No. 52072-9-II

COURT OF APPEALS FOR THE STATE OF WASHINGTON
DIVISION TWO

CITY OF TACOMA

Appellant,

v.

ARTHUR BANKS, ET. AL.,

Respondents.

BRIEF OF RESPONDENTS

ACLU OF WASHINGTON FOUNDATION

John Midgley, WSBA #6511
Lisa Nowlin, WSBA #51512
901 Fifth Avenue, Suite 630
Seattle, WA 98164
206 624-2184
jmidgley@aclu-w.org
lnowlin@aclu-wa.org

Attorneys for Respondents

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

I. Introduction

This case involves a dispute over public records relating to cell site simulator technology employed by the Tacoma Police Department ("TPD"). Cell site simulators are electronic surveillance tools used to track cell phones and therefore to locate individuals law enforcement officers are searching for. Cell site simulators continue to be the subject of intense public interest and controversy.

The Public Records Act exists for the very purpose of shedding light on the activities of government officials and law enforcement, to prevent government from operating in the shadows, and to enable the public to hold public officials accountable. As RCW 42.56.030 states, "[t]he people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created."

This case is not about when or how TPD can use cell site simulators; this case is about transparency and fulfilling the mandates of the Public Records Act ("PRA"). Plaintiffs, as Respondents-Cross Appellants ("Plaintiffs"), do not argue that all information about cell site simulators must be disclosed. Plaintiffs do argue that the PRA requires

certain processes be followed, and that those processes were not followed in this case.

Plaintiffs show below that TPD's multiple failures to provide information about TPD's use of cell site simulator technology violate the PRA. The Washington State Supreme Court has held that the PRA "is a strongly-worded mandate for broad disclosure of public records." *Hearst Corp. v. Hoppe*, 90 Wn.2d 123, 127, 580 P.2d 246 (1978). The legislative purpose of the act is "nothing less than the preservation of the most central tenets of representative government, namely, the sovereignty of the people and the accountability to the people of public officials and institutions." *Progressive Animal Welfare Soc. v. Univ. of Wash.*, 125 Wn.2d 243, 251, 884 P.2d 592 (1994) ("*PAWS*"). Under these principles, the PRA entitles Plaintiffs to judgment, additional public records, monetary penalties, and attorneys' fees and costs. The trial court granted Plaintiffs some relief and those holdings should be affirmed. In addition, Plaintiffs request that this Court grant relief requiring a renewed search for responsive public records and the release of information about use of cell site simulators that is currently redacted or withheld.

II. Issues Presented on Cross Appeal

Because the issues presented on cross appeal are subject to de novo review, we have not included assignments of error.

1. Where a public agency's search for public records was inadequate in that it did not look in obvious places for responsive records, where Plaintiffs identified additional locations of records that should have been searched, and where the agency failed to produce, report, and/or find many responsive records, should an additional search be ordered?
2. Does the Public Records Act exemption for "specific intelligence information" exempt information about makes and models of equipment and general information about how a technology operates? –

III. Issues Presented on the City of Tacoma's Appeal

1. Did TPD violate the Public Records Act by failing to produce multiple available records that were responsive to Plaintiffs' PRA request?
2. Did the trial court abuse its discretion in ordering penalties for the records identified that TPD did not produce?
3. Did the trial court abuse its discretion in ordering attorneys' fees and costs for the PRA violations?

IV. Statement of the Case

A. Cell Site Simulators and Their Use by the Tacoma Police Department

Cell site simulators are surveillance tools employed by law enforcement agencies to locate cell phones and their users. Sometimes known as "StingRays," this technology is an indiscriminate and intrusive means of collecting information. Plaintiffs' experts explained how the technology works:

> Cellular devices are designed to frequently reconnect to cell towers to maintain the best signal strength and performance; they continuously scan for new cell towers and routinely connect to different towers that are broadcasting stronger signals or other desirable properties. …
>
> Cell-site simulators are radio devices that mimic the signals of cell towers. They usually consist of a radio transceiver to transmit and receive cellular signals and a computer that stores data and runs software to operate the radio transceiver. Cell-site simulators cause cellular devices to automatically connect and transmit data to them as they would with a normal cell tower. This data includes metadata like electronic serial numbers (ESNs) and subscriber identifiers.[1] … Once the [identifying information] of a subscriber is known, it can be entered into the equipment to determine if the subscriber's device is within range of the transceiver. If the subscriber's cellular device is within range and connects to the cell-site simulator, then, using radio direction finding equipment, the operator can precisely locate the position of that device.
>
> Cell-site simulators can also be used to identify unknown cellular devices — for example, a prepaid cell phone with an anonymous

[1] Subscribers are customers to telecommunication companies, such as AT&T or Verizon, and identifiers are numbers or other information that can be used to identify subscribers or devices. CP 886.

> subscriber. By collecting cellular metadata of all cellular devices within range at multiple locations, an operator can discover whether the same cellular device was used in different places by looking for duplicates in different datasets. […] This functionality requires that cellular metadata (including metadata from bystander devices) be stored for a period of time because the metadata collected at each location must be compared before the operator can discard the bystander information.

CP 886–887. *See also*, Spencer McCandless, Note, *Stingray Confidential*, 85 Geo. Wash. L. Rev. 993 (2017); Coleman L. Torrans, Comment, *How Did They Know That? Cell Site Simulators And The Secret Invasion of Privacy*, 92 Tul. L. Rev. 519 (2017).

Cell site simulator devices were likely developed for military use but have more recently been deployed by domestic law enforcement. *Stingray Confidential* at 999. Cell site simulator technology is fundamentally different from the older "pen, trap, and trace" technology: instead of capturing the numbers that a phone dials, or numbers that are dialed to a phone number and tracing the signals, a cell site simulator precisely locates a phone and therefore a person. *Id*. at 1012–13.

In 2014, it was discovered that TPD had been using one or more cell site simulator devices since 2009 (CP 733 (Tacoma Citizen Review Panel Minutes)), and had not disclosed its use to anyone, including judges who were approving warrants for telephone location interceptions. CP 1510 at 76:8–79:15. The secrecy that surrounded the cell site simulator

in Tacoma was consistent with nationwide, intentional efforts by the FBI to keep all information about cell site simulators secret, through non-disclosure agreements ("NDAs") that entities were forced to enter into prior to obtaining the technology. *How Did They Know That?* at 537–41; *Stingray Confidential* at 1001–08. TPD was subject to an FBI-initiated NDA, the existence of which the FBI tried to suppress, but which was eventually released to PRA requesters along with other records related to the cell site simulator. CP 111–16 (Non-disclosure Agreement).

The revelation of TPD's use of cell site simulator technology was followed by a number of requests for records under the Public Records Act. The PRA request made by the Plaintiffs in this case—three pastors and one community activist in Tacoma—is the subject of this case. CP 649–57 (PRA request and related correspondence); 1–27 (Complaint).

In recognition of the inherent intrusiveness of cell site simulator technology, many state and federal officials have created safeguards to limit its use and effects. In 2015, the Washington Legislature enacted the current version of RCW 9.73.260, which requires warrants for the use of cell site simulator devices that mandate more specific information than for other telephone location interception warrants, and includes special reporting and data deletion requirements for cell site simulator devices. The Legislature also added RCW 9.73.270, which contains specific limits

on the use of cell site simulator technology by the "state and its political subdivisions."[2] Similarly, the United States Department of Justice has promulgated a lengthy set of instructions and controls on the use of cell site simulator devices, including explicit instructions to delete data captured by a cell site simulator. CP 995–1001.

Through records obtained and discovery taken in this case, Plaintiffs have so far learned the following about TPD's use of cell site simulator technology:

- Instead of seeking warrants specifically to use the cell site simulator when needed (as required by statute), TPD obtains warrants that authorize the use of a cell site simulator in every situation in which TPD is seeking the location of a phone (all "pen, trap, and trace" warrants). CP 787; CP 1498 at 31:2–21; Appellant's Opening Brief at 4 ("Appellant's Br.") (citing CP 1497; 1594).

[2] The current statutes are RCW 9.73.260 and RCW 9.73.270, attached as Appendix A. The bill adding these references to CSS and the special requirements for CSS use, Laws of 2015, ch. 222, §1-4, attached as Appendix B, was entitled "Cell Site Simulator Devices—Collection of Data—Warrant." In addition to the data-deletion requirement, the new provisions require significantly more information to support a warrant for use of a CSS than for other forms of telephone location or interception activities.

- There remains no formal record of cell site simulator approval or use, as the process is intentionally done orally to prevent creation of a written record. CP 808; CP 1609; CP 1615–16.
- TPD has no reliable record or log for when and under what circumstances cell site simulator equipment has been used. CP 808; 853–856.
- There are no written TPD protocols or policies governing use of cell site simulator technology. CP 816.
- TPD denies that its cell site simulator equipment (including the laptop computer required to operate the cell site simulator) obtains or stores any data that needs to be deleted, despite significant evidence to the contrary. CP 861 at 45:16–18.

Plaintiffs' cross appeal seeks additional public records that they believe should have been searched for and provided in response to Plaintiffs' PRA request; the failure to do so deprives the public of important information about TPD's use of cell site simulator technology.

B. Plaintiffs' Request for Public Records, TPD's Response, and Filing of Suit.

Plaintiffs requested public records related to TPD's use of cell site simulator technology by letter dated September 2, 2015 ("PRA Request"). CP 649–57 (PRA request and related correspondence). TPD responded

with two batches of records provided on October 28, 2015, and December 18, 2015, and also provided privilege logs for records identified but withheld or redacted. CP 743–49. After TPD's disclosures were completed, Plaintiffs filed this case claiming unlawful withholding of a number of records and categories of records, and unlawful redactions of records. CP 1–27.

C. Procedure Below

After pretrial discovery, Plaintiffs moved for partial summary judgment and the City of Tacoma ("City") moved for summary judgment. CP 461–81; 632–39. Both sides submitted documents, declarations, and deposition excerpts. The United States submitted a Supplemental Statement of Interest and supporting declarations regarding the withholding of information and redactions regarding cell site simulator equipment. CP 1126–36. Plaintiffs requested *in camera* review of records that TPD identified and withheld (CP 764–65) and an order requiring TPD to make an additional search for documents CP 770–71. RP at 5 (April 13, 2018). There was no live testimony.

