insufficient to justify nondisclosure." (**ACLU**, supra at 74.) The California Supreme Court recently re-emphasized this required inquiry under section 6255: "The critical point is that a court applying section 6255(a) cannot allow 'vague safety concerns' to foreclose the public's right of access." American Civil Liberty Union v. Superior Court (Aug. 31, 2017) 2017 LEXIS 6758 at 24.

In discussing the agency's burden to support its redactions, the **ACLU** court wrote: "'Because the agency has full knowledge of the contents of the withheld records and the requester has only the agency's affidavits and descriptions of the documents, its affidavits must be specific enough to give the requester 'a meaningful opportunity to contest' the withholding of the documents and the court to determine whether the exemption applies.' '[T]he agency must describe 'each document or portion thereof withheld, and for each withholding it must discuss the consequences of disclosing the sought-after information.'" (**ACLU**, supra at 83.)

Public Interest in Disclosure

Respondents do not challenge that there is a public interest in disclosure of agreements and other documents about Stingray products and other technologies used by law enforcement to conduct surveillance using cellular data. The public interest in disclosure of information about the procurement (including costs) and use of this type of law enforcement tool is substantial.

United States argues that Petitioner "does not explain how information regarding the technical specifications and capabilities, make and models, or descriptions of the operational deployment of the equipment" would support her broader inquiry into the privacy concerns and the propriety of using public funds for Stingray technology. (SOI 14.) That there may be a countervailing interest against disclosure (see below) does not mean that the public does not also have an interest in understanding how the Stingray technology works and is used by LBPD. Technical and operational information could assist in the public's understanding of the Stingray technology. Thus, there is a public interest in disclosure of such information.

Public Interest against Disclosure

In its first opposition, Respondents argued inter alia that there is a strong public interest against disclosure because LBPD signed an NDA with FBI and consistently adheres to that agreement. Respondents also argue that disclosure would impact the effectiveness of the program and limit the tactical abilities of law enforcement. (Oppo. 2, 5.) Respondents' first opposition provided no evidence to support these assertions. Respondents' supplemental opposition provides only a conclusory discussion of the balancing under section 6255, but does submit more detailed evidence. (Suppl. Oppo. 3-4.) The United States provides a more robust legal discussion, and relies largely on the Hansen declaration. (SOI 8-18.)

United States cites to two criminal cases that applied the official information privilege under Evidence Code section 1040 to confidential law enforcement information.[6] 6 (SOI 8-9; see People v. Walker (1991) 230 Cal.App.3d 230, 235 ["Just as the disclosure of an informer's identity may destroy his ... usefulness in criminal investigations, the identification of a hidden observation post will likely destroy the future value of the location for police surveillance."]; In re David W. (1976) 62 Cal.App.3d 840, 847 ["To allow public knowledge of the location of the secret identification number would destroy its very purpose and would remove a valuable investigatory device that may lead to the discovery of vehicle thefts."].) Although Walker and David W. are criminal cases, they support the proposition that the balancing under sections 1040 and 6255 weighs for withholding confidential information that, if made public, would undermine the law enforcement purposes of the cell site simulator technology.

In his declaration, Hansen asserts that three categories of information should be protected: "(1) technical specifications and capabilities of cell site simulator systems; (2) techniques and tradecraft employed in operating cell site simulator equipment; and (3) makes and models of cell site simulator systems." (Hansen Decl. ¶ 16.) Hansen states that the three categories are comprised of the following information about cell site simulators:

Category 1 "includes information about capabilities of equipment and capabilities sought through upgrades of equipment; platforms and modes on which the equipment can be operated; functionality; limitations; descriptions of equipment installations; technical specifications of equipment; and information about/descriptions of particular configurations of the equipment." (¶ 16a.)

Category 2 "includes information about the physical locations and platforms on which cell site simulator equipment deployed by LBPD operates, as well as information about how and where the equipment can or would be used." (¶ 16b.)

Category 3 "includes the names and models of cell site simulator systems and the components necessary to configure the systems in various ways." (¶ 16c.)

Hansen explains in broad terms why disclosure of these categories of information could allow criminals and other persons to ascertain law enforcement's capabilities and limitations with the use of cell site simulators, and to develop countermeasures. (Id. ¶¶ 18-22.) The court understands Hansen to be stating that the redactions at issue fall within these categories, although he is unable to provide more specifics in open court without jeopardizing the information. (See Hansen Decl. ¶ 16a-c and footnotes 4-6; and ¶ 21.)

