ROBERT M. SEINES (WSBA No. 16046)
Attorney at Law
P.O. Box 313
Liberty Lake, WA 99019
Phone: 509-844-3723
Fax: 509-255-6003
Email: rseines@msn.com

Hanni M. Fakhoury (admitted *pro hac vice*)
Jennifer Lynch (CA SBN 240701)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Fax: 415-436-9993
Email: hanni@eff.org

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA, Plaintiff, v. LEONEL MICHEL VARGAS, Defendant.	Case No.: 13-cr-06025-EFS **SUPPLEMENTAL BRIEF *AMICUS CURIAE* OF ELECTRONIC FRONTIER FOUNDATION IN RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING TAKING WITNESS TESTIMONY ON VIDEO SURVEILLANCE POLE CAMERA**

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

TABLE OF CONTENTS

I. INTRODUCTION 1

II. ARGUMENT 1

A. MORE DETAILS ABOUT THE CAMERA ARE RELEVANT TO RESOLVING THE FOURTH AMENDMENT ISSUE. 1

1. The Technical Details Are Needed to Determine Whether the Surveillance Camera Used by the Government is in "General Public Use." 1

2. The Technical Details of the Camera Allow the Court to Determine the "Actual" Surveillance that Took Place. 6

B. THE GOVERNMENT SHOULD BE REQUIRED TO DISCLOSE THE DETAILS OF THE CAMERA TO THE COURT AND MR. VARGAS. 10

1. Brady and Rule 16 Require Disclosure to Mr. Vargas 10

2. Because the Details of the Video Surveillance Are Already Known, the Law Enforcement Privilege Does Not Apply. 12

III. CONCLUSION 14

TABLE OF AUTHORITIES

Federal Cases

Albuquerque Publ'g Co. v. DOJ,
726 F. Supp. 851 (D.D.C. 1989) 13

Brady v. Maryland,
373 U.S. 83 (1963) 1, 10, 11, 12

Dow Chemical Co. v. United States,
476 U.S. 227 (1986) 2

Florida v. Harris,
133 S. Ct. 1050 (2013) 12

Florida v. Jardines,
133 S. Ct. 1409 (2013) 7

Giglio v. United States,
405 U.S. 150 (1972) 11

Joffe v. Google,
--- F.3d ----, 2013 WL 6905957 (9th Cir. 2013) 4

Kyllo v. United States,
533 U.S. 27 (2001) .... *passim*

Nat'l Sec. Archive v. FBI,
759 F. Supp. 872 (D.D.C. 1991) 13

Rosenfeld v. DOJ,
57 F.3d 803 (9th Cir. 1995) 13

Roviaro v. United States,
353 U.S. 53 (1957) 12, 13

Shafer v. City of Boulder,
896 F. Supp. 2d 915 (D. Nev. 2012) 5, 6

Silverman v. United States,
365 U.S. 505 (1961) 2

United States v. Ahrndt,
2013 WL 179326 (D. Or. Jan. 17, 2013) 4

United States v. Cedano–Arellano,
332 F.3d 568 (9th Cir. 2003) 11

United States v. Cortez–Rocha,
394 F.3d 1115 (9th Cir. 2005) 12

United States v. Gamez-Orduno,
235 F.3d 453 (9th Cir. 2000) 11

United States v. Green,
670 F.2d 1148 (D.C. Cir. 1981) 12

United States v. Guzman-Padilla,
573 F.3d 865 (9th Cir. 2009) 11

United States v. Jones,
132 S. Ct. 945 (2012) 8

United States v. Kyllo,
37 F.3d 526 (9th Cir. 1994) 9

United States v. Mandel,
914 F.2d 1215 (9th Cir. 1990) 11

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010) 8

United States v. Rigmaiden,
844 F.Supp.2d 982 (D. Ariz. 2012) 1

United States v. Stever,
603 F.3d 747 (9th Cir. 2010) 11

United States v. Strifler,
851 F. 2d 1197 (9th Cir. 1988) 11

United States v. Thomas,
726 F.3d 1086 (9th Cir. 2013) 11

United States v. Van Horn,
789 F.2d 1492 (11th Cir. 1986) 13

State Cases

Commonwealth v. Augustine,
--- N.E.3d ---, 467 Mass. 230 (Mass. 2014) 8, 9

State v. Earls,
70 A.3d 630 (N.J. 2013) 8, 9

Federal Statutes

5 U.S.C. § 552(b)(7)(E) 13, 14

Federal Rules

Federal Rule of Criminal Procedure 16 .... 1, 10, 11, 12

Constitutional Provisions

U.S. Const., amend. IV .... *passim*

U.S. Const., amend. V 11

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

INTRODUCTION

Understanding the specific technical capabilities of the surveillance equipment used by the government in this case is relevant to determining the ultimate issue before this Court: whether six weeks of continuous video surveillance of the constitutionally protected front yard of Mr. Vargas' home violated his reasonable expectation of privacy. These capabilities matter in order to allow the Court to determine whether the camera is in "general public use," as well as to understand the "actual" surveillance that took place.