The trial court held that TPD conducted an inadequate search and violated the PRA with respect to each of the eleven responsive documents Plaintiffs had obtained since the PRA search closed. CP 1650–58. Neither in its opinion on summary judgment nor in its opinion on Plaintiffs'

Motion for Reconsideration did the trial court rule on Plaintiffs' request that TPD be ordered to search for documents in locations it had previously failed to search. CP 1650-1658; RP at 37–38 (4/13/18); CP __ (Order on Plaintiffs' Motion for Reconsideration/Clarification, designated February 13, 2019). The court did not review any redacted or withheld material *in camera,* but held that the identified-but-withheld material and redactions that Plaintiffs sought were exempt from PRA disclosure under RCW 42.56.240(1). CP 1657. The trial court imposed $182,340.00 in PRA penalties, $109.885.00 in attorneys' fees, and $5,645.04 in costs on the City. CP 1658. Plaintiffs filed a Motion for Reconsideration on the issue of a new search, which the court denied. CP 1663-68; CP __ (Order on Plaintiffs' Motion for Reconsideration/Clarification, designated February 13, 2019). The City appealed and Plaintiffs cross appealed.

V. Standard of Review

Substantive PRA questions are reviewed *de novo*. *Fisher Broad. v. City of Seattle*, 180 Wn.2d 515, 522, 326 P.3d 688 (2014). Public agencies bear the burden of showing that their search was adequate, *Neighborhood All. of Spokane Cty v. Spokane Cty.*, 172 Wn.2d 702, 721, 261 P.3d 119 (2011), and that PRA exemptions apply to any responsive record withheld from a PRA requester, RCW 42.56.550(1). Penalties imposed by a trial court for violations of the Public Records Act are reviewed for abuse of

discretion. *Yousoufian v. Office of Ron Sims,* 152 Wn.2d 421, 430–31, 98 P.3d 463 (2004). Trial court determinations of attorneys' fees and costs are also reviewed for abuse of discretion. *Sanders v. State*, 169 Wn.2d 827, 866–67, 240 P.3d 120 (2010).

VI. Argument on Plaintiffs' Cross Appeal

A. Tacoma Police Department's Public Records Search Was Inadequate, and the Court Should Order the Department to Search Further.

1. The Burden of Proof of an Adequate Search Lies with the City and the City Has Not Met Its Burden

Plaintiffs submitted their PRA Request to TPD on September 2, 2015. CP 649–50. And though the City undertook a search for documents, it is clear from the numerous custodians and locations that the City failed to search that the search it conducted was not adequate.

On a motion for summary judgment in a Public Records Act case, the agency "bears the burden, beyond material doubt, of showing its search was adequate." *Neighborhood All.*, 172 Wn.2d at 721. The adequacy of a search under the PRA is judged by a standard of reasonableness— "the search must be reasonably calculated to uncover all relevant documents." *Id.* at 720 (citing *Weisberg v. U.S. Dep't of Justice*, 705 F.2d 1344, 1351 (D.C. Cir. 1983)). This test should be applied consistent with the "congressional intent tilting the scale in favor of disclosure." *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 117

F. Supp. 3d 46, 57 (D. D.C. 2015) (internal quotation marks and citation omitted).[3] "What will be considered reasonable will depend on the facts of each case." *Neighborhood All.,* 172 Wn.2d at 720. An agency must search every place where responsive records are "reasonably likely to be found." *Id*. (emphasis omitted). "[A]n inadequate search is comparable to a denial because the result is the same, and should be treated similarly in penalty determinations, at least insofar as the requester may be entitled to costs and reasonable attorneys' fees under RCW 42.56.550(4)." *Id.* at 721.

To meet its burden, the agency should provide reasonably "detailed, nonconclusory" descriptions of the search, which should include "search terms and the type of search performed, and . . . establish that all places likely to contain responsive materials were searched." *Id*.; *see also Steinberg v. United States Dep't of Justice*, 23 F.3d 548, 552 (D.C. Cir. 1994) (finding search adequate where affidavit described "with particularity the files that were searched, the manner in which they were searched, and the results of the search.").

[3] Although the *Elec. Privacy Info. Ctr.* case was brought under the federal Freedom of Information Act (FOIA), Washington courts have consistently held that the standards governing the adequacy of a search under the PRA are the same as for FOIA. *Neighborhood All.*, 172 Wn.2d at 719; *see also Hearst Corp.*, 90 Wn.2d at 128 ("The state act closely parallels the federal Freedom of Information Act ... and thus judicial interpretations of that act are particularly helpful in construing our own." (internal citation omitted)).

The trial court correctly found that TPD's search was inadequate. The court focused its discussion on the eleven documents that were known to have been withheld, though much more evidence of the inadequacy of the search was also before the court. All of this evidence points to a clearly inadequate search. CP 1650–58; *see infra*, Section VII.A (responding to the City's appeal addressing those findings).

At the outset of this case, Defendant's description of the search conducted was severely lacking in detail. The City's description of steps taken by Michael Smith, TPD's Legal Advisor, in responding to the PRA Request mainly constituted who he spoke to, not the actual steps he took to conduct the search, let alone search terms. CP 462–64. In its Reply on its Motion for Summary Judgment, the City submitted additional affidavits from Mr. Smith and Detective Terry Krause to attempt to remedy the deficient description of its search. CP 1373–76; 1391–94.

But the City's eventual provision of more detail about the search it conducted does not cure the inadequacy of the search itself. Even as described in more detail, the search was inadequate in several ways: The City failed to search email accounts for numerous officers, it failed to search for warrants, it failed to search at South Sound 911 where many

TPD records are kept, and most tellingly, it failed to search the cell site simulator itself.[4]

2. *The City Failed to Search the Cell Site Simulator and Associated Laptop for Data Collected During the Use of the Cell Site Simulator*

The first request in Plaintiffs' PRA Request at issue is for "[a]ll records regarding TPD's acquisition, *use*, or lease of Cell Site Simulators . . .." CP 16 (emphasis added). Despite Plaintiffs' request for all cell site simulator usage records, the City did not search for records on the device itself. That the data may not have been in the traditional form of a document is no defense—the PRA defines "public record" broadly to include "'existing data compilations from which information may be obtained' 'regardless of physical form or characteristics.'" *Fisher Broad.*, 180 Wn.2d at 524 (quoting RCW 42.56.010(4), (3)).

The records contained in the cell site simulator laptop are clearly responsive to Plaintiffs' request; they are the very records of the use of the

[4] In the context of data collection and storage, Plaintiffs use the term "cell site simulator" to include the associated laptop computer that is used to operate the cell site simulator. Because the laptop is necessary to operate the cell site simulator, the two are an integrated system. *See also* CP 1085 at 115:12-18 (referring to laptop as "part of the [cell site simulator] equipment"). Discussions of information and documents available on the cell site simulator include information on the associated computer.

cell site simulator.[5] Because it took the position no such records exist when they very likely do, TPD failed to look for the most pertinent of these records, failed to disclose these records, and failed to provide these records.

TPD's position that the cell site simulator collects no data during use is wholly unfounded. Peter Ney and Ian Smith, experts in computer security whose research focuses on cell site simulators and cellular network security, prepared an expert report on cell site simulators based on publicly available information, including Harris Corporation manuals for cell site simulators, and their technological expertise. *See* CP 885–93 (Peter Ney and Ian Smith, Expert Report).[6]

---

[5] An argument that many of these documents fall within a PRA exemption is unavailing. Even if the records are exempt, the City must search the records, identify them, and explain its reasons for withholding them. *See* RCW 42.56.210(3).

[6] While Mr. Ney and Mr. Smith have not physically examined the cell site simulators owned by the City of Tacoma or confirmed the precise version of the software being used, they have thoroughly explained the foundations of their opinions. Documents provided by TPD indicate that it received the StingRay model cell site simulator in 2008 and later received the Hailstorm model. CP 888. The experts reviewed Harris Corporation manuals written for the StingRay and Hailstorm models, and the software described in the manuals also utilizes the same cellular protocols that TPD officers were trained to use. *Id*. To the extent the Court has any doubts about the reliability of the experts' opinions, Mr. Ney and Mr. Smith are willing and able to examine the equipment owned by the City of Tacoma and to modify their report if necessary.

The Expert Report explains how data is entered into a cell site simulator during operation. For example, to locate a specific cellular device, the operator can use the cell site simulator in two ways. As previously described on pages 4-5, the first method requires the operator to enter the target device's unique identifier (IMSI number) into the laptop. Once the target device connects with the "cell tower" that is the cell site simulator, the operator can precisely locate the position of the device. CP 886–87. The second method is used to identify an unknown device, where the cell site simulator collects and saves the metadata of all cellular devices within range of the cell site simulator in multiple locations, and then compares the collected data for each location to determine which device(s) were in each location. CP 887.

As detailed in the expert report, the cell site simulator, by nature of how it operates, collects data from all cellular devices within its range. In both methods of operation, data is saved every time the cell site simulator is used, whether the data is collected or manually entered. The software on the cell site simulator is designed to store data to files that are easily accessible on the computer and easily exported in a number of formats, including Microsoft Excel. CP 889–92. Additional stored data includes properties of nearby cell towers and operator GPS coordinates. CP 889. Indeed, this information is saved in a database and the software includes

features for labeling, organizing, and viewing the data. CP 889–90. The City has not made any attempt to rebut the experts' conclusions.

In light of this information, Detective Krause's assertion that "there's no data collected. There's nothing retained. There's nothing to purge[,]" is simply not true. CP 861 at 45:17–18. This is further evidenced by Harris Corporation manuals, (CP 990–93 (Sealed[7] Expert Report Exs. 6 & 7) (discussing saving and exporting of data)), Department of Justice policy guidance on cell site simulators that recommends deletion of data (CP 1000), and Washington law (RCW 9.73.260(6)(c) (requiring periodic deletion of information and metadata collected by cell site simulators)). It is hard to believe there is no data when all of these relevant sources say there is data to be deleted.

It was only in April 2018—over two and a half years after Plaintiffs submitted their PRA request, over two years after TPD sent Plaintiffs its final PRA production, and two years after this lawsuit was

[7] Plaintiffs submitted Exhibits 6 and 7 to the Superior Court on March 19, 2018, along with a Motion to Seal. CP 1097-1102. Defendant did not file an opposition to Plaintiffs' Motion to Seal, and to Plaintiffs' knowledge, the Motion to Seal remains pending. While the manuals comprising Exhibits 6 and 7 are publicly available, Plaintiffs, out of an abundance of caution, filed them under seal due to distribution warnings on the manuals. *See* Sam Biddle, *Long-Secret Stingray Manuals Detail How Police Can Spy on Phones*, THE INTERCEPT (Sept. 12, 2016, 11:33 AM), https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

filed—that Defendant finally performed even a cursory search of the cell site simulator. *See* CP 1393–94 (Decl. of Terry Krause in Supp. of Def.'s Reply on Def.'s Mot. for Summ. J.) (stating for first time that he had searched the cell site simulator). Detective Krause provided no details of his "search"—such as when it occurred or how it was conducted. The only detail he provides is that he searched "by file extension." *Id*. But any search of the cell site simulator and associated laptop must be "reasonably calculated to uncover all relevant documents." *Neighborhood All.*, 172 Wn.2d at 720. A search for certain file extensions (presumably for files ending in, for example, ".doc" or ".pdf") is not reasonably calculated to uncover relevant documents if the relevant information is not stored in Word documents or PDFs, but rather in a database. CP 889–93 (expert report discussing database on cell site simulator and how data can be exported). The PRA defines "public records" broadly and includes information in databases. *Fisher Broad.*, 180 Wn. 2d at 524.