Hansen also submits evidence that LBPD executed an NDA with FBI as a prerequisite to purchasing the cell site simulator systems from Harris Corp. Among other things, LBPD agreed not to disclose publically "any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities)." (Hansen Decl. ¶¶ 13-14, Exh. B.)

Based on Hansen's law enforcement background and duties, the court finds that his testimony is credible and supports a general conclusion that there is a strong public interest against disclosure of confidential technical and operational information that would show how the Stingray technology works. (See Hodai v. City of Tucson (2016) 365 P.3d 959, 965 [FBI declaration supported finding that there was public interest against disclosure for information regarding how Stingray technology works].) For similar reasons, the court also finds a public interest against disclosure of the identities of undercover detectives or vehicles that, if disclosed, could help criminals counteract LBPD's use of the Stingray technology in the field. (See Cox Decl. ¶ 6.) As to redactions that fall within this general category, the court concludes that the public interest in confidentiality clearly outweighs the public interest in disclosure.[7] 7

However, Hansen's declaration lacks specifics as to the redactions at issue. Neither Respondents nor the United States provide a particularized explanation for each redaction that would establish (1) that the redacted information is covered by the NDA and has not already been made public, and (2) that the information shows how the Stingray technology works or could be used to determine how the technology works. (See e.g. Hansen Decl. ¶ 16a., b., c.; Respondents' List of Exemptions; see American Civil Liberties Union of Northern Cal. V. Sup. Ct. (2011) 202 Cal.App.4th 55, 74, 83; see Long Beach Police Officers Assn. v. City of Long Beach (2014) 59 Cal.4th 59, 74-75 ["particularized showing" required to outweigh public interest in disclosure].)

Because neither the court nor Petitioner can determine which redactions, if any, contain this type of information, some type of in camera review (as discussed further below) is necessary.

However, Hansen does not explain in any detail why there would be a public interest against disclosure of non-technical or non-operational business information about the Stingray products. Petitioner's CPRA request sought agreements about Stingray products and related confidentiality agreements. It appears that the documents that were produced are mostly procurement related records, such as purchase orders, invoices, or related correspondence. Respondents appear to have redacted, inter alia, the names and addresses of vendors (Exh. 5 at 5, 16); general product descriptions (Exh. 5 at 5, 7-10, 49-50, 85-87); the scope of work and description of applicable documents (Exh. 5 at 85-94); and public website addresses (Exh. 5 at 74). The name of the primary vendor of Stingray (Harris) is already publicly known. (See Cox Decl. ¶ 5.) It is not clear why pricing information, general product descriptions, or public websites would be confidential or would disclose technical or operational information that would show how Stingray products work.

Hansen argues that "disclosure of even minor details about cell site simulators may cause harm to law enforcement efforts … because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance itself." (Hansen Decl. ¶ 19.) He further argues that "disclosure of what appears to be innocuous information about cell site simulators may provide adversaries … with information about the capabilities, limitations, and circumstances of the equipment's use." (Ibid.) The court is not persuaded by these generalized assertions that the balancing weighs for withholding non-technical or non-operational business information, such as the vendor name or pricing information.

Based on the showing that has been made by Respondents, the court concludes that information about non-technical or non-operational business information, such as the vendor name or pricing information may not be redacted from the documents produced.

While conceding the potential that the first two categories identified by Hansen are not disclosable, Petitioner suggests that the third category – "makes and models of cell site simulator systems" – requires no protection. She also argues that a subset of Hansen's categories one and two – "platforms and modes on which the equipment can be operated" – also would not "obviate" the Stingray technology. (Petitioner's Response filed 1/20/17 ("Resp.") 4-5.) Respondent may respond further to this argument at the hearing.

Government Code Section 6254(k) and Evidence Code Section 1040

Section 6254(k) exempts from disclosure "[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." Evidence Code section 1040(a) and (b)(2) state that "[a] public agency has a privilege to refuse to disclose official information", i.e., "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 prior to the time the claim of privilege is made," if "[d]isclosure 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...."

"The weighing process mandated by Evidence Code section 1040 requires review of the same elements that must be considered under section 6255." (CBS, Inc. v. Block (1986) 42 Cal.3d 646, 656.)