The government's effort to have it both ways – to claim that the camera is both "in general public use" but that the details are subject to the law enforcement privilege – must fail. If the camera is in "general public use," then the law enforcement privilege does not apply and the details of the camera should be disclosed. But if the government wishes to claim the details of the camera are law enforcement privileged, then the camera necessarily is not "in general public use," making its warrantless use unconstitutional. The only way for the Court to make this determination – and the government to comply with its obligations under *Brady v. Maryland*, 373 U.S. 83 (1963) and Federal Rule of Criminal Procedure 16 – is to order the government to disclose the details of the camera to both the Court *and* Mr. Vargas.

ARGUMENT

A. MORE DETAILS ABOUT THE CAMERA ARE RELEVANT TO RESOLVING THE FOURTH AMENDMENT ISSUE.

1. The Technical Details Are Needed to Determine Whether the Surveillance Camera Used by the Government is in "General Public Use."

The technical details of the camera are important because the government has claimed that the camera at issue is in "general public use." *See* Government's Memorandum Regarding Taking Witness Testimony on Video Surveillance Pole

Camera, ("Gov. Testimony Brief"), ECF No. 80, at 6-7, Government's Supplemental Briefing on Defendant's Motion to Suppress Evidence From Video Surveillance Pole Camera ("Gov. Suppression Brief"), ECF No. 60 at 4-5. This phrase is relevant because the Supreme Court held in *Kyllo v. United States*, 533 U.S. 27 (2001) that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search" at least when the technology is "not in general public use." *Kyllo*, 533 U.S. at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)); *see also Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986) ("surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

The government has argued that the camera is "in general public use" and thus no "search" occurred under the Fourth Amendment. Gov. Suppression Brief at 4. It references commercial cameras available for a few hundred dollars and notes that Detective Clem testified that the camera was "commercially available." Gov. Testimony Brief at 12 (quoting Clem Testimony at 17-20).

But the only way to determine whether the camera is "in general public use" is to know about the camera's specific technical capabilities. The government notes the Supreme Court has stated, "Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations." *Dow Chemical*, 476 U.S. at 238 n. 5 (1986); Gov. Testimony Brief at 6. But by withholding the technical details of the camera, the government is also withholding the facts necessary to assess the Fourth Amendment issue.

The government compounds the problem by taking an inconsistent position about the camera. On the one hand, it claims it is "in general public use," similar to cameras that are available at electronic stores, and thus outside of *Kyllo* – making any further

inquiry into the technical details of the camera unnecessary. Gov. Suppression Brief at 4-5; Gov. Testimony Brief at 2, 7. On the other hand, it claims if the details of the camera must be disclosed, they are law enforcement sensitive and should only be given to the Court for *in camera* review. Gov. Testimony Brief at 7-13. But the government cannot have it both ways: if the camera is in "general public use," then there is no need to rely on the law enforcement privilege or *in camera* review because presumably, any member of the public is able to determine the details of the camera. If the camera is law enforcement sensitive, then it is by definition not "in general public use," *Kyllo* applies, and the surveillance is unconstitutional.