Defendant's failure to search the cell site simulator during the actual PRA search in 2015—the eleventh-hour search for documents by "file extension" notwithstanding—is emblematic of the inadequacy of Defendant's search for records. The cell site simulator is central to Plaintiffs' PRA request and must be searched, and must be searched in a way that is reasonably calculated to uncover relevant information.

Plaintiffs are not asking Defendant to search "every possible place a record may conceivably be stored[.]" Appellant's Br. at 10 (quoting *Neighborhood All.*, 172 Wn.2d at 719–20). Plaintiffs are simply asking Defendant to search those places where records are "reasonably likely to be found[,]" including searching the cell site simulator itself for the kind of data it almost certainly captures. *Id*.

3. *The City Failed to Search for Warrants and to Adequately Search All Reasonable Custodians*

The failure to adequately search emails and search for warrants is starkly highlighted by Detective Christopher Shipp's CR 30(b)(6) testimony. He testified that warrants authorizing the use of cell site simulators were emailed to telecommunications companies from the individual email accounts of officers in the Tech Unit; that officers would disclose the use of cell site simulators to prosecutors "verbally or by email;" and that officers might email or call a telecommunications company for additional information needed for operating the cell site simulator. CP 790–96; 837–39; 808; 813–15. Detective Krause also indicated that when the cell site simulator is utilized on behalf of other jurisdictions, the authorizing warrant might be scanned, faxed, or received in hard copy. CP 852–53. Yet not a single one of those records was

provided. This withholding stems from the Tech Unit's failure to search for warrants[8] and failure to search all relevant custodians.

The City admits that the only officers asked to look for documents were the two or three detectives in the Tech Unit and the Chief's office. CP 1115; 1279–80. While the detectives in the Tech Unit are the only ones who *operate* the cell site simulator, the cell site simulator is utilized for the benefit of non-Tech Unit officers' cases. Because it is highly likely that officers utilizing the cell site simulator would have emails discussing such use (CP 808–10) they should have been identified as custodians and should have conducted searches for responsive documents.

4. *The City Failed to Search South Sound 911*

The City's search is also inadequate due to the complete failure to search any documents held for TPD by South Sound 911. Even apart from the request for information about the warrants, Plaintiffs' PRA request specifically asked for all records regarding "use" of the cell site simulator. CP 16 at Request 1. South Sound 911 maintains a reporting system called "Enforcer" that all TPD officers have real-time access to. CP 828–32. Patrol officers enter initial reports into the Enforcer system, and then

[8] Plaintiffs assert a need for all warrants relating to capturing data from phones—pen, trap, and trace warrants—because, as the City admits, all warrants for phone data authorize the use of the cell site simulator. Appellant's Br. at 4.

supplemental reports can be added. *Id*. These reports can be created and accessed from TPD computers, including laptops in patrol cars. *Id*. "[A] vast majority of all documents that are the primary source material for an investigation are going to be at South Sound 911." CP 873.

The City claims that a search of South Sound 911 was not reasonably likely to turn up responsive documents, but this is based simply on conclusory statements by Michael Smith rather than any detailed explanation of why a search of the main platform used by TPD officers would not have any references to cell site simulators.[9] CP 474; 1281–83. Indeed, Christopher Shipp testified in the 30(b)(6) deposition that the investigative files might indicate that a pen, trap and trace warrant was pursued, and that all pen, trap and trace warrants authorize cell site simulator use. CP 786–87, 801–05. At a minimum, it is common sense that, for records pertaining to TPD's use of cell site simulators—an investigative tool—TPD must search their main investigative records platform.

[9] Detective Christopher Shipp testified that he intentionally does not mention cell site simulators in any case reports because Detectives Jeffrey Shipp and Terry Krause had told him that public disclosure of the use of cell site simulators was undesirable. CP 1299–1300. Though it may have been one Detective's unofficial practice to intentionally omit referring to using a cell site simulator, that is not sufficient grounds for TPD to choose not to even search for documents in its investigative platform.

In sum, TPD did not conduct an adequate search for records in response to Plaintiffs' PRA Request. The City failed to search custodians that, based on their officers' testimony, were likely to have responsive emails, and failed to search their primary investigative platform. And more importantly, the City failed to search for data from the cell site simulator itself during the PRA search and did nothing more than a tardy, superficial search of the laptop during summary judgment, as detailed above. These omissions make it clear that the City's search was not "reasonably calculated to uncover all relevant documents," and it has not met its burden of showing "beyond material doubt" that its search was adequate. *Neighborhood All.*, 172 Wn.2d at 720–21**.**

5. *This Court should order a new search.*

In *Neighborhood Alliance,* the Washington Supreme Court discussed potential remedies for an inadequate search as it discussed whether an inadequate search constitutes a separate cause of action under the PRA:

> [W]e now hold that the failure to perform an adequate search is at least an aggravating factor, to be considered in setting the daily-penalty amount.
>
> An adequate search is a prerequisite to an adequate response, so an inadequate search is a violation of the PRA because it precludes an adequate response. But we again put off for another day the question whether the PRA supports a freestanding daily penalty when an agency conducts an inadequate search but no responsive documents

> are subsequently produced. A prevailing party in such an instance is at least entitled to costs and reasonable attorney fees.

Neighborhood All., 172 Wn.2d at 724–25 (citations omitted). Because in *Neighborhood Alliance* the crucial document that was not searched had already been destroyed, the court did not consider another available remedy that could make whole a PRA requester who has not been provided an adequate PRA search: an order to search further.

Contrary to the City's assertion that the "Court isn't allowed to grant any relief other than a violation of the PRA for existent documents and a dollar amount" (RP 11 (4/13/18)), the Supreme Court of Washington has found that in a PRA context, a trial court has "broad discretionary power to shape and fashion injunctive relief to fit the particular facts, circumstances, and equities of the case before it." *Resident Action Council v. Seattle Hous. Auth.*, 177 Wn.2d 417, 445, 327 P.3d 600 (2013) ("*RAC*") (internal citation omitted). In *RAC*, the trial court ordered a wide range of relief, including injunctive relief requiring that properly redacted records be produced electronically (rather than in paper format) and that the defendant publish procedures related to public records requests. *Id*. at 446–47.

If the court in *RAC* had the authority to order injunctive relief regarding the *format* of the documents and for new agency procedures,

surely this Court has the authority to order that the City remedy its inadequate search. It is of no consequence that the City has not identified the specific documents Plaintiffs are requesting—the City has an obligation under the PRA to search for the documents and the Court has the power to enforce the PRA.

"A party seeking an injunction must show (1) a clear legal or equitable right, (2) a well-grounded fear of immediate invasion of that right, and (3) actual and substantial injury as a result." *Id.* at 445–46 (internal citation omitted). As in *RAC*, injunctive relief is appropriate here: Plaintiffs have "a clear right to appropriate production of requested documents," TPD "has refused to produce those documents," and Plaintiffs "remain[] without the public records [they] ha[ve] requested." *Id.* at 446. Plaintiffs are not asking the Court to do anything new under the PRA. "On numerous occasions [the Supreme Court of Washington has] allowed detailed 'disclosure orders' in PRA cases to remedy an agency's failure to comply with the PRA." *Id.* (citing cases). Plaintiffs, relying on the testimony of Defendant's own agents, have shown that several categories of documents almost certainly exist. This Court should order TPD to search for them.

B. The Challenged Redactions and Withheld Records Were Not Exempt As "Specific Intelligence Information" Under RCW 42.56.240(1) And Should Be Provided.

In addition to the City's inadequate search for documents, Plaintiffs also appeal TPD's improper redaction of model and pricing information (CP 1008–21; 1031–42; 1051–60) and its complete refusal to produce the cell site simulator manuals, even in a redacted form. *See* CP 745–746 (TPD privilege logs). The City claimed these materials exempt from PRA disclosure under RCW 42.56.240(1). Plaintiffs objected and requested that the trial court view these materials *in camera* as permitted by RCW 42.56.550(3). CP 764. The court did not view the materials to our knowledge, but nevertheless held that they were exempt.

For a record to be exempt from disclosure under RCW 42.56.240(1), it must meet four requirements: (1) it must be "[s]pecific intelligence information" or "specific investigative records" (2) "compiled by" (3) "investigative, law enforcement, and penology agencies," (4) "the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy." *See Haines-Marchel v. State, Dep't of Corr.*, 183 Wn. App. 655, 665–66, 334 P.3d 99 (2014) (recognizing four elements to RCW 42.56.240(1)). "The agency bears the burden of proving that refusing to disclose 'is in accordance with a statute

that exempts or prohibits disclosure in whole or in part of specific information or records.'" *PAWS*, 125 Wn.2d at 251–52 (citing RCW 42.17.340(1) (Recodified as RCW 42.56.550(1))). The language of the statute limits the exemption to "specific" information and records. This exemption is further limited by the Washington Supreme Court's mandate that it be construed narrowly. *Wade's Eastside Gun Shop, Inc. v. Dep't of Labor and Indus.*, 185 Wn.2d 270, 280–281, 372 P.3d 97 (2016).

The records Plaintiffs seek do not fall within the narrowly construed exemption. Plaintiffs do not dispute that TPD is a law enforcement agency or that it compiled the records. But the City cannot demonstrate that (1) portions of the withheld and redacted information qualify as "specific intelligence information"[10] or that (2) the information is essential to effective law enforcement. Therefore, the City cannot meet its burden of showing that the documents are exempt.

1. *The withheld information is not "specific intelligence information."*

The RCW 42.56.240(1) exemption only applies to *specific intelligence* information—the information must be *intelligence*

[10] Neither party has ever contended that any of the withheld materials are "specific investigative records." *See also Haines-Marchel*, 183 Wn. App. at 666 ("Records are specific investigative records if compiled as a result of a specific investigation focusing with special intensity upon a particular party." (internal citations and quotations omitted)).

information, and beyond that, it must be *specific* intelligence information. Examples of what may comprise specific intelligence information include "'the gathering or distribution of information, especially secret information,' or 'information about an enemy' or 'the evaluated conclusions drawn from such information.'" *Haines-Marchel*, 183 Wn. App. at 667 (citing *King Cty. v. Sheehan*, 114 Wn. App. 325, 337, 57 P.3d 307 (2002)). The withheld and redacted information Plaintiffs seek do not fall within this definition, or any other plain reading of "specific intelligence information."