As argued by United States, a finding that the NDA makes the information confidential is only the starting point in the analysis under section 1040. Respondents and United States would still need to show that the balancing weighs against disclosure.

For the reasons stated above, the court concludes that the current record supports a finding under section 1040 that the balancing weighs in favor of non-disclosure as to the information described by Hansen as categories 1 through 3, with the exception of makes and models of cell site simulator systems and platforms and modes on which the equipment can be operated – which requires further argument. The court finds that balancing weighs in favor of disclosure of non-technical or non-operative information.

Government Code Section 6254(f)

Respondents argue that section 6254(f) exempts the redacted information from disclosure because it was acquired in confidence pursuant to an NDA with the FBI. (Suppl. Oppo. 3.) The United States argues that technical and operational information regarding cell site simulators is protected by section 6254(f) because it was obtained in confidence, it relates to the "security and safety" of the cell site simulator system, and its release could enable adversaries to impede the investigative use of the cell site simulator systems. (SOI 18-19.)

Government Code section 6254(f) generally exempts "records of complaints to, or 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, or any investigatory or security files compiled by any other state or local agency for correctional, law enforcement, or licensing purposes."

The term "intelligence information" in section 6254(f) "protect[s] information furnished in confidence, even if that information does not reveal the identity of a confidential source." (**ACLU** of Northern California, Inc. v. Deukmejian (1982) 32 Cal.3d 440, 443 [finding that exemption applied to index cards that contained the names of suspects and confidential sources].) The Deukmejian court held that "the 'intelligence information' exemption bars disclosure to the **ACLU** of personal identifiers, confidential sources, and confidential information relating to criminal activity" found on the index cards at issue. (Id. at 452.) In this factual context, Deukmejian is not authority for the broad proposition asserted by Respondents that any information that is "acquired in confidence" by a law enforcement agency pursuant to a NDA is exempt. Respondents must still show that the information acquired pursuant to an NDA is "intelligence information or security procedures." Moreover, Respondents fail to show that the NDA protects all of the redacted information.

Respondents and United States argue that section 6254(f) should be read to exempt disclosure of "investigative techniques and procedures," even

though the statute does not expressly exempt such information, because the parallel federal Freedom of Information Act ("FOIA") does exempt investigative techniques and procedures. (Suppl. Oppo. 3; State. Of Interest 18-19.) Respondents and United States read too much into the "parallel construction" language of Deukmejian. As the California Supreme Court later explained:

In **ACLU**, … [w]e certainly did not hold that the CPRA was to be interpreted as if it incorporated the FOIA criteria….[¶¶]

Because the CPRA did not define "intelligence information" we looked elsewhere for assistance-primarily to the FOIA. In doing so we simply applied the well-accepted principle of statutory interpretation that permits reference to a similar statute "to guide the construction" of the statute in question….[¶¶]

This exercise in "parallel construction" (**ACLU**, supra, 32 Cal.3d at p. 451) did not, however, include incorporating the statutory FOIA criteria into the CPRA.

(Williams v. Sup.Ct. (1993) 5 Cal.4th 337, 353.)

While the FOIA may be consulted as guidance in interpreting the CPRA, Deukmejian does not support reading specific provisions of the FOIA into the CPRA.

Respondents and United States do not cite any California case law that has interpreted "records of intelligence information or security procedures" in section 6254(f) to encompass investigative techniques and procedures. Nor do they provide a persuasive interpretation of the statute. However, section 6254(f) does exempt documents or portions of documents that deal with security and safety procedures of a law enforcement agency. (See Northern Cal. Police Practices Project v. Craig (1979) 90 Cal.App.3d 116, 121-122; see 79 Ops. Cal. Atty. Gen. 206 (Cal.A.G.), 1996 WL 531758 at *2].) The court concludes that "intelligence information or security procedures" could include, for instance, operational instructions on how to use the cell site simulator technology so as to maintain the security of the system and prevent discovery by criminals. Petitioner has not cited any case law that would challenge that interpretation.[8] 8

Respondents have apparently claimed that the section 6254(f) exemption applies to all of the redactions at issue. (Suppl. Oppo. Exh. A.) As stated, the court is not convinced that the fact LBPD obtained the Stingray technology pursuant to an NDA establishes, in itself, that the redacted information is "intelligence information or security procedures."