The only way to resolve this dispute then is by ordering the government to provide these details. Importantly, the only thing in the record to suggest the camera is in "general public use" is the government's bare assertion. The operation of the camera for six weeks, in addition to the government's claim that the technical details are law enforcement sensitive, undermine this assertion. And based on the details of the video surveillance already disclosed to this Court at the suppression hearing, the consumer cameras referenced by the government, such as a "Dropcam" or "Netcam" have primitive technical capabilities compared to the camera used by the government here. *See* Gov. Suppression Brief at 4.

First, these consumer cameras require a wireless Internet connection – usually connecting to a home's wireless Internet – in order to stream the surveillance footage.[1]

---

[1] *See* https://www.dropcam.com/ ("Keep an eye on your home or business from anywhere with Dropcam, the super simple way to monitor places, people and pets."); http://www.belkin.com/us/F7D7602-Belkin/p/P-F7D7602/ ("The camera connects to your home's Wi-Fi router and starts streaming video and audio to your smartphone or tablet. You don't even need a computer or laptop.")

If the pole camera required a wireless Internet connection in order to stream footage back to Detective Clem at the police station, it is necessary to determine which wireless connection was used. Did the camera connect to a wireless Internet signal from Mr. Vargas' home? From one of Mr. Vargas' neighbors? If so, did it log into an unsecured (non-password protected) network? Or did it break into a secured (password protected) network? These questions are not speculative, but crucial in determining the Fourth Amendment issues here because they suggest additional government misconduct. *See, e.g., United States v. Ahrndt,* 2013 WL 179326, *8 (D. Or. Jan. 17, 2013) (unpublished) (Fourth Amendment expectation of privacy in files shared over unsecured wireless network); *Joffe v. Google*, --- F.3d ----, 2013 WL 6905957 (9th Cir. 2013) (wireless network signals not "radio communications" and thus interception not exempt under Wiretap Act exception). And if this camera did not use a wireless Internet signal to relay the images to Detective Clem, then the question becomes, how did it broadcast its images? If the camera used a satellite, for example, then the device is clearly not in "general public use."

Another way these cameras likely differ is in zoom and pan capabilities. A "Dropcam Pro" for example has a 130-degree field of view and an 8x zoom,[2] and is clearly advertised as providing a way to monitor a particular room in a house.[3] Belkin explains its NetCam Wi-Fi Camera can "show[] you more of the room so you know

---

[2] *See* https://www.dropcam.com/product.

[3] *See, e.g.,* "Guard Your Gear," https://www.dropcam.com/home-security ("Whether it's a vintage toy collection or a closet of expensive film equipment, having a wireless security camera *in the room* provides additional peace-of-mind. A well-placed Dropcam is also a great way to scare off those with sneaky intentions.") (emphasis added).

what's really going on."[4] Meanwhile, the camera here could show details from 150 yards – 1½ football fields – away. *See* Gov. Testimony Brief at 4; Clem Testimony at 9. This sophisticated equipment is a far cry from these consumer cameras.

There are many more differences that can be determined simply by comparing the limited facts about with the website advertisements for these consumer cameras. The consumer cameras referenced by the government are clearly intended for indoor use.[5] They need to be plugged into an electrical wall outlet or through some sort of consumer grade rechargeable battery. The camera employed by the government here, however, obviously cannot be plugged into an electrical wall outlet because it is outside on a power pole. Perhaps it plugged directly into the power pole it was installed on, or used special industrial grade batteries to operate for an extended period of time. Presumably the government's camera is waterproof and able to withstand the elements, unlike the consumer cameras cited by the government. A Dropcam allows a user to store up to 30 days of footage.[6] But the surveillance here lasted six weeks, and Detective Clem testified he had no intended stop date in mind. Clem Testimony at 25.

Ultimately, all of these differences suggest that the camera used by the government is not in "general public use." As the district court in *Shafer v. City of Boulder*, 896 F. Supp. 2d 915 (D. Nev. 2012) noted, a "long-range, infrared, heavy-duty, waterproof, daytime/nighttime camera[]. . .undoubtedly contain[s] superior video-

---

[4] http://www.belkin.com/us/F7D7601-Belkin/p/P-F7D7601/.