Model and pricing information on an invoice is not "intelligence information," let alone "specific intelligence information"—it is merely information about what item has been purchased and the amount that Accounts Payable must write a check for. Model and pricing information do not fall within any of the examples provided by our courts: model and pricing information are not related to the gathering or distribution of secret details or information about an enemy, and they certainly do not contain evaluated conclusions. Neither do the manuals in their entirety qualify as specific intelligence information.

The definition of specific intelligence information by *Sheehan* and other courts has consistently been akin to something gleaned from an investigation into criminal activity. *Sheehan*, 114 Wn. App. at 337. In

Sheehan, King County argued that a list of officers' names was intelligence information because it contained the names of undercover officers, and officers who might someday go undercover. *Id*. at 338. The court refused to so hold because "to construe the 'specific intelligence information' exemption so broadly as to include the names of officers who might someday go undercover would fly in the face of the thrice-repeated legislative mandate that exemptions under the public records act are to be narrowly construed." *Id.* (citations omitted).

In the court below, the City and the United States mistakenly relied on comparisons to a series of cases that only evaluate the question of whether records are "essential to effective law enforcement." *See Fischer v. Wash. Dep't of Corr.*, 160 Wn. App. 722, 725–26, 254 P.3d 824 (2011) (considering whether the nondisclosure of surveillance videos was essential to effective law enforcement); *Gronquist v. State*, 177 Wn. App. 389, 399, 313 P.3d 416 (2013) (analyzing whether surveillance tapes were essential to effective law enforcement).

In *Haines-Marchel*, the court appears to conclude that the *Fischer* and *Gronquist* Courts reached the issue of whether "how a police agency carries out investigations qualifies as specific intelligence information" *Haines-Marchel*, 183 Wn. App. at 667–68 (emphasis omitted), but this is an erroneous interpretation of those cases. The only disputed issue in

Fischer was whether the nondisclosure of the surveillance videos was "essential to effective law enforcement"—it was undisputed that the surveillance video tapes constituted specific intelligence information—and therefore the *Fischer* Court did not undertake an analysis of what constituted specific intelligence information. *See Fischer,* 160 Wn. App. at 725–26. The *Haines-Marchel* Court relies on *Fischer* and *Gronquist* in evaluating whether specific intelligence information can include methods of investigation, but this reliance is misplaced, as *Fischer* and *Gronquist* only evaluated whether investigative methods could be "essential to effective law enforcement." *Haines-Marchel,* 183 Wn. App at 667–69; *Fischer,* 160 Wn. App. at 725–26; *Gronquist*, 177 Wn. App. 399.

Even applying the *Haines-Marchel* Court's erroneous reasoning to the case at hand, make, model, and pricing information do not constitute "specific intelligence information." The *Haines-Marchel* Court found that textual descriptions of how the State Department of Corrections evaluated and responded to informants' tips and how security cameras were deployed (placement, times of recording, etc.) constituted investigative methods and therefore "specific intelligence information." Make, model, and pricing information for cell site simulators do not reveal TPD's deployment methods of using cell site simulators, and therefore, even under *Haines-Marchel*, do not constitute specific intelligence information.

At argument before the Court below, the United States relied entirely on drawing a connection between knowing the make and model of a cell site simulator and knowing the capabilities of the Tacoma Police Department to justify withholding the information as essential to effective law enforcement. RP 28–29 (4/13/18). There was no attempt at the hearing to prove that these records constituted specific intelligence information within the narrow interpretations of this exemption. The trial court focused on the effective law enforcement argument alone, but the analysis set forth by the PRA requires much more than this. *Id*. at 34. The City has never demonstrated that the make, model, pricing, or manuals themselves concern "the gathering or distribution of information" or contain "evaluated conclusions"—in other words, specific intelligence information.

With regard to the manuals, while some information in the cell site simulator manual may constitute specific intelligence information, the entire manual does not. TPD may redact specific intelligence information contained in the manual, but it bears the burden of justifying those redactions. TPD's withholding of the manuals in their entirety is not justified.

2. *The withheld and redacted information is not "essential to effective law enforcement."*

The PRA's goal is transparency and accountability, meaning that the public has a right to understand what equipment is being used to surveil the public and how the public's money is being used to do so. The secrecy around the make and model of equipment is not essential to effective law enforcement. Any argument that the price and model of the cell site simulator equipment should be exempt from disclosure because it would reveal information regarding TPD's cell site simulator and the resources available to TPD is applicable to *all* technology and equipment in TPD's possession—from radar speed detectors to Tasers to wiretaps to x-ray cameras. Knowing the make and model of TPD's speed detectors reveals TPD's capabilities, but it does not make that information "essential to effective law enforcement" (or "specific intelligence information" for that matter), nor does it diminish the public's right under the PRA to know such information. Indeed, holding such information to be "essential to effective law enforcement" would set the bar so low, it is difficult to imagine what technology would *not* fall within the exemption under such a standard.

In *Fischer* and *Gronquist*, the court decided that the prison video surveillance recordings were exempt from disclosure because of

"information about investigative methods that would be disclosed, such as which cameras were recording, which were dummies, when cameras were off or on, their resolution and field of view[.]" *Haines-Marchel*, 183 Wn. App. at 667–668. These decisions focused entirely on the question of whether that information, which could be revealed by the disclosure of these surveillance videos, was essential to effective law enforcement. Such information relates to *how* the equipment is being *deployed* and so *Fischer* and its progeny do not control the case at hand; the manual, make and model, and pricing data do not reveal TPD's methods of deploying and utilizing the cell site simulator.

The argument that disclosing an operating manual or pricing information would disclose the same sort of developed strategy for gathering or distribution of information, information about an enemy, or evaluated conclusions from such information, does not apply. Nothing in the *Fischer* opinion suggests that the *Fischer* Court would have found information about camera models or pricing information exempt, or similar identifying information contained in manuals. "Essential to effective law enforcement" is a demanding standard and one prong of a narrowly construed PRA exemption. It is not enough that law enforcement would prefer to not disclose the information, or if it would be "inconvenient" to law enforcement; it must be *essential* to effective law

enforcement. Because the withheld information is not "essential to effective law enforcement," it is not exempt under RCW 42.56.240(1).

If the Court does not have enough information to evaluate the propriety of the redactions, Plaintiffs request that the Court review *in camera* the contested public records that were withheld or redacted in order to determine whether all or part of these records should have been withheld. "Courts may examine any record in camera in any proceeding brought under this section." RCW 42.56.550(3)(pertinent part).

3. *The operating manual.*

The City completely withheld one set of public records it identified as "Operator's manuals for cell sit [sic] simulators," even though the manuals do not in their entirety qualify as specific intelligence information essential to effective law enforcement. [11] CP 745. The PRA provides, in pertinent part, "the exemptions of this chapter are inapplicable to the extent that information, the disclosure of which would violate personal privacy or vital governmental interests, can be deleted from the specific

[11] Plaintiffs anticipate that the City will argue the manuals have been destroyed. Whether or not they have is relevant to the remedy the Court may implement, but has no bearing on the City's liability for improperly withholding them at the time it responded to Plaintiffs' PRA request. Furthermore, while the record is clear that the original hard copy manual was destroyed, Detective Jeffrey Shipp's testimony is that later manuals are saved electronically on the laptop associated with the cell site simulator. CP 1079-85.

records sought." RCW 42.56.210(1). The City should have produced the manuals with redactions:

> In general, the Public Records Act does not allow withholding of records in their entirety. Instead, agencies must parse individual records and must withhold only those portions which come under a specific exemption. Portions of records which do not come under a specific exemption must be disclosed.

PAWS, 125 Wn.2d at 261 (citing RCW 42.17.310(2) (Recodified as RCW 42.56.210(1))).

While there is no prior evaluation by any Washington appellate court whether an entire manual could be exempt under the PRA, the Federal Communications Commission (FCC) did conduct an analysis of this very question in response to a request for cell site simulator manuals under the Freedom of Information Act (FOIA) and determined that the manuals should be produced in redacted form. *In the Matter of Matthew Keys Shawn Musgrave*, 31 FCC Rcd. 11398 (FCC 2016) (available at CP 1091) ("*Musgrave*"). "In interpreting Washington's Public Disclosure Act, our courts may look to the federal courts and their interpretation of FOIA." *Sheehan*, 114 Wn. App. at 344 (citation omitted). While the FCC is not a federal court, the analysis is no less persuasive.

The FCC's decision included the analysis of an exemption under FOIA very similar to RCW 42.56.240(1), that is, "'records or information

compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations or prosecutions… if such disclosure could reasonably be expected to risk circumvention of the law.'" *Musgrave*, 31 FCC Rcd. at 11401 (citing 5 U.S.C. § 552(b)(7)(E)). For purposes of the cell site simulator manual, this FOIA exemption is comparable enough to the PRA exemption claimed by TPD to provide guidance.

In *Musgrave*, the FCC directed the disclosure of "(1) paragraph and section headings that do not refer to technical or operational matters, (2) information about how required notifications are displayed on the products, (3) the FCC ID numbers of products, and (4) unrevealing section headings from technical specification tables." *Id.* at 11402. Further, the FCC directed previously redacted information to be produced in unredacted form, including, "(1) Harris's telephone and fax numbers on page i of the Manual, (2) a phrase disclosed at page B-1 ¶ 5 but redacted from pages i and ix, and (3) the letter headings for sections of the glossary on pages A1-A2." *Id.* Similarly, there is nothing about this information that would warrant an exemption under RCW 42.56.210(1).

In the lower court, the United States argued that the manual in this case is in the possession of a particular law enforcement agency, rather than the FCC, and therefore disclosure is more harmful. *See* CP 1133–35.

But who possesses the manual is insufficient to distinguish *Musgrave*, or to make the manual "essential for effective law enforcement." The same principles underlying the FCC's opinion in *Musgrave* are applicable here. Indeed, the FCC considered the fact that disclosure of some of the information could be harmful to law enforcement, and still affirmed disclosure of the manual, with redactions. *Musgrave,* 31 FCC Rcd. at 11401–02.