Neither the declaration of Lieutenant Cox nor Respondents' list of exemptions provides sufficient information to support a finding that the redacted information is exempt under section 6254(f). United States cites to paragraphs 17 to 22 of the Hansen declaration to support its arguments that the redacted information is exempt under section 6254(f). (SOI 19.) The Hansen declaration is too general to allow a determination as to whether any specific redacted information is exempt under section 6254(f).

Based on the evidence and arguments presented, the court concludes Respondent has not shown that the redacted information is exempt under section 6254(f). For instance, information about unit pricing, the vendor's name, and similar details regarding LBPD's purchase of the technology does not seem to involve security procedures or "intelligence information" as contemplated by section 6254(f).

Trade Secrets of Vendors

Respondents have provided only terse briefing to support their argument that the redactions were made to protect trade secrets. (Oppo. 4; Suppl. Oppo. 3-4.) The declaration of Eric Trew attaches a briefing in which Harris Corp. recommends that certain information should be withheld as trade secrets, but this briefing is not an evidentiary document.

The CPRA exempts "[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law…." (Gov. Code § 6254(k).) Under the Uniform Trade Secrets Act, "Trade secret" is "information… that: [¶] (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and [¶] (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." (Civ. Code § 3426.1(d); see also Gov. Code § 6254.7(d).) Section 6276.44 of the CPRA provides that documents which constitute trade secrets pursuant to Evidence Code section 1060 are exempted from disclosure.[9] 9

"An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others." (Futurecraft Corp. v. Clary Corp. (1962) 205 Cal.App.2d 279, 289.)

Respondents have not presented verified evidence to establish that any of the redacted information constitutes a trade secret.[10] 10 A review of the redacted records does not assist Respondents or Harris Corp. For instance, a vendor's name, address, or public website do not appear facially to be trade secrets. Respondents have not met their burden to establish that the redactions contain trade secret information or that such information is exempt from disclosure. As Respondents have not made any evidentiary showing in support, the court concludes that in camera review for trade secrets is not justified. (See American Civil Liberties Union of Northern Cal. V. Sup. Ct. (2011) 202 Cal.App.4th 55, 87 ["a trial court's prerogative to inspect documents in camera 'is not a substitute for the government's burden of proof, and should not be resorted to lightly'"].)

Other Redactions Proposed by Harris Corp.

In addition to the alleged trade secret information, Harris Corp. contends that the redactions include its banking information and tax ID number, and the names, email addresses, and phone numbers of Harris employees. (Suppl. Oppo. Exh. D.)

Petitioner has not identified any public interest in disclosure of the banking information or tax ID of Harris Corp. The court concludes that there is a public interest against disclosure of such information that clearly outweighs any public interest in disclosure. (§ 6255.) However, Respondents would need to identify specifically where this information is contained in the redactions.

Harris Corp. states, without supporting evidence, that Harris employees have been harassed when their names were released for prior public records act requests. It seems likely that the records at issue would contain the work email addresses and phone numbers of Harris employees, not their personal contact information. In meet and confer, Petitioner's counsel offered that the last names of Harris employees and all email addresses could be redacted. (Schlueter Decl. ¶ 10.) It is unclear if Respondents rejected that offer, and the reasons they did so. The court agrees that Petitioner's suggestion to redact the last name of Harris employees and all email addresses adequately balances privacy rights with the interest in public disclosure.

Withheld Documents

Petitioner briefly argues in her moving brief that Respondent "may well have" withheld documents responsive to the May 12, 2015 request. Petitioner points to a document allegedly received by another agency from the FBI involving wireless collection technology. (OB 7, Exh. 7.) It would be speculative to conclude from this exhibit that Respondent, a different agency, received the FBI letter and failed to produce it. Therefore, Petitioner fails to show that Respondent has withheld any responsive documents.

In Camera Review

In camera review of the unredacted records is permitted under the CPRA. The agency claiming the exemptions should make a sufficient showing to justify the in camera review. (See e.g. Gov. Code § 6259(a); see American Civil Liberties Union of Northern Cal. V. Sup. Ct. (2011) 202 Cal.App.4th 55, 74 ["Because the agency opposing disclosure bears the burden of proving that an exemption applies," it has the burden to submit evidence, including for in camera review]; see also Id. at 87 ["a trial court's prerogative to inspect documents in camera 'is not a substitute for the government's burden of proof, and should not be resorted to lightly'"].) Even though the court has found that certain categories of information are properly redacted under the Public Records Act, as Petitioners point out, there is insufficient information about the redacted material to ascertain whether it fits into one of those categories.

