IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR SKAGIT COUNTY, WASHINGTON

CITY OF SEDRO-WOOLLEY and CITY OF STANWOOD, Washington municipal corporations, Plaintiffs, vs. JOSE RODRIGUEZ, an individual, Defendant.	Case No. 25-2-00717-29 MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR DECLARATORY JUDGMENT

I. INTRODUCTION

Plaintiffs City of Stanwood and City of Sedro-Woolley (hereinafter the "Cities") submit this Memorandum in support of their Motion for Declaratory Judgment. The Cities respectfully request the Court issue a Declaratory Judgment that the data and images stored in the Flock AWS Cloud system are not public records unless and until a public agency accesses the particular data. In the alternative, if the Court finds that the data and images stored in the Flock AWS Cloud system *are* public records, Plaintiffs request the Court declare that data and images are categorically exempt from public disclosure under RCW 42.56.540, as disclosure is contrary to public policy. Furthermore, they are exempt under RCW 42.56.240, as they constitute specific intelligence information. For the reasons set forth in this Memorandum, Declaratory Judgment

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

consistent with the Cities' interpretation of public records case law is necessary to preserve individual privacy rights and protection of public safety, as well as to ensure efficient administration of other vital governmental functions.

II. FACTUAL SUMMARY

The Cities largely rely on the facts set out in their Complaint and shall reiterate facts here necessary to provide context and clarification to the arguments set forth below. Flock Safety's (or "Flock's") technology uses a combination of hardware and software to capture and analyze vehicle data. Their cameras (or cameras with their software installed), which are used by both law enforcement and private entities, capture multiple still images of every vehicle that enters their field of vision. This raw data is then processed by a proprietary and patented **artificial intelligence (AI)** model that uses a "neural network" to identify a vehicle's specific features, such as make, model, color(s), license plate number, and even bumper stickers or damage.

The following is a simplified breakdown of the process used by Flock Safety technology as described in their patent, No. US 11,030,892 B1:

1. **Image Capture:** Flock cameras continuously capture images of vehicles passing in their field of vision, capturing between 6-12 raw images of each vehicle.
2. **AI Analysis:** The raw images are immediately filtered and analyzed by Flock's AI software. The AI essentially "learns" to identify and categorize vehicle characteristics, creating a "Vehicle Fingerprint™."
3. **Data Storage:** The images are filtered, organized, and categorized, and are then encrypted and securely stored on Flock's cloud network. The raw images are discarded immediately.

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

4. **Permitted Use:** Only authorized users from customer organizations (law enforcement or private entities) can search and access the data. They must input a specific reason for any search, such as a case number or missing person report, ensuring the search is for a "Permitted Purpose."
5. **Auditing:** Flock maintains a log of all searches, including the user, date, time, and reason for the search. Customers can run audits to ensure their personnel are using the system appropriately and not for personal or improper reasons. This is a critical feature for preventing misuse.
6. **Data Deletion:** All images are automatically deleted from Flock's cloud system on a rolling 30-day basis. If a law enforcement agency needs data for an ongoing investigation, they must download it to their own secure systems before the 30-day period ends.

The Flock system simply modernizes the City's existing framework for intelligence gathering. It operates under the same strict governance as foundational law enforcement tools like the National Criminal Information Center (NCIC) and Criminal Justice Information Services (CJIS). Access to this sensitive data is locked down—only certified personnel with the requisite training, credentials, and a specific, legal basis for inquiry are permitted to utilize the system. This model guarantees accountability and limited use.

III. APPLICABLE LAW

A. RCW 42.56 – The Public Records Act.

The purpose of the Public Records Act ("PRA"), is "to provide [the public] full access to non-exempt public records." *Am. Civil Liberties Union of Wash. v. Blaine Sch. Dist. No. 503*

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

(ACLUI), 86 Wn.App. 688, 695, 937 P.2d 1179 (1997). The provisions of the PRA are to be liberally construed, and its exemptions are to be narrowly construed. *See*, RCW 42.56.030.

The PRA defines a "public record" as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." RCW 42.56.010(3). "Writing" is then further defined to mean:

> handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated.