In any event, the manuals do not appear to be limited to one model of cell site simulator and are in fact applicable to multiple models. *See Musgrave,* 31 FCC Rcd. at 11398–99 & n.7 (noting that the single user manual produced is associated with the StingRay, StingRay II, and KingFish models); CP 1189 (Harris Corp. manual); CP 992–93 at 15–21 (filed under seal) (manual applicable to StingRay I, StingRay II, KingFish, HailStorm, HailStorm AmberJack, and HailStorm ArrowHead models/setups). As shown above, the make and model is not specific intelligence information at all, let alone essential to effective law enforcement, but even so, given the breadth of models covered by a single manual, disclosure of the manual would not reveal the particular make and model possessed by TPD.

The City has not met its burden to establish that the manuals are exempt from disclosure in their entirety and it should be required to

produce them in redacted form. TPD must analyze the manuals under Washington PRA law and disclose all information that is not specific intelligence information essential to effective law enforcement. Given that there are differences in the FOIA exemption and the PRA exemption, TPD's disclosure may include information beyond what was ordered disclosed in *Musgrave*.

Like the redactions, if the Court does not have enough information to evaluate the propriety of the withholdings, Plaintiffs request that the Court review *in camera* the withheld manuals to determine whether part of these records should be produced. *See* RCW 42.56.550(3).

VII. Response to City's Appeal

A. Inadequacy of the Search

As discussed above in Section VI.A, the City did not perform an adequate search for documents in response to Plaintiffs' PRA request. The City is correct that the fact that it withheld documents does not, alone, necessarily make its search inadequate. *Neighborhood All.*, 172 Wn.2d at 737–38. Nor do Plaintiffs contend that the City's search was inadequate solely due to the eleven documents it failed to produce. But, failure to identify and produce multiple clearly responsive documents—many of which were provided to other PRA requesters—is certainly evidence of an unreasonable search. And, as we have shown, TPD's search overall was

inadequate due to its failure to search several locations and custodians in a thorough manner. At the same time, by themselves the eleven documents that the City did not produce—which include emails, an invoice, a spreadsheet, a warrant template, and meeting minutes—are strong evidence that the City's search was inadequate and justify the trial court's finding of inadequacy.

However, even if this Court were to determine that the City's search was not inadequate, Plaintiffs were nevertheless deprived of these eleven documents in violation of the PRA. A violation of the PRA occurs whenever any public record is wrongfully withheld. RCW 42.56.550(4) (the court has discretion to impose penalties for "any public record" that is withheld). *See, e.g.*, *Yousoufian*, 152 Wn.2d at 429–30 (discussing predecessor penalty statute regarding "any requested public record" wrongfully withheld). This foundational PRA statute and penalties for "any record" wrongfully withheld are independent from the question of an inadequate search. Any wrongfully withheld document equals a violation.

Thus, a finding of inadequacy of the search is not a prerequisite to determining that the City violated the PRA by withholding and failing to provide responsive documents in its possession. As to each of the contested documents the trial court ruled on, that court was correct in finding a PRA violation, and this Court should so hold as well.

B. TPD Violated the PRA On All of the Responsive Documents Found Since the Search Closed

The eleven documents for which the trial court found PRA violations were all clearly responsive to Plaintiffs' PRA request (CP 649 – 650), which can only be read as requesting every record relating to the acquisition and use of cell site simulator technology. The City acknowledges that ten of the eleven were responsive (Appellant's Br. at 21–34), and the trial court correctly found all eleven were responsive. In its appeal, the City provides no justification for why any of these documents were not provided; individually and in the aggregate they show a failure to abide by the commands of the PRA.

The City cannot and does not claim that PRA exemptions support nondisclosure of these records. *See* RCW 42.56.550(1) (burden on public agency to show exemptions support nondisclosure). And none of the City's other proffered reasons for each failure to disclose supports its attempts to avoid PRA liability for these records.

1. *Warrant Template*

The City is mistaken to suggest that the warrant template (CP 704–24) is not responsive to Plaintiffs' PRA request. It is difficult to fathom how a Word document that is used by TPD as the template for *all* warrants

seeking cell site simulator authorization could be considered non-responsive. Plaintiffs' requests included the following:

- "All records regarding TPD's acquisition, use, or lease of Cell Site Simulators, including but not limited to, communications, invoices, purchase orders, contracts, loan agreements, grant applications, evaluation agreements, and delivery receipts." (CP 649 at Request 1).
- "All applications submitted to state or federal courts for warrants, orders, or other authorizations for use of Cell Site Simulators in criminal investigations, as well as any warrants, orders, authorizations, denials of warrants, denials of orders, denials of authorizations, and returns of warrants associated with those applications." (CP 650 at Request 10).

The warrant template is undoubtedly a record regarding TPD's "use" of cell site simulators responsive to PRA Request 1: it is the document that TPD fills out and presents to the court for authorization to use the device. Along with PRA Request 10 regarding warrants, it is obvious that Plaintiffs were seeking records of just this kind. The document shows exactly the language that is used in all of the applications for warrants that authorize the cell site simulator. As discussed elsewhere, TPD has not provided any of the actual warrants, which makes the failure

to provide this document—which contains clear information about what all of the warrants say and what actions a court authorizes—egregious. This was a clear denial of what anyone reading the PRA request would know Plaintiffs were seeking.

Even though this document is a template and not filled in, it obviously meets the definition of a public record for use of the cell site simulator, which "includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function… *regardless of physical form or characteristics*." RCW 42.56.010(3) (emphasis added). The template shows how TPD applies for and uses cell site simulator technology and is clearly "…*associated with…*" warrant applications. (CP 650 at Request 10 (emphasis added)). The template is responsive to Plaintiffs' PRA request and was not provided until its existence was disclosed during discovery.

The City's attempt to characterize the Word document as a "blank form" is misleading. A "blank form" implies a formal document that seeks information, like something you would fill out at the DMV or a doctor's office, which does not itself contain information. That is not the case with the warrant template. It is not a public, formal form to be filled out, devoid of any information on its own. It is a non-publicly available Word document that TPD detectives use as a starting point when preparing

warrants for cell site simulator use. The document is comprised of a proposed order, an application and an order sealing documents. In these documents, "cell site simulator" is mentioned more than 20 times.

In a further attempt to avoid liability, Appellants argue that Plaintiffs were not specific enough in their PRA request because they "did not expressly ask for any blank forms or a warrant template." Appellant's Br. at 17. This is not the standard the PRA requires. The PRA requires requestors to identify with reasonable clarity the documents that are desired so that the agency can locate the record. Appellant's Br. at 15. A requestor need not divine and identify every possible format in which records could exist. The fact that Plaintiffs did not use the City's magic words of "blank form" or "warrant template" does not make the warrant template any less responsive to their PRA request.

The City cites *Wright v. State,* 176 Wn. App. 585, 309 P.3d 662 (2013), in support of its claim that the PRA request was not specific enough. But Wright requested only public records about a specific Child Protective Services case she was involved in; after filing suit she claimed a PRA violation because the State did not also provide CPS investigative manuals and protocols. The court found that a "request for 'any and all documents relating to Amber Wright' did not include the DSHS protocols and manual with 'reasonable clarity[.]'" *Id.* at 594. In contrast, Plaintiffs'

PRA request, which contains no fewer than fourteen subparts related to cell site simulators, specified with more than reasonable clarity that Plaintiffs wanted all records related to the use and deployment of cell site simulator technology. The warrant template is well within that ambit.

Conversely, the City also claims Plaintiffs' use of the phrase "all records" is too broad under RCW 42.56.080(1) and case law. But the statute says the opposite: "…a request for all records regarding a particular topic or containing a particular keyword or name *shall not* be considered a request for all of an agency's records." (Emphasis added). Plaintiffs request for all records related to use of the cell site simulator and for warrants related to the cell site simulator is exactly what the statute allows for and is not overbroad.

The cases the City cites do not lead to a different result. In *Hangartner v. City of Seattle*, 151 Wn. 2d 439, 90 P.3d 26 (2004), the Court found overbroad a PRA request for "all books, records, documents of every kind and the physical properties of the Elevated Transportation Company," which was not further limited by topic or keyword as required by the statute. The holding in *Bonamy v. City of Seattle*, 92 Wn. App. 403, 960 P.2d 447 (1998), was that there was no clear request for specific public records at all. Here, Plaintiffs appropriately sought a range of records specifically related to the cell site simulator; the warrant template

is well within that range and should have been provided. TPD's intentional withholding of the document as "non-responsive" and its failure to provide it violated the PRA.

2. *Records Disclosed During Discovery or Found Separately*

Records the City disclosed during discovery (CP 672–700): The City argues with respect to the clearly responsive email chains in Exhibits 5–9, that because the City cannot now—three years later—locate the records in their original locations, the City cannot be held liable for failing to produce records that do not exist. This argument is baseless. First, it is a logical fallacy to conclude that the records must not have existed at the time of the PRA request because the City does not have them *now*. Second, the City itself provided these records to the Plaintiffs during discovery in this case—as part of its disclosure that it had already provided them to other PRA requesters but not to Plaintiffs—and so must have had them at the time of Plaintiffs' PRA request and continuously thereafter until their disclosure in June 2016. The City has no defense that these records "did not exist" at the relevant time.[12] TPD was required to

[12] Contrary to the City's claims that the records had been deleted by the time of Plaintiffs' PRA request, the affidavit of the person in charge of the PRA search says only that he believes they may have been deleted by the time of the PRA request, while at the same time acknowledging that these records were provided to other PRA requesters and then to Plaintiffs in

conduct an adequate search for the records *at the time of the request.* The fact that those records are not found on a particular computer *now* is irrelevant to whether TPD violated the PRA at the time of Plaintiffs' request.[13]

Notably, many of these documents are especially important public records in response to Plaintiffs' request, as they emphasize the position of the federal government regarding release of information about the cell site simulator and may have influenced TPD's decisions about what to release in response to Plaintiffs' PRA request. The City has provided no reasonable excuse for TPD's failure to earlier provide these clearly important and responsive public records that obviously were in TPD's possession and control when TPD responded to Plaintiffs' PRA request.

Advisory Committee Minutes and Agenda (CP 725–35): The City claims that these records need not have been found by TPD because they were in a location that it did not need to search, and that in any event they were available on a City website so TPD had no obligation to provide

---

discovery—thus conceding the City had the records up to the time they were disclosed in discovery. CP 1117.

[13] The cases the City cites are inapposite. *See, Bldg. Indus. Ass'n of Wash. v. McCarthy*, 152 Wn. App. 720, 739, 218 P.3d 196 (2009) (dealing with "records that did not exist at the time of a request."); *West v. Wash. Dep't of Nat. Res*., 163 Wn, App. 235, 244, 258 P.3d 78 (2011) (noting the state agency "inadvertently lost [the contested] e-mails almost one year before West made his request.")

them under the PRA. Neither claim justifies the failure to provide these records.

The records at issue are meeting minutes of two meetings of the City of Tacoma Citizen Review Panel. At both meetings, TPD personnel discussed the revelation that TPD had been using cell site simulator technology and answered questions about cell site simulator use. As the City admits, these records were obviously responsive to Plaintiffs' PRA request.

The City nevertheless claims it is unreasonable to expect it to look for these records at the City Manager's Office. But the person in charge of TPD's search testified that in he does sometimes request that the City Manager's Office be checked when complying with PRA requests and that he could not recall whether that happened in this case. CP 1116. He also noted that some of the records TPD did disclose to Plaintiffs directly refer to the meetings at issue. *Id.* TPD was obligated under the PRA to search a commonly searched, and therefore clearly "reasonable" location for these directly responsive records. *Neighborhood All.*, 172 Wn.2d at 736 (discussing situation, as here, where "the agency's own responses show another place where responsive records might be found without an unreasonable burden on the agency…"). Lastly, the minutes indicate that

Tech Unit officers presented at the meetings, and therefore should have known about the existence of related records.

Neither is it an excuse under the PRA (much less an actual exemption) that an undisclosed record was available elsewhere. *Hearst Corp.*, 90 Wn.2d at 132. To hold otherwise would require requestors to scour the Internet and the public realm for unidentified documents that may or may not exist, with no guidance from the agency.

Billing Spreadsheet (CP 658–71): Appellants argue that the billing spreadsheet at issue, referred to as Exhibit 4, is not evidence of a PRA violation due to an agreement with Plaintiffs' prior attorneys. Appellants misunderstand Plaintiffs' argument. Appellant's Br. at 30–33. Plaintiffs do not question Appellants' assertion that an agreement was reached to edit the billing spreadsheet to contain only instances where the cell site simulator was used. Rather, Plaintiffs contend that the edited spreadsheet provided pursuant to the parties' agreement at the time of the PRA Request omits several instances of cell site simulator usage, as Exhibit 4 itself shows.

In its second and final disclosure of records on December 18, 2015, TPD provided a two-page document entitled "2015 Spreadsheet." CP 1259–61. This spreadsheet contains entries for only three dates in 2015, the last of which is June 27, 2015. When compared to Exhibit 4—

the full 2015 spreadsheet—the truncated "2015 Spreadsheet" does not contain all of the uses of the cell site simulator in 2015, despite the parties' agreement.

Detective Krause testified that the best way to determine from the billing spreadsheets whether the cell site simulator has been deployed is if the words "capture" or "attempt capture" appear. CP 854–55. In Exhibit 4, the word "capture" appears eleven times in connection with entries in 2015 before the date of when TPD sent the 2015 Spreadsheet to Plaintiffs in mid-December of 2015. CP 668–70.

The contested spreadsheet therefore appears to demonstrate numerous instances where TPD used the cell site simulator, but that the City failed to disclose to Plaintiffs. When TPD deploys the cell site simulator is central to Plaintiffs' PRA request and should have been fully disclosed. The Superior Court correctly determined that Appellants violated the PRA by failing to disclose *all* instances where the cell site simulator was used, and this Court should affirm.

Invoice (CP 739–41): The City simply claims inadvertence in TPD's failure to provide this document, which amounts to an admission of a PRA violation and a plea for a reduced penalty. The City makes no legal defense to support the nondisclosure. The Superior Court's holding should be affirmed.

C. The Trial Court Did Not Abuse Its Discretion on PRA Penalties

Where a violation of the PRA has been found, the court has discretion to award the prevailing party "an amount not to exceed one hundred dollars for each day that he or she was denied the right to inspect or copy said public record." RCW 42.56.550(4). Penalties imposed by a trial court for violations of the Public Records Act are reviewed for abuse of discretion. *Yousoufian*, 152 Wn.2d at 430–31. Determination of a PRA per diem penalty involves determining: (1) the amount of days the party was denied access to the public record and (2) the appropriate amount of the penalty. *Yousoufian v. Office of Ron Sims*, 168 Wn.2d 444, 459, 229 P.3d 735 (2010). Although the existence or absence of an agency's bad faith is the principal factor for consideration, no showing of bad faith is necessary before a penalty may be imposed on an agency. *Amren v. City of Kalama*, 131 Wn.2d 25, 36–38, 929 P.2d 389 (1997).

It is undisputed that the City failed to provide numerous responsive documents to Plaintiffs, and the City's attempts to avoid liability are not persuasive. The trial court found that TPD's search was inadequate and that TPD had withheld numerous records, and properly applied the *Yousoufian* factors to implement fair and reasonable penalties "to deter improper denials of access to public records" and hold agencies

"accountable to the people of the State." CP 1652 (citing *Faulkner v. Wash. Dep't of Corr.*, 183 Wn. App. 93, 332 P.3d 1136 (2014); *Yousoufian*, 168 Wn.2d at 444.) The trial court did not abuse its discretion in awarding substantial penalties.

In *Yousoufian*, the court set forth guidelines for determining appropriate PRA violation penalties. Aggravating factors that may increase the penalty are:

> (1) a delayed response by the agency, especially in circumstances making time of the essence, (2) lack of strict compliance by the agency with all the PRA procedural requirements and exceptions, (3) lack of proper training and supervision of the agency's personnel, (4) unreasonableness of any explanation for noncompliance by the agency, (5) negligent, reckless, wanton, bad faith, or intentional noncompliance with the PRA by the agency, (6) agency dishonesty, (7) the public importance of the issue to which the request is related, where the importance was foreseeable to the agency, (8) any actual personal economic loss to the requestor resulting from the agency's misconduct, where the loss was foreseeable to the agency, and (9) a penalty amount necessary to deter future misconduct by the agency considering the size of the agency and the facts of the case.

Yousoufian, 168 Wn.2d at 467–68 (footnotes omitted). The Supreme Court recently added an additional aggravating factor that is relevant here: "[T]he failure to perform an adequate search is at least an aggravating factor, to be considered in setting the daily-penalty amount."

Neighborhood All., 172 Wn.2d at 724. Mitigating factors that may decrease the penalty are:

> (1) a lack of clarity in the PRA request, (2) the agency's prompt response or legitimate follow-up inquiry for clarification, (3) the agency's good faith, honest, timely, and strict compliance with all PRA procedural requirements and exceptions, (4) proper training and supervision of the agency's personnel, (5) the reasonableness of any explanation for noncompliance by the agency, (6) the helpfulness of the agency to the requestor, and (7) the existence of agency systems to track and retrieve public records.

Yousoufian, 168 Wn.2d at 467 (footnotes omitted).

The City failed to produce multiple types of documents from several locations and continues to argue that it had no obligation to produce several of the withheld documents. This is not an instance where a single document was overlooked, or a folder was forgotten about. The issue was pervasive. Emails were withheld. An invoice was withheld. A spreadsheet of cell site simulator usage was improperly edited. Citizen Review Panel minutes where cell site simulators were discussed in response to public outcry were withheld. The key document used to create warrants authorizing cell site simulators was intentionally withheld, and indeed, the City's position is that it would have no obligation to provide it to Plaintiffs today. The trial court was fully justified not only in finding

multiple PRA violations (and referencing the *Yousoufian* factors) but also in determining the search was inadequate. CP 1650–58.

In addition to the baseline PRA violations and the finding of an inadequate search –which alone justify significant penalties–several of the aggravating *Yousoufian* factors are present: negligence (factor 5); the explanations for failure to produce are questionable (factor 4); there are reasons to doubt TPD's PRA methods and supervision as exhibited in the inadequate search (factors 2 and 3); and deterrence of future inadequate searches (factor 9). In addition, as demonstrated by the over 35 PRA requests TPD received regarding cell site simulators (CP 96–97) and the presence of the media at the penalties hearing, there is understandably great continuing public interest (factor 7) in TPD's deployment of the intrusive cell site simulator technology. *See* RP at 5 – 7 (5/24/18).

Even under the City's suggested reformulation of the factors into four (Appellant's Br. at 39–40), which Plaintiffs do not concede necessarily controls application of the factors, the trial court did not abuse its discretion. Two of the suggested collapsed factors—high public importance of the underlying issue and "incentive to induce future compliance" fully support the trial court's imposition of the substantial daily penalties imposed.

Moreover, the trial court did find that the warrant template had been deliberately withheld, which is an instance of bad faith that justifies the heavy penalty imposed for that document. And the trial court properly exercised its discretion in determining that the many PRA violations it found demonstrate a strong need to deter future failures to provide all responsive records and otherwise comply with the PRA. The City's arguments that TPD followed all PRA requirements and that the City has adequate training and supervision are based on the City's failed attempts to show that the PRA was not violated as to the missing documents. The trial court properly recognized that the missing documents showed a failure of the PRA system and the need for deterrence and reform.

Looking holistically at the situation – the inadequate search, the numerous withheld documents, the City's willful withholding – it is clear that the trial court did not abuse its discretion in setting penalties.

D. The Trial Court Did Not Abuse Its Discretion on Attorneys' Fees and Costs.

The trial court's order on attorneys' fees and costs should stand unless this court finds an abuse of discretion. *Sanders*, 169 Wn.2d at 867. The City does not challenge the trial court's award of costs, so that award is conceded. The City's allegations about the fee award do not support a finding of abuse of discretion.

The City correctly states that attorneys' fees in a PRA case are determined under the familiar "lodestar" method, i.e., a reasonable hourly rate multiplied by a reasonable number of hours expended on the case. *Sanders*, 169 Wn.2d at 869. The trial court correctly cited and applied this method. CP 1657. The court reduced Plaintiffs' proposed rates to a rate the court found was closer to the rates in the local Pierce County community. *Compare* CP 1405 (footnote 3) (rates requested) with CP 1657 (court's determination of rates).

The trial court did award the adjusted fees for all hours claimed by Plaintiffs, but the hours claimed were already heavily discounted for duplication of effort, change of counsel in the middle of the case, and because Plaintiffs did not prevail on all issues, as explained in Plaintiffs' counsels' declarations. CP 1419–37. It was well within the trial court's discretion to accept counsels' sworn statements that these discounts were made in the fee claim itself.

Contrary to the City's suggestion (Appellant's Br. at 36), there were in fact three, not two, main issues the trial court ruled on, and Plaintiffs prevailed on two of them. The trial court found that TPD violated the PRA as to each of the eleven records Plaintiffs claimed could have been provided, and also held generally that TPD's search was inadequate for a number of reasons. Plaintiffs prevailed on both of these

major parts of the case. Although Plaintiffs did not prevail on one claim regarding the PRA exemptions as applied to redactions and withholding, this claim—and the work performed on it—was inextricably bound with the other two. While unsuccessful claims that are truly unrelated to the successful claims should result in a discount in attorney fee awards, related claims do not. *Ermine v. City of Spokane*, 143 Wn.2d 636, 643, 23 P.3d 492 (2001) (citing *Hensley v. Eckerhart*, 461 U.S. 424, 440, 103 S. Ct. 1933, 76 L. Ed. 2d 40 (1983)). Moreover, "the extent of a plaintiff's success is the crucial factor in determining the proper attorney's fees award[.]" *Id.*[14] The redaction claim was not wholly unrelated to Plaintiffs' overall successful challenge to the City's handling of their PRA request.

Even if the Court finds that the redaction claim is unrelated to Plaintiffs' other claims, reduction of Plaintiffs' attorneys' fees by one third is not warranted for many reasons. First, many hours were spent by Plaintiffs' counsel on discovery, which is necessary to building the case and not specific to any one issue (and if it were specific to an issue, it would not be to the propriety of the PRA exemptions relied on in redacting and withholding documents, as that is a legal issue).

[14] *Ermine* involved a fee claim under 42 U.S.C. § 1988 in a civil rights case, but the "lodestar" principles apply in such cases as they do in PRA cases.

Second, while the propriety of the City's application of PRA exemptions can be considered a third issue in this case, it was significantly smaller than the other two, as evidenced by the briefings and oral arguments. Indeed, the trial court dedicates only a single sentence to the issue in the entirety of its nine-page opinion. CP 1657.

Given the overall level of success, the heavy discounts Plaintiffs made to their fee claim in the first place, the trial court's lowering of the hourly rates, and that the redaction was the smallest of the three issues, the trial court did not abuse its discretion in the award of fees. At most, if this court determines the redaction issue was sufficiently separate, time entries specifically referencing that part of the research and briefing should simply be subtracted from the fee award.

VIII. Request for Attorneys' Fees on Appeal

Public Records Act fees are available to a party challenging an agency's actions who prevails on appeal. *PAWS*, 125 Wn.2d at 271. Pursuant to RAP 18.1, Plaintiffs-Respondents request fees on appeal.

IX. Conclusion

For all of the foregoing reasons, this Court should hold that TPD conducted an inadequate search and wrongfully withheld and redacted information about cell site simulators as detailed above. The Court should order TPD to conduct an additional search for documents and affirm the

trial court's assessment of penalties, costs and fees for the PRA violations that court found, and remand the case for further proceedings.

Respectfully submitted this 13th day of February, 2019.

By:
/s/John Midgley
John Midgley, WSBA #6511
Lisa Nowlin, WSBA #51512
AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 Fifth Avenue, Suite 630
Seattle, WA 98164
206 624-2184
jmidgley@aclu-w.org
lnowlin@aclu-wa.org

Attorneys for Plaintiffs-Respondents

No. 52072-9-II

COURT OF APPEALS FOR THE STATE OF WASHINGTON
DIVISION TWO

CITY OF TACOMA

Appellant,

v.

ARTHUR BANKS, ET. AL.,

Respondents.

CERTIFICATE OF SERVICE

I declare, under penalty of perjury and under the laws of the State of Washington, that I caused to be served a copy of the Brief of Respondents and the attached Appendix A and Appendix B via the AOC Portal on February 13th, 2019 on the following. Per the request of the court I caused the same Brief of Respondents and Appendices to be re-filed and served as a single document on the date below:

COUNSEL FOR APPELLANT

Margaret A. Elofson, WSBA #23038
Tacoma Deputy City Attorney
747 Market Street, Suite 1120
Tacoma, WA 98402
253-591-5885
margaret.elofson@ci.tacoma.wa.us

Signed this 14th day of February, 2019, at Seattle, King County, WA.

By: */s/Kaya McRuer*

Kaya McRuer, Paralegal
ACLU OF WASHINGTON FOUNDATION
901 5th Avenue, Suite 630
Seattle, Washington 98164
(tel) (206) 624-2184
kmcruer@aclu-wa.org

APPENDIX A

RCW 9.73.260

Pen registers, trap and trace devices, cell site simulator devices.

(1) As used in this section:

(a) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications, and such term includes any electronic storage of such communication.

(b) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include:

(i) Any wire or oral communication;

(ii) Any communication made through a tone-only paging device; or

(iii) Any communication from a tracking device, but solely to the extent the tracking device is owned by the applicable law enforcement agency.

(c) "Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications.

(d) "Pen register" means a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(e) "Trap and trace device" means a device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

(f) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (i) Identifying, locating, or tracking the movements of a communications device; (ii) intercepting, obtaining, accessing, or forwarding the communications, stored data, or metadata of a communications device; (iii) affecting the hardware or software operations or functions of a communications device; (iv) forcing transmissions from or connections to a communications device; (v) denying a communications device access to other communications devices, communications protocols, or services; or (vi) spoofing or simulating a communications device, cell tower, cell site, or service , including, but not limited to, an international mobile subscriber identity catcher or other invasive cell phone or telephone surveillance or eavesdropping device that mimics a cell phone tower and sends out signals to cause cell phones in the area to transmit their locations, identifying information, and communications content, or a passive interception device or digital analyzer that does not send signals to a communications device under surveillance. A cell site simulator device does not include any device used or installed by an electric utility, as defined in RCW **19.280.020**, solely to the extent such device is used by that utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

(2) No person may install or use a pen register, trap and trace device, or cell site simulator device without a prior court order issued under this section except as provided under subsection (6) of this section or RCW **9.73.070**.

(3) A law enforcement officer may apply for and the superior court may issue orders and extensions of orders authorizing the installation and use of pen registers, trap and trace devices, and cell site simulator devices as provided in this section. The application shall be under oath and shall include the identity of the officer making the application and the identity of the law enforcement agency

conducting the investigation. The applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(4) If the court finds that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation and finds that there is probable cause to believe that the pen register, trap and trace device, or cell site simulator device will lead to obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed or reasonably appears about to be committed, or will lead to learning the location of a person who is unlawfully restrained or reasonably believed to be a witness in a criminal investigation or for whose arrest there is probable cause, the court shall enter an ex parte order authorizing the installation and use of a pen register, trap and trace device, or cell site simulator device. The order shall specify:

(a)(i) In the case of a pen register or trap and trace device, the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; or

(ii) In the case of a cell site simulator device, the identity, if known, of (A) the person to whom is subscribed or in whose name is subscribed the electronic communications service utilized by the device to which the cell site simulator device is to be used and (B) the person who possesses the device to which the cell site simulator device is to be used;

(b) The identity, if known, of the person who is the subject of the criminal investigation;

(c)(i) In the case of a pen register or trap and trace device, the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; or

(ii) In the case of a cell site simulator device: (A) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the device to which the cell site simulator device is to be attached or used; (B) if known, the physical location of the device to which the cell site simulator device is to be attached or used; (C) the type of device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used; (D) the geographic area that will be covered by the cell site simulator device; (E) all categories of metadata, data, or information to be collected by the cell site simulator device from the targeted device including, but not limited to, call records and geolocation information; (F) whether or not the cell site simulator device will incidentally collect metadata, data, or information from any parties or devices not specified in the court order, and if so, what categories of information or metadata will be collected; and (G) any disruptions to access or use of a communications or internet access network that may be created by use of the device; and

(d) A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device, or cell site simulator device relates.

The order shall direct, if the applicant has requested, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register, trap and trace device, or cell site simulator device. An order issued under this section shall authorize the installation and use of a: (i) Pen register or a trap and trace device for a period not to exceed sixty days; and (ii) a cell site simulator device for sixty days. An extension of the original order may only be granted upon: A new application for an order under subsection (3) of this section; and a showing that there is a probability that the information or items sought under this subsection are more likely to be obtained under the extension than under the original order. No extension beyond the first extension shall be granted unless: There is a showing that there is a high probability that the information or items sought under this subsection are much more likely to be obtained under the second or subsequent extension than under the original order; and there are extraordinary circumstances such as a direct and immediate danger of death or serious bodily injury to a law enforcement officer. The period of extension shall be for a period not to exceed sixty days.

An order authorizing or approving the installation and use of a pen register, trap and trace device, or cell site simulator device shall direct that the order be sealed until otherwise ordered by the court and

that the person owning or leasing the line to which the pen register, trap and trace device, and cell site simulator devices is attached or used, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register, trap and trace device, or cell site simulator device or the existence of the investigation to the listed subscriber or to any other person, unless or until otherwise ordered by the court.

(5) Upon the presentation of an order, entered under subsection (4) of this section, by an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in subsection (4) of this section.

Upon the request of an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such law enforcement officer all additional information, facilities, and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in subsection (4) of this section. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this section. A good faith reliance on a court order under this section, a request pursuant to this section, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(6)(a) Notwithstanding any other provision of this chapter, a law enforcement officer and a prosecuting attorney or deputy prosecuting attorney who jointly and reasonably determine that there is probable cause to believe that an emergency situation exists that involves immediate danger of death or serious bodily injury to any person that requires the installation and use of a pen register, trap and trace device, or cell site simulator device before an order authorizing such installation and use can, with due diligence, be obtained, and there are grounds upon which an order could be entered under this chapter to authorize such installation and use, may have installed and use a pen register, trap and trace device, or cell site simulator device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with subsection (4) of this section. In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register, trap and trace device, or cell site simulator device, whichever is earlier. If an order approving the installation or use is not obtained within forty-eight hours, any information obtained is not admissible as evidence in any legal proceeding. The knowing installation or use by any law enforcement officer of a pen register, trap and trace device, or cell site simulator device pursuant to this subsection without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter and be punishable as a gross misdemeanor. A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law

enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

(b) A law enforcement agency that authorizes the installation of a pen register, trap and trace device, or cell site simulator device under this subsection (6) shall file a monthly report with the administrator for the courts. The report shall indicate the number of authorizations made, the date and time of each authorization, whether a court authorization was sought within forty-eight hours, and whether a subsequent court authorization was granted.

(c) A law enforcement agency authorized to use a cell site simulator device in accordance with this section must: (i) Take all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order; (ii) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the applicable court order immediately following such collection and must not transmit, use, or retain such information or metadata for any purpose whatsoever; and (iii) must delete any information or metadata collected from the target specified in the court order within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

[**2015 c 222 § 2; 1998 c 217 § 1.**]

NOTES:

Effective date—2015 c 222: See note following RCW **9.73.270**.

*Local government reimbursement claims: RCW **4.92.280**.*

RCW 9.73.270

Collecting, using electronic data or metadata—Cell site simulator devices—Requirements.

The state and its political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without (1) that person's informed consent, (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or (3) acting in accordance with a legally recognized exception to the warrant requirements.

[**2015 c 222 § 1.**]

NOTES:

Effective date—2015 c 222: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately [May 11, 2015]." [**2015 c 222 § 4.**]

APPENDIX B

CERTIFICATION OF ENROLLMENT

ENGROSSED SUBSTITUTE HOUSE BILL 1440

Chapter 222, Laws of 2015

64th Legislature
2015 Regular Session

CELL SITE SIMULATOR DEVICES--COLLECTION OF DATA--WARRANT

EFFECTIVE DATE: 5/11/2015

Passed by the House April 16, 2015
Yeas 96 Nays 0

FRANK CHOPP

Speaker of the House of Representatives

Passed by the Senate April 14, 2015
Yeas 47 Nays 0

BRAD OWEN

President of the Senate

Approved May 11, 2015 2:05 PM

JAY INSLEE

Governor of the State of Washington

CERTIFICATE

I, Barbara Baker, Chief Clerk of the House of Representatives of the State of Washington, do hereby certify that the attached is **ENGROSSED SUBSTITUTE HOUSE BILL 1440** as passed by House of Representatives and the Senate on the dates hereon set forth.

BARBARA BAKER

Chief Clerk

FILED

May 12, 2015

Secretary of State
State of Washington

ENGROSSED SUBSTITUTE HOUSE BILL 1440

AS AMENDED BY THE SENATE

Passed Legislature - 2015 Regular Session

State of Washington 64th Legislature 2015 Regular Session

By House Public Safety (originally sponsored by Representatives Taylor, Goodman, Pollet, Scott, Condotta, Shea, G. Hunt, Young, Moscoso, Smith, Ryu, Jinkins, Magendanz, Farrell, and McCaslin)

READ FIRST TIME 02/17/15.

AN ACT Relating to prohibiting the use of a cell site simulator device without a warrant; amending RCW 9.73.260; adding a new section to chapter 9.73 RCW; and declaring an emergency.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** A new section is added to chapter 9.73 RCW to read as follows:

The state and its political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without (1) that person's informed consent, (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or (3) acting in accordance with a legally recognized exception to the warrant requirements.

Sec. 2. RCW 9.73.260 and 1998 c 217 s 1 are each amended to read as follows:

(1) As used in this section:

(a) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the

use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications, and such term includes any electronic storage of such communication.

(b) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include:

(i) Any wire or oral communication;

(ii) Any communication made through a tone-only paging device; or

(iii) Any communication from a tracking device, but solely to the extent the tracking device is owned by the applicable law enforcement agency.

(c) "Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications.

(d) "Pen register" means a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(e) "Trap and trace device" means a device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

(f) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (i) Identifying, locating, or tracking the movements of a communications device; (ii) intercepting, obtaining, accessing, or forwarding the communications, stored data, or metadata of a communications device; (iii) affecting the hardware or software operations or functions of a communications device; (iv) forcing transmissions from or connections to a communications device; (v) denying a communications device access to other communications

devices, communications protocols, or services; or (vi) spoofing or simulating a communications device, cell tower, cell site, or service, including, but not limited to, an international mobile subscriber identity catcher or other invasive cell phone or telephone surveillance or eavesdropping device that mimics a cell phone tower and sends out signals to cause cell phones in the area to transmit their locations, identifying information, and communications content, or a passive interception device or digital analyzer that does not send signals to a communications device under surveillance. A cell site simulator device does not include any device used or installed by an electric utility, as defined in RCW 19.280.020, solely to the extent such device is used by that utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

(2) No person may install or use a pen register ((~~or~~)), trap and trace device, or cell site simulator device without a prior court order issued under this section except as provided under subsection (6) of this section or RCW 9.73.070.

(3) A law enforcement officer may apply for and the superior court may issue orders and extensions of orders authorizing the installation and use of pen registers ((~~and~~)), trap and trace devices, and cell site simulator devices as provided in this section. The application shall be under oath and shall include the identity of the officer making the application and the identity of the law enforcement agency conducting the investigation. The applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(4) If the court finds that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation and finds that there is probable cause to believe that the pen register ((~~or~~)), trap and trace device, or cell site simulator device will lead to obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed or reasonably appears about to be committed, or will lead to learning the location of a person who is unlawfully restrained or reasonably believed to be a witness in a criminal investigation or for whose arrest there is probable cause, the court shall enter an ex parte order authorizing the installation and use of a pen register ((~~or~~

~~a~~)), trap and trace device, or cell site simulator device. The order shall specify:

(a)(i) In the case of a pen register or trap and trace device, the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; or

(ii) In the case of a cell site simulator device, the identity, if known, of (A) the person to whom is subscribed or in whose name is subscribed the electronic communications service utilized by the device to which the cell site simulator device is to be used and (B) the person who possesses the device to which the cell site simulator device is to be used;

(b) The identity, if known, of the person who is the subject of the criminal investigation;

(c)(i) In the case of a pen register or trap and trace device, the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; or

(ii) In the case of a cell site simulator device: (A) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the device to which the cell site simulator device is to be attached or used; (B) if known, the physical location of the device to which the cell site simulator device is to be attached or used; (C) the type of device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used; (D) the geographic area that will be covered by the cell site simulator device; (E) all categories of metadata, data, or information to be collected by the cell site simulator device from the targeted device including, but not limited to, call records and geolocation information; (F) whether or not the cell site simulator device will incidentally collect metadata, data, or information from any parties or devices not specified in the court order, and if so, what categories of information or metadata will be collected; and (G) any disruptions to access or use of a communications or internet access network that may be created by use of the device; and

(d) A statement of the offense to which the information likely to be obtained by the pen register ((~~or~~)), trap and trace device, or cell site simulator device relates.

The order shall direct, if the applicant has requested, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register ((~~or~~)), trap and trace device, or cell site simulator device. An order issued under this section shall authorize the installation and use of a: (i) Pen register or a trap and trace device for a period not to exceed sixty days; and (ii) a cell site simulator device for sixty days. An extension of the original order may only be granted upon: A new application for an order under subsection (3) of this section; and a showing that there is a probability that the information or items sought under this subsection are more likely to be obtained under the extension than under the original order. No extension beyond the first extension shall be granted unless: There is a showing that there is a high probability that the information or items sought under this subsection are much more likely to be obtained under the second or subsequent extension than under the original order; and there are extraordinary circumstances such as a direct and immediate danger of death or serious bodily injury to a law enforcement officer. The period of extension shall be for a period not to exceed sixty days.

An order authorizing or approving the installation and use of a pen register ((~~or a~~)), trap and trace device, or cell site simulator device shall direct that the order be sealed until otherwise ordered by the court and that the person owning or leasing the line to which the pen register ((~~or~~)), trap and trace device, and cell site simulator devices is attached or used, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register ((~~or~~)), trap and trace device, or cell site simulator device or the existence of the investigation to the listed subscriber or to any other person, unless or until otherwise ordered by the court.

(5) Upon the presentation of an order, entered under subsection (4) of this section, by an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with

respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in subsection (4) of this section.

Upon the request of an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such law enforcement officer all additional information, facilities, and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in subsection (4) of this section. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this section. A good faith reliance on a court order under this section, a request pursuant to this section, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(6)(a) Notwithstanding any other provision of this chapter, a law enforcement officer and a prosecuting attorney or deputy prosecuting attorney who jointly and reasonably determine that there is probable cause to believe that an emergency situation exists that involves immediate danger of death or serious bodily injury to any person that requires the installation and use of a pen register ((~~or a~~)), trap

and trace device, or cell site simulator device before an order authorizing such installation and use can, with due diligence, be obtained, and there are grounds upon which an order could be entered under this chapter to authorize such installation and use, may have installed and use a pen register ((~~or~~)), trap and trace device, or cell site simulator device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with subsection (4) of this section. In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register ((~~or~~)), trap and trace device, or cell site simulator device, whichever is earlier. If an order approving the installation or use is not obtained within forty-eight hours, any information obtained is not admissible as evidence in any legal proceeding. The knowing installation or use by any law enforcement officer of a pen register ((~~or~~)), trap and trace device, or cell site simulator device pursuant to this subsection without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter and be punishable as a gross misdemeanor. A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

(b) A law enforcement agency that authorizes the installation of a pen register ((~~or~~)), trap and trace device, or cell site simulator device under this subsection (6) shall file a monthly report with the administrator for the courts. The report shall indicate the number of authorizations made, the date and time of each authorization, whether a court authorization was sought within forty-eight hours, and whether a subsequent court authorization was granted.

(c) A law enforcement agency authorized to use a cell site simulator device in accordance with this section must: (i) Take all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order; (ii) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the applicable

court order immediately following such collection and must not transmit, use, or retain such information or metadata for any purpose whatsoever; and (iii) must delete any information or metadata collected from the target specified in the court order within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

NEW SECTION. **Sec. 3.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 4.** This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately.

Passed by the House April 16, 2015.
Passed by the Senate April 14, 2015.
Approved by the Governor May 11, 2015.
Filed in Office of Secretary of State May 12, 2015.

--- END ---

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION

February 14, 2019 - 10:21 AM

Transmittal Information

Filed with Court:	Court of Appeals Division II
Appellate Court Case Number:	52072-9
Appellate Court Case Title:	City of Tacoma, Appellant v Arthur C. Banks,et al, Respondents
Superior Court Case Number:	16-2-05416-7

The following documents have been uploaded:

- 520729_Briefs_20190214101740D2686803_1821.pdf
  This File Contains:
  Briefs - Respondents/Cross Appellants
  The Original File Name was 2019 02 14 Respondents Cross Appeal and Response refiled as one document.pdf

A copy of the uploaded files will be sent to:

- imartinez@aclu-wa.org
- jmidgley@aclu-wa.org
- kmcruer@aclu-wa.org
- margaret.elofson@ci.tacoma.wa.us
- pleadings@aclu-wa.org

Comments:

Good morning, This is a re-filing of the Brief of Respondents and Appendix A and Appendix B filed yesterday. At the request of the Court, we have re-filed the Brief with the Appendices attached as one document.

Sender Name: Legal Assistant - Email: legalprogramassistant@aclu-wa.org
Filing on Behalf of: Lisa Nowlin - Email: lnowlin@aclu-wa.org (Alternate Email: pleadings@aclu-wa.org)

Address:
901 5th Avenue, Suite 630
Seattle, WA, 98164
Phone: (206) 624-2184

Note: The Filing Id is 20190214101740D2686803