Based on the Hansen and Cox declarations, the NDA, and the supplemental briefing, the court concludes that an in camera review of the unredacted records is necessary to determine whether the redactions actually contain information the court has found exempt from disclosure. The court suggests that the parties select a sampling of unredacted documents for in camera review. The parties should meet and confer regarding methodology for the proposed sampling, and should also address at the hearing the appropriate persons, if any, to participate in the in camera review.

Conclusion

Respondents may redact from the records the banking information and tax ID number of Harris Corporation. Respondents may redact the last names and email addresses of Harris employees. Respondents may redact confidential technical and operational information that shows how the Stingray technology works. Respondents may redact the identities of undercover detectives or vehicles that, if disclosed, could help criminals to counteract how LBPD uses the Stingray technology in the field. (See Cox Decl. ¶ 6.)

Respondents may not redact non-technical or non-operational information regarding the CSS products, including pricing information, general product descriptions, or public websites. The parties should further address at the hearing whether "makes and models of cell site simulator systems" or "platforms and modes on which the equipment can be operated" is non-disclosable under 6255 or 6254(k).

The court concludes that some type of in camera review of the unredacted records is necessary to determine whether the information redacted actually covers the type of information the court has concluded is non-disclosable. The court will discuss the structure of the in camera review with the parties at the hearing.

In all other respects, including with regard to trade secrets, Respondents have not met their burden to justify the redactions and also have not shown a need for in camera review.

FOOTNOTES:

The petition also sought to compel disclosure of documents in response to a CPRA request dated March 17, 2015. Petitioner concedes that Respondent has now complied with the March 17, 2015 request. (See Opening Brief (OB) 1.)

In her opening brief, Petitioner refers to Stingray as an IMSI catcher. (OB 5.) In his declaration, Hansen groups Stingray with cell site simulator technologies, which he differentiates from IMSI catchers. (See e.g. Hansen Decl. ¶¶ 4-6, fn. 2.)

Section 517 states in full: "The Solicitor General, or any officer of the Department of Justice, may be sent by the Attorney General to any State or district in the United States to attend to the interests of the United States in a suit pending in a court of the United States, or in a court of a State, or to

attend to any other interest of the United States."

espondents and United States have not argued in their papers that the redacted information is non-responsive to Petitioner's May 12, 2015 CPRA request.

The United States gives the most attention to, and discusses first in its brief, the official information privilege under sections 6254(k) and 1040, and the public-interest balancing under sections 1040 and 6255.

As discussed below, the balancing under section 6255 is similar to that under section 1040.

Petitioner appears to concede that technical information "about how the technology works" could be exempt under section 6255 because of the risk it could allow criminals to circumvent surveillance. (OB 13.)

Cook v. Craig (1976) 55 Cal.App.3d 773, 783-784, cited by Petitioner in the opening brief, held that the CHP was required to produce "its procedural regulations governing the investigation of citizen complaints about the conduct of CHP personnel." It did not hold or suggest that section 6254(f) does not apply to technical information about a law enforcement tool, such as a cell site simulator.

Evidence Code section 1060 provides that: "If he or his agent or employee claims the privilege, the owner of a trade secret has a privilege to refuse to disclose the secret, and to prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice."

As stated, the Harris Corp. briefing is not verified.

Other rulings by Hon. Mary H. Strobel

Francisca Eugenia Nunez Vs Director Of The Department Of Motor Vehicles

Jose Vazquez , Et Al. Vs Alma Hernandez , Et Al.

Michele Sims Vs Commission On Teacher Credentialing, Et Al.

Felipa Baccari Vs City Of Long Beach, Et Al.

American Federation Of State, County And Municipal Employees, Local 1902, Afl-Cio, Et Al. Vs Foothill Municipal Water District Board Of Directors

Monica Blut Vs Oceans International Packing And Shipping, Inc., A California Corporation

Fe&M Inc Vs City Of Glendale

John Doe Vs Timothy P White Et Al

A G Johnson Vs City Of Lynwood Et Al

Earth Tek Engineering Corp Vs Deacon Corp Et Al