[5] *See* "Technical Specs and Requirements," https://www.dropcam.com/product ("designed for indoor use").

[6] *See* "View it Later," https://www.dropcam.com/ ("Add our optional Cloud Recording service to save up to 30 days (720 hours) of continuous video. Review footage on your device and share favorite clips with family and friends.").

recording capabilities than a video camera purchased from a department store." *Shafer*, 896 F. Supp. 2d at 932. *Shafer* concluded such a camera is "not in general public use" under *Kyllo* and therefore using one for an extended period of time was a "search" that was "presumptively unreasonable without a warrant." *Id.* (citing *Kyllo*, 533 U.S. at 40).

Given all of these differences between the consumer cameras and the invasive camera used by the government here, this Court should find the camera used to monitor Mr. Vargas' home for six weeks is not in "general public use" and under *Kyllo*, the warrantless use of the device violated the Fourth Amendment. If the government wants to argue otherwise, it should be ordered to disclose on the record the details of the specific device here to show how it is substantially similar to ones available for consumers to purchase.[7] But it cannot argue that it is both in "general public use" and yet refuse to disclose its details. It can only be one or the other.

2. The Technical Details of the Camera Allow the Court to Determine the "Actual" Surveillance that Took Place.

The government also mischaracterizes the potential Fourth Amendment problem here. It emphasizes the Court should only look at how the camera was *actually* used, and not hypothetical invasions of privacy implicated by potential or unused capabilities of the camera. *See* Gov. Testimony Brief at 2, 4-6. It claims the only actual use of the

[7] Detective Clem's testimony that the camera used here was "commercially available" is true but irrelevant. Clem Testimony at 17. The camera was undoubtedly "commercially available" to law enforcement because presumably Detective Clem, the Kennewick Police Department or the FBI did not manufacture and assemble the camera, but bought it from a company that did. But there are many vendors who sell devices to law enforcement customers only, ensuring that those kinds of devices are not in "general public use."

camera was "the two-hour selection of [] surveillance that encompasses the incriminating photographs attached to and relied upon in the application for search warrant." Gov. Testimony Brief at 2; *see also* ECF No. 72. Thus, the government argues, simply reviewing that footage is enough to resolve the constitutional issue before the Court.

But that of course is incorrect; the actual output of the surveillance was the entire six weeks in which the government watched the constitutionally protected front yard of Mr. Vargas's home, not the government's cherry-picked two hours.[8] As Detective Clem testified, when he initiated the surveillance he did not have an end date in mind. In essence, he was waiting for Mr. Vargas to do something illegal before applying for a search warrant. It the entirety of the six weeks of prolonged surveillance – not simply a two hour portion of it – that is ultimately under constitutional attack.

Where the challenge to surveillance is to its duration and intensity – especially when the technology is not "in general public use" – then an understanding of the device's capabilities plays a role in deciding the issue. Otherwise, there is no way to determine whether Mr. Vargas constitutionally "exposed" his home to the specific type of surveillance the government aimed at him.

---

[8] The government notes the surveillance "did not result in any intrusion into any area of the interior of the Defendant's residence." Gov. Testimony Brief at 5. But that is irrelevant because as EFF explained in its initial amicus brief, the front yard of the home is clearly constitutionally protected curtilage. *See Florida v. Jardines*, 133 S. Ct. 1409, 1415 (2013); *see also* Brief *Amicus Curiae* of Electronic Frontier Foundation in Support of Defendant's Motion to Suppress Pole Camera Evidence ("EFF Amicus Brief"), ECF No. 59, at 3.

As EFF explained it its initial *amicus* brief, determining whether something is "exposed" to the public requires this Court to "ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do." *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010); *see* EFF Amicus Brief at 7-12. Relying on the concurring opinions in *United States v. Jones*, 132 S. Ct. 945 (2012), a number of courts looking at specific technologies have found constitutional problems because of the potential to reveal sensitive information, even if the particular case in which the evidence was used did not include those details. But those opinions looked at the technology at issue in detail in order to asses the constitutional issue.