RCW 42.56.010(4). The PRA does not define what it means for a record to be "relating to the conduct of government." Access to public records is a vital mechanism designed to foster accountability, trust, and transparency in government operations. However, not all data held by the government is considered a "public record." Certain sensitive information is not merely "exempt"; it is specifically categorized as outside the scope of public records altogether to create a crucial firewall. This hard boundary protects citizens by ensuring the government itself cannot access or compile information that is wholly irrelevant to its core, defined functions—thereby preventing potential misuse and reinforcing the principle of limited government authority.

B. WAC 44-14 – Public Records Act–Model Rules.

The Washington Administrative Code describes the three-part test to determine if a record is a "public record": "The document must be: [a] '**writing,**' containing information '**relating to the conduct of government'** or the performance of any governmental or proprietary function, '**prepared, owned, used, or retained'** by an agency." *See*, WAC 44-14-03001.

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

As to when a record relates to the conduct of government, the WAC provides:

> [a]lmost all records held by an agency relate to the conduct of government; however, some do not. A purely personal record having absolutely no relation to the conduct of government is not a 'public record.' *Even though a purely personal record might not be a 'public record,' a record of its existence might be if its existence was used for a governmental purpose*.

WAC 44-14-03001(2) (emphasis added). There is no further guidance regarding when a record relates to the conduct of the government.

C. Public Records Case Law.

Washington courts have held that "[a]ll three elements of [the above] three-prong test must be satisfied for a record to be a public record." *Dragonslayer v. State Gambling* Comm'n, 139 Wn.App. 433, 444, 161 P.3d 428 (2007) (overruled on other grounds). Therefore, "[t]he determination of whether a document is a 'public record' is critical for purposes of the [PRA]." *Oliver v. Harborview Med. Ctr,* 94 Wn.2d 559, 565, 618 P.2d 76 (1980).

When determining whether a record is a public record under the PRA, courts look at the three-part test described above, as well as looking at the content of the record and the "role the [record] play[s] in the [government] system." *Yacobellis v. City of Bellingham (Yacobellis I),* 55 Wn.App. 706, 711-12, 780 P.2d 272 (1989). The Court in *Yacobellis* found that courts "look[] at all the circumstances, such as whether the documents were in the agency's control, were generated within the agency, were placed into the agency's files and were used by the agency." *Id*.

Generally, when looking at all of the circumstances around a public records request, Washington courts interpret the PRA in a liberal manner that favors disclosure of records to the requester. However:

> when privacy is threatened, or in the rare occasions when a requestor has sought to misuse the law, courts have not hesitated to apply the law in a manner that protects rights and prevents abuses, because these goals are consistent with, not contrary to, the intent and spirit of the PRA.

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

See, Public Records Act Deskbook: Washington's Public Disclosure and Open Public Meetings Laws, § 2.2(3) (Wash. State Bar Assoc. 2d ed. 2014 & Supp. 2020). The PRA expressly recognizes that in certain circumstances, public disclosure is "clearly not be in the public interest" and can cause "irreparable harm" to public agencies and third parties. RCW 42.56.540. "The policy behind the [PRA] is to ensure 'full access to information concerning the conduct of government on every level' while remaining '[m]indful of the right of individuals to privacy.'" *Bellevue John Does v. Bellevue School Dist.*, 164 Wn.2d 199, 209, 189 P.3d 139 (2008) (quoting RCW 42.17A.001(11)[1]). When the PRA was enacted by initiative, the people "contemplate[d] some balancing of the public interest in disclosure against the public interest in the 'efficient administration of government.'" *Dawson v. Daily*, 120 Wn.2d 782, 798, 845 P.2d 995 (1993) (quoting RCW 42.17A.001(11)) (overruled on other grounds by *Progressive Animal Welfare Society v. Univ. of Wash.*, 125 Wn.2d 243, 261 n.7, 884 P.2d 592 (1994)).

D. Fourth Amendment Case Law Overview.

The Fourth Amendment prohibits unreasonable searches and seizures of "persons, houses, papers, and effects" and requires that warrants authorizing a search or seizure be based on probable cause and describe with particularity the place to be searched and the person or things to be seized. Supreme Court precedent is clear that the Fourth Amendment protects *people*, not places.

---

[1] RCW 42.17A.001 is a recodification of the initial intent section from the original Citizens' initiative that enacted both the provisions of the current Public Records Act in Title 42.56 RCW and the campaign finance disclosure laws in Title 42.17A RCW. See Laws of Wash. 1973 Ch.1, §1(11) (enacting Initiative Measure No. 276 (1972).

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

The Fourth Amendment is only implicated by government *action* that is a search or a seizure. Generally, observation of activities that take place entirely in public is *not* considered a search. However, in 2012, the Supreme Court held in *United States v. Jones* that planting a GPS device on a car and using it to track was a search. 132 S. Ct. 945, 181 L. Ed. 2d 911, 565 U.S. 400 (2012). While the *Jones* decision was decided narrowly based upon the trespass of a personal vehicle, the Supreme Court left open the door to the possibility that prolonged tracking via GPS could be considered a "search." The Court further addressed this issue in *Carpenter v. United States* in 2018 in the context of third-party data held by cell phone companies. 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). The Court held that "cell phone location information is not truly 'shared' as one normally understands the term because cell phones and the services they provide are indispensable to participation in modern society." The Court emphasized that while a cell phone customer "voluntarily" shares that information with their cell phone provider, the actual pervasiveness in our society and the dependence on cell phones for personal safety, employment, and social connection calls into question the "voluntariness" of the shared data. Justice Sotomayor expressed specific concern about the "aggregated" data that tracking devices allow. The Fourth Circuit has applied this reasoning stating that "prolonged tracking … invades the reasonable expectation of privacy that individuals have in the whole of their movements." *Leaders of A Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021). This is not unlike our modern-day society which compels participation in the public sphere for most, if not all, basic needs. The majority of people cannot survive without being seen in public on at least a semi-regular basis.

IV. ARGUMENT

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

The rapid pace of technological innovation consistently outstrips the development of legal frameworks, leaving laws and courts in a perpetual state of "catch up." This gap is particularly pronounced in the realm of public records cases where new technologies, like automated license plate readers (ALPRs), introduce complex legal questions and intersections of governmental transparency and constitutional rights. These technologies create a cross-section of public concerns—balancing privacy, public safety, and governmental transparency. Citizens worry about constant surveillance and the potential for a government that tracks their every movement, but law enforcement agencies advocate for these tools as essential "eyes and ears" to help solve crimes, expedite necessary caretaker functions, and ensure public safety. Utilization of aggregated data, either by the government or individuals, presents a serious invasion of privacy, even when that information is gathered initially in a public setting. Imagine an individual being able to request, and therefore track, the license plate "hits" of a judge, ex-partner, political rival, or even just a friend as a "prank." This is exactly the caution that the Court in *Carpenter* articulated when it found that even publicly gathered, or voluntarily given, data can result in an invasion of privacy and is therefore a *private* record.

A. The Public Records Act and ALPR Technology.

The Washington State Public Records Act (PRA), RCW 42.56, defines a public record as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." RCW 42.56.010(3). While the Cities concede that the images captured by ALPRs are "writings" under this definition, the central argument is that these images, at the moment of capture, do **not** meet the "relating to the conduct of government" or "performance of any governmental or proprietary function" requirement.

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

The images, in their raw form, are merely snapshots of vehicles in a public space. They contain no information related to a specific law enforcement investigation or governmental function. Instead, they are instantly filtered, tagged, and filed in a database. It is only when a law enforcement official actively queries the database for a specific purpose—such as searching for a stolen vehicle or a car associated with a suspect—that the image becomes "used" by the government in a way that relates to its governmental function. Therefore, the raw data stream from ALPRs to the online cloud system should not be considered a public record. These are the data and images requested by Defendant. The WAC itself identifies that a wholly private record "held" by an agency is only a public record if that private record *was used for a governmental purpose*. The images captured and filtered by Flock are never held by the government agencies *until* they are used for a governmental purpose.

There are few clear explanations of "information related to the conduct of government" or "related to a proprietary function." The Washington State Office of the Attorney General Open Government Resource Manual states that any record a government *has* meets this definition.[2] However, this definition is not helpful when a public agency does not have a record in its possession. When a public agency has a limited right to access records, is the record itself related to the conduct of government or only the contract that allows that right? For example, a requestor may not request all the driver's licenses that are registered within City limits. Law enforcement has a *right* to search the Department of Licensing database for that information if it is pertinent in an investigation or caretaking function, but not for a public records request. While this is not

---

[2] *See*, Washington State Office of the Attorney General, *Chapter 1*, Open Government Resource Manual, § 1.2 (accessed October 6, 2025), available at https://www.atg.wa.gov/Open-Government-Resource-Manual/Chapter-1

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

a perfect analogy because the Department of Licensing itself is a public agency, public records case law *does* care about the location and character of records when determining if a record is a public record that the agency subject to the litigation must provide. *See generally*, *Nissen v. Pierce County*, 183 Wash.2d 863, 357 P.3d 45 (2015) and *West v. Thurston County (West II)*, 168 Wn.App. 162, 183, 275 P.3d 1200 (2012) (holding that a "'writing' prepared by an agency's insurer-appointed lawyers is not automatically a public record under former RCW 42.56.010(2) if the agency never physically possessed the documents.")

The Merriam-Webster dictionary definition of "conduct" has different potential meanings: (1) the manner in which a person behaves; or (2) the action or manner of managing an activity or organization. The Cities do not dispute that the contract with Flock itself and any data obtained by City searches within the Flock system "contain information related to the conduct of government," however, the Cities maintain that the images or data logs captured by the Flock system do not contain any information that meet the above definition of "conduct." Vehicle images themselves do not relate to the "manner in which the [government] behaves." The *contract* with Flock identifying that the City has the right to access those images for "legitimate law enforcement purposes" is the only information related to the conduct of government. Similarly, vehicle images themselves do not contain information about the action or manner of managing an activity or organization. The search queries and search results contain that information after a City has utilized the system.

To contend that a government entity must request third-party records, records that have been substantially altered with patented third-party technology, is advocating for broader surveillance and less transparency than the technology is intended to provide. The Flock Safety system is a "query-based" system that operates in response to a user query. In an article from the

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

Annual Review of Criminology, Christopher Slobogin and Sarah Brayne identify this type of technology as likely an "evidence-only" technology. *See*, Christohpher Slobogin and Sarah Brayne, *Surveillance Technologies and Constitutional Law*, Annu. Rev. Criminol. December 08, 2023, at 10.

Similar to a drug sniffing dog that is wandering around an airport, unless an alert by the dog establishes probable cause to search a particular piece of luggage, the wandering around and gathering of information by the dog is not a search. Again, the Cities recognize this is an imperfect analogy since the dog and handler are presumably not creating "writings" as they pass by unalerted luggage, however, it is relevant to when the government action becomes "conduct" of government under a legal standard of the Fourth Amendment and therefore when a private record is used for a governmental purpose.

If a City were to access information from the Flock system without a legitimate law enforcement purpose, there very well could be Fourth Amendment implications as legal analysis and understanding continually play catch up to our technological advances. Under the contracts that limit access to the Flock system to legitimate law enforcement purposes, the Fourth Amendment is not implicated under current jurisprudence. To assert that the Flock data are public records requires one to conclude that the government is then required to participate in systematic and unchecked surveillance of any person that is in public. Since the Supreme Court is clear that the Fourth Amendment protects people and not places, this conclusion creates an absurd and illegal obligation on governments that attempt to utilize technology to provide public safety without significant inconvenience.

B. Public Policy and the PRA.

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

The PRA, though generally broad with narrowly defined exemptions, provides an avenue to prevent the release of records for reasons of public policy. This legal provision is perfectly suited for situations where technology has advanced more quickly than the legal system. The release of a vast trove of ALPR data could create a *de facto* public surveillance system. It could also reveal the patterns of police operations, such as where and when they are monitoring traffic, which could be exploited by those seeking to evade law enforcement. Allowing the release of this data could be abused by individuals or organizations to harass citizens, track individuals' movements for malicious purposes, and inhibit effective law enforcement by revealing operational details.

The judiciary can and should use the public policy exemption to prevent such abuse and protect sensitive information and government functions from unintended consequences of technological advancement.

C. Specific Intelligence Information.

While the PRA mandates broad disclosure of public records, the "PRA's mandate for broad disclosure is not absolute." *R.A.C. v. Seattle Housing Authority*, 177 Wn.2d 417, 432, 327 P.3d 600 (2013). "Public policy may sometimes require right to know to yield" to serve the public interest. *Soter v. Cowles Publ'g Co.,* 131 Wn. App. 882, 130 P.3d 840 (2006), aff'd, 162 Wn.2d 716, 174 P.3d 60 (2007). "Achieving an informed citizenry is a goal sometimes counterpoised against other important societal aims." *Servais v. Port of Bellingham*, 127 Wn.2d 820, 827, 904 P.2d 1124 (1995) (quoting *Spokane Police Guild v. Liquor Control Board*, 112 Wn.2d 30, 33-34, 769 P.2d 283 (1989)). The PRA itself is a "recogn[ition that] society's interest in an open government can conflict with its interests in protecting personal privacy rights and with the public need for preserving the confidentiality of criminal investigatory matters, among other concerns." *Servais*, 127 Wn.2d at 827 (quoting *Spokane Police Guild*); see also *Freedom*

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

Foundation v. Gregoire, 178 Wn.2d 686, 705, 310 P.3d 1252 (2013) (justifying recognize of implied constitutional exemption in part because "protecting the chief executive's access to candid advice" sometimes serves "the public interest"). Embodied in the PRA is "inherent clash" between these public interests. *Newman v. King County*, 133 Wn.2d 565, 572, 947 P.2d 712 (1997)

To effectuate these "countervailing" and sometime "conflicting" or "clashing" public interests, courts interpreting the PRA "must balance the interest of the citizens in knowing what their public officers are doing in the discharge of public duties against the interest of the general public in having the business of government carried on efficiently and without undue interference." *Dawson*, 120 Wn.2d at 798-99 (internal citation omitted).

"The legislature recognizes that public disclosure exemptions are enacted to meet objectives that are determined to be in the public interest." Laws of 2007, ch. 198 §1 (uncodified legislative finding). While courts have often noted that the disclosure mandate of the PRA should be liberally construed and exemptions should be narrowly construed, "[t]he general mandate that the [PRA] be liberally construed does not permit us to ignore the plain language of [a] specific public disclosure exemption." *BIAW v. Dep't of Labor & Indus.,* 123 Wn. App. 656, 666, 98 P.3d 537 (2004). "It is well-settled that we interpret statutes to avoid absurd results" and therefore courts should reject a narrow interpretation of an exemption when "[s]uch a narrow reading of [it] would ignore" the purpose of the exemption that the legislature intended. *N.W. Gas Ass'n v. W.U.T.C.,* 141 Wn. App. 98, 119, 168 P.3d 443 (2007); *see also*, *Haines-Marchel v. DOC*, 183 Wn. App. 655, 668-69, 334 P.3d 99 (2014) (rejecting an interpretation of the "intelligence information" exemption that "would risk shrinking the scope" of the exemption so it was "superfluous").

The "intelligence information" exemption in RCW 42.56.240(1) is an example of an exemption that serves the efficient administration of government and protects privacy. The

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

exemption expressly provides that the following information is exempt from disclosure: "Specific intelligence information … compiled by investigative, law enforcement, … the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy." RCW 42.56.240(1).

Specific intelligence information includes information about "particular methods or procedures for gathering or evaluating intelligence information." *Haines-Marchel*, 183 Wn. App. at 669. Courts have recognized that information about surveillance technology and the output of that technology qualify as "specific intelligence information." *See, e.g.*, *Fischer v. DOC*, 160 Wn. App. 722, 725-26, 254 P.3d 824 (2011) (footage from surveillance cameras); *Banks v. City of Tacoma*, 2021 WL 2229038 at *10 (Wn. App. June 2, 2021) (unpublished) (information about the make, model, and pricing regarding cell-site simulator).

To determine whether "nondisclosure … is essential to effective law enforcement," courts look at how disclosure would impact the effectiveness of the surveillance tool at issue. Nondisclosure is essential when disclosure could allow persons "to determine weaknesses and exploit those weaknesses," thus undermining the effectiveness of the surveillance tool. *Fischer*, 160 Wn. App. at 726-27; *see also*, *Banks*, supra, at *11 (nondisclosure of make/model/pricing information was essential to effective law enforcement because "criminals could combine information about the makes and models of Tacoma equipment with publicly available information about the capabilities of various cell site simulators to thwart their effectiveness and evade law enforcement detection").