Two recent cases concerning historical cell site records show how this is done. In *State v. Earls*, 70 A.3d 630 (N.J. 2013), the New Jersey Supreme Court ruled police needed a search warrant to obtain historical cell site records from a cell phone company because the information revealed "not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so." *Earls*, 70 A.3d at 642 (citing *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring)). The Massachusetts Supreme Judicial Court recently relied on this passage from *Earls* when it too required police to use a search warrant to obtain historical cell site records. *Commonwealth v. Augustine*, --- N.E.3d ---, 467 Mass. 230, 248 (Mass. 2014) (citing *Earls*, 70 A.3d at 642).

In neither *Earls* nor *Augustine* was there any suggestion that the police *actually* used the historical cell site records to create this detailed map of a person's movements. In *Earls*, the police used the information over a number of hours to locate the defendant. *Earls*, 70 A.3d at 633-34. In *Augustine*, police obtained two weeks worth of cell site data in order to pinpoint the defendant at the scene of the crime. *Augustine*, 467 Mass. at 233-34. Nonetheless, in assessing whether the defendants exposed their location to the public and thus surrendered their expectation of privacy, the courts necessarily had to

1 consider the capabilities of the technology, and not simply how the technology at issue
2 was specifically used against the defendant before the court. Thus, both opinions first
3 present lengthy technical descriptions of historical cell site data records before
4 considering the implications of the technology and ultimately deciding whether a search
5 warrant was required. *See Earls*, 70 A.3d at 636-38 ("For a better understanding of the
6 issues presented, we begin by examining how cell phones function."); *Augustine*, 467
7 Mass. at 236-37 ("A brief explanation of cellular telephone technology informs our
8 discussion of the issues raised").

9 Even *Kyllo* required judicial fact-finding about the technological capabilities of
10 the thermal imaging device. When the case was before the Ninth Circuit, the court
11 found that it did not have adequate facts to determine whether the use of the thermal
12 imaging device intruded upon Kyllo's expectation of privacy because the district court
13 "held no evidentiary hearing and made no findings regarding the technological
14 capabilities of the thermal imaging device used in this case." *United States v. Kyllo*, 37
15 F.3d 526, 530-31 (9th Cir. 1994); *see also Kyllo*, 533 U.S. at 30. The Ninth Circuit
16 explained that the Fourth Amendment "inquiry cannot be conducted in the abstract" and
17 that the court needed "some factual basis for gauging the intrusiveness of the thermal
18 imaging device, which depends on the quality and the degree of detail of information
19 that it can glean." *Kyllo*, 37 F.3d at 530-31. Thus, for the thermal imaging device, the
20 Court's "analysis will be affected by whether, on the one extreme, this device can detect
21 sexual activity in the bedroom, as Kyllo's expert suggests, or, at the other extreme,
22 whether it can only detect hot spots where heat is escaping from a structure." *Id.* But
23 without "explicit findings, we are ill-equipped to determine whether the use of the
24 thermal imaging device constituted a search within the meaning of the Fourth
25 Amendment." *Id.* It thus remanded to the district court to making "findings on the
26 technological *capacities* of the thermal imaging device used in this case." *Id.* (emphasis
27 added).
28

Before the Supreme Court, these specific technological capacities – and not just the way the technology was used against Kyllo – were crucial to the Court's holding that the use of a thermal imaging device to view the inside of the home was a "search" under the Fourth Amendment. It cautioned that although "the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. It noted some "devices may emit low levels of radiation that travel 'through-the-wall,' but others, such as more sophisticated thermal-imaging devices, are entirely passive, or 'off-the-wall" and that some thermal imaging devices "*might* disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath." *Id.* at 37, n. 3, 38 (emphasis added).

Thus, the specific technological capabilities of the video surveillance are relevant in determining the ultimate Fourth Amendment issue.

B. THE GOVERNMENT SHOULD BE REQUIRED TO DISCLOSE THE DETAILS OF THE CAMERA TO THE COURT AND MR. VARGAS.

1. ***Brady* and Rule 16 Require Disclosure to Mr. Vargas**

The government claims alternatively that if it must produce specific information about the camera, it should be permitted to do so through an *ex parte* submission to this Court because the information requested by Mr. Vargas would reveal "sensitive law enforcement information" not subject to disclosure. *See* Gov. Testimony Brief at 2; 7-12. But the government is wrong. As explained above, the camera cannot both be "in general public use" and yet so sensitive that its details cannot be disclosed publicly. Regardless of whether it is "in general public use" or not, the government's discovery obligations under *Brady* and Rule 16 of the Federal Rules of Criminal Procedure means it must disclose the technical details of the camera not simply to this Court, but to Mr. Vargas himself.

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

The Fifth Amendment to the U.S. Constitution's guarantee of due process requires the government to disclose to the defense any evidence "favorable to an accused" and "material either to guilt or to punishment." *Brady*, 373 U.S. at 87. Evidence is "material" if "there is a reasonable probability that its disclosure would have affected the outcome of the proceedings." *United States v. Guzman-Padilla*, 573 F.3d 865, 890 (9th Cir. 2009) (internal quotation marks, citation omitted). Federal Rule of Criminal Procedure 16 effectuates these constitutional rights by granting "criminal defendants a broad right to discovery," including the requirement that the government disclose "documents" or "data" in "the government's possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E)(i); *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010). *Brady*'s discovery obligations extend to facts relevant to raising Fourth Amendment challenges. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process"). And "Rule 16 permits discovery that is 'relevant to the development of a *possible* defense.'" *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added) (quotations omitted).

Brady also requires the disclosure of evidence that "bears on the credibility of a significant witness in the case." *United States v. Strifler*, 851 F. 2d 1197, 1201 (9th Cir. 1988); *see also Giglio v. United States*, 405 U.S. 150, 154 (1972). Disclosure obligations apply to information about the reliability of "witnesses" the government does not call at trial and that are not human, such as video surveillance. For example, the government must disclose records about a drug-detecting dog, including training and certification records and the "handler's log," in order to allow the defense to assess the dog's reliability and effectively cross-examine the handler at a suppression hearing. *United States v. Thomas*, 726 F.3d 1086, 1096 (9th Cir. 2013) (citing *United States v. Cedano–Arellano*, 332 F.3d 568, 570-71 (9th Cir. 2003)); *see also United States v.*

Cortez–Rocha, 394 F.3d 1115, 1118 n.1 (9th Cir. 2005) (disclosure of drug detecting dog evidence is "mandatory"). The U.S. Supreme Court explained last term that a criminal defendant must be able to challenge the reliability of a drug-detecting dog, noting specifically that the dog's performance in the field may be relevant, noting "circumstances surrounding a particular alert may undermine the case for probable cause" in some instances. *Florida v. Harris*, 133 S. Ct. 1050, 1057-58 (2013).

Under *Brady* and Rule 16 then, disclosure of the specific capabilities of this video camera is necessary. First, information that sheds light on the specific video equipment used by the government is material to a motion to suppress because, as explained above, these details are relevant to determining whether the technology used by the government is in "general public use" and to grasp the "actual" surveillance that took place. Second, the capabilities of the video surveillance will allow Mr. Vargas to assess and challenge the reliability of the surveillance. Just as information about a drug-detecting dog's performance is relevant to assessing the dog's credibility and its performance in the field for purposes of a suppression motion, the same is true of the specific technical capabilities of the video camera here.

2. Because the Details of the Video Surveillance Are Already Known, the Law Enforcement Privilege Does Not Apply.

The government claims it is permitted to skirt its discovery obligations because the information sought by Mr. Vargas is entitled to the "law enforcement privilege," which permits law enforcement to keep sensitive details about its investigation from a criminal defendant. Gov. Testimony Brief at 7-12. The Supreme Court recognized the privilege in *Roviaro v. United States*, 353 U.S. 53 (1957), which ruled the police can keep the identity of an informant secret. *See Roviaro*, 353 U.S. at 61-62. Other courts have extended the privilege to cover details about electronic surveillance. *See, e.g., United States v. Green*, 670 F.2d 1148, 1155 (D.C. Cir. 1981) (location of police

observation post subject to privilege); *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986) ("nature and location" of electronic surveillance equipment privileged).