When considering whether disclosure could interfere with effective law enforcement by undermining the effectiveness of the surveillance tool, the Court should take into account how the potentially exempt intelligence information could be used with other publicly available information. *Banks*, supra, at *10-*11 (when determining whether seemingly innocuous information about cell-site simulators is exempt, the court should consider how that information

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

could be combined with other publicly available information about the surveillance tool). Limited previous disclosure of similar information should therefore be weighed against additional disclosures and does not waive the application of the exemption to future requests. *Gaston v. DOC*, 2018 WL 3548391 (Wn. App. Apr. 5, 2018) (unpublished case) (exemption applied to request for specific prison surveillance video that had been shown during a criminal trial); *Fischer*, 160 Wn. App. at 726-26 (exemption applied to prison videos even though monitors showing those videos could be viewed by prisoners traveling to the prison library).

Applying this exemption, courts have held that surveillance videos used to monitor inmates were exempt as intelligence information because disclosure would allow inmates to determine the location and functionality of the cameras and then evade their coverage. *Fischer*, 160 Wn. App. at 827-28; *Gronquist v. DOC*, 177 Wn. App. 389, 399-01, 313 P.3d 416 (2013). Similarly, information about cell-site simulators that would allow persons to determine the functionality of those surveillance tools has also been held exempt under RCW 42.56.240(1). *Banks*, supra, at *11.

Here, the Flock Safety System and the data it produces qualifies as intelligence information because the Flock Safety System is a surveillance tool used by police departments to identify persons suspected of committing crimes. As in *Fischer* and *Gronquist*, nondisclosure of the data from the Flock Safety System is essential for effective law enforcement because disclosure of the data would reveal the location and functionality of the cameras. This data could be then aggregated and used to map those locations, which would then allow persons to evade the cameras by avoiding those locations.

Nondisclosure is also essential to protect people's rights to privacy. Law enforcement agencies are subject to strict requirements to ensure the Flock Safety System is not used for any improper purposes. It cannot be used for personal purposes. It cannot be used to aid in

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

immigration enforcement. It cannot be used to monitor persons engaged in First Amendment activities.

Persons making PRA requests would not be subject to any such limitations. See RCW 42.56.080(2) ("such [requestors] shall not be required to provide information as to the purpose for the request" subject to very narrow exceptions). If data from the Flock Safety System were subject to public disclosure, a person unhappy with the decision of a government official could use Flock data to track the daily movements of that official. Similarly, a disgruntled suiter could track a would-be paramour. Or a suspicious spouse could track a partner suspected of stepping out of the relationship. Nondisclosure is essential to prevent these (and infinite other possible) abuses.

V. CONCLUSION

For all the foregoing reasons, the Cities of Stanwood and Sedro-Woolley respectfully request the Court issue a Declaratory Judgment stating that the data and images held within the Flock AWS Cloud system are not public records under the Public Records Act (PRA) unless and until a City government accesses them.

This interpretation of the PRA is not only consistent with the language of the law, but also aligns with the principles of privacy and public safety. At the moment of their creation, the images and data captured by the Flock system do not meet the legal definition of a "public record" because they are not yet "prepared, owned, used, or retained" by a governmental entity in a manner that "relates to the conduct of government." Instead, they are raw, non-governmental data held by a third-party vendor.

A contrary ruling would impose an unconstitutional obligation on local governments, compelling them to become *de facto* public repositories of mass surveillance data on private citizens. Such an interpretation would not only violate the spirit of the Fourth Amendment, but

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119

would also create a significant risk of abuse, enabling the tracking and harassment of individuals by anyone with an interest in their movements. By limiting the scope of public records to only those data points that a City government has actively accessed for a legitimate, governmental purpose, the Court can uphold both governmental transparency and individual privacy rights, as well as ensure the efficient administration of vital government functions.

In the alternative, if the Court finds that the data and images stored in the Flock AWS Cloud system *are* public records, even when not accessed by a public agency for a law enforcement purpose, Plaintiffs request the Court declare that data and images are categorically exempt from public disclosure under RCW 42.56.540, as disclosure is contrary to public policy. Furthermore, they are exempt under RCW 42.56.240, as they constitute specific intelligence information.

DATED this 8th day of October, 2025.

THOMPSON, GUILDNER & ASSOCIATES, INC., P.S.

By _____
EMILY GUILDNER, WSBA No. 46515
NIKKI THOMPSON, WSBA No. 37884
Attorneys for Plaintiffs

THOMPSON, GUILDNER & ASSOCIATES, INC. P.S.
110 Cedar Avenue, Suite 102
Snohomish, WA 98290
360.568.3119