But this privilege is "limited" and "sensitive law enforcement information must be disclosed if it is needed for an effective defense," including details about electronic surveillance. *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 988 (D. Ariz. 2012); *see also Van Horn*, 789 F.2d at 1508 ("The privilege will give way if the defendant can show need for the information."). While the Ninth Circuit has not established specific standards for when the privilege applies, it is clear it can cover information like the location where electronic surveillance is conducted because disclosure could "hamper future law enforcement efforts by enabling adversaries of law enforcement to evade detection." *Rigmaiden*, 844 F. Supp. 2d at 998. That is consistent with the rationale underlying *Roviaro*, where the Supreme Court worried that disclosing an informant's identity would deter others from reporting crime. *Roviaro*, 353 U.S. at 59.

But when these concerns are absent, the privilege should not apply. *See Roviaro*, 353 U.S. at 60 ("The scope of the privilege is limited by its underlying purpose . . . once the identity of the informer has been disclosed to those who would have cause to resent the communication, the privilege is no longer applicable."). For purposes of requests for law enforcement documents under the Freedom of Information Act, the Ninth Circuit has in fact noted that the exemption for disclosure of documents concerning law enforcement "techniques and procedures" only applies with resect to "investigative techniques not generally known to the public." *Rosenfeld v. DOJ*, 57 F.3d 803, 815 (9th Cir. 1995); *see* 5 U.S.C. § 552(b)(7)(E). Information about techniques or procedures that "would leap to the mind of the most simpleminded investigator" are not privileged. *Rosenfeld*, 57 F.3d at 815 (citing *Nat'l Sec. Archive v. FBI*, 759 F. Supp. 872, 885 (D.D.C. 1991)); *see also Albuquerque Publ'g Co. v. DOJ*, 726 F. Supp. 851, 857-58 (D.D.C. 1989) (ordering disclosure of records "pertaining to techniques that are commonly described or depicted in movies, popular novels, stories or magazines, or on

1 television," including "eavesdropping, wiretapping, and surreptitious tape recording and
2 photographing.").

3 Here, there is nothing to keep privileged as revealing the specific technical
4 capabilities of the camera would not hamper law enforcement's ability to investigate
5 crime, nor create a reasonable risk of future circumvention of the law. *See* 5 U.S.C.
6 § 552(b)(7)(E). The technique – video surveillance – is well known to the general public.
7 Further, this request is not for other locations of pole cameras in use by the FBI or the
8 Kennewick police department generally,[9] but only for more details about the specific
9 camera used in Mr. Vargas' case. Unlike revealing the location or placement of other
10 cameras, disclosing this camera's technical details would not allow future criminal
11 suspects to evade surveillance; those suspects will continue to go about their lives.

12 Since these details are not privileged, they should be disclosed to Mr. Vargas.

13 **CONCLUSION**

14 For these reasons, the government should be ordered to disclose the technical
15 details of the camera to this Court and Mr. Vargas.

16

17 Dated: March 31, 2014 Respectfully submitted,

18

19 */s/ Robert M. Seines*
ROBERT M. SEINES
20 Attorney at Law
P.O. Box 313
21 Liberty Lake, WA 99019
Phone: 509-844-3723
22 Email: rseines@msn.com

23

24

25 [9] Detective Clem already testified about the specific location where the pole camera was
26 installed and the parts of Mr. Vargas' home he was watching. *See* Clem Testimony at 5-
27 7. Presumably, no one is going to Mr. Vargas' home now, especially because he is
28 incarcerated.

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

/s/ Hanni M. Fakhoury
Hanni M. Fakhoury
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Email: hanni@eff.org

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the Eastern District of Washington by using the appellate CM/ECF system on March 31, 2014. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: March 31, 2014

Respectfully submitted,

/s/ Robert M. Seines
ROBERT M. SEINES
Attorney at Law
P.O. Box 313
Liberty Lake, WA 99019
Phone: 509-844-3723
Email: rseines@msn.com

/s/ Hanni M. Fakhoury
Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
Email: hanni@eff.org

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION