UNITED STATES DISTRICT COURT EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,

Plaintiff,

VS.

LEONEL MICHEL VARGAS,

Defendant

Case No.: CR-13-6025-EFS

Defendant's Reply Memorandum Regarding Privilege

(509)586-3091

The government claims a privilege to keep secret the "technology" of the surveillance system used here without a warrant. The government claims the actual method for surveillance and concealment is irrelevant to the Fourth Amendment inquiry, and that the secret capability of the technology is worthy of protection.

SUMMARY OF ARGUMENT

Any unreasonable search is unconstitutional. The manner and means of any search, including the nature of the technology employed, is relevant and admissible for the court's consideration of whether the government conducted itself reasonably. The defendant asserts that how the government conducts surveillance is always an appropriate consideration when evaluating constitutional limitations. The capabilities of the technology employed here is directly relevant to the court's consideration both of the DEFENDANT'S REPLY MEMORANDUM-1

JOHN S. MATHESON, ESQ. 315 W. KENNEWICK, AVE. KENNEWICK, WA 99336

1 2 3

4 5

DEFENDANT'S REPLY MEMORANDUM- 2

intensity of the intrusion and the necessity for prior judicial consideration. The defendant asserts that any unrestricted continuous video recorded surveillance of a home and curtilage by police, especially when recording indefinitely, with remote control of pan and zoom, requires both disclosure of the technical capabilities and requires a warrant with judicial oversight and limitation prior to placement.

Argument

The government would extend the limited privilege under Roviaro v. United States, 353 U.S. 53, 59, 77 S.Ct. 623, 627, 1 L.Ed. 2d 639 (1957), which grants a limited privelege to withhold the identity of confidential informants. The government claims the two part balancing test in Roviaro supports the government. This argument misses the mark. Roviaro doesn't support the government's position. In this case, the government has no interest in protecting the safety of an informant or the flow of information from an informant to the government, the reasons for the Roviaro limited privilege. Since the reasons for the rule do not apply, the privilege (and the balancing test) do not support the claimed privilege in this case. Id. at 62, 77 S.Ct. at 628-29.

The government also relies upon the privilege to withhold the secret observation post in <u>US v. Green</u>, 670 F.2d 1148 (1981) and the secret undercover car, <u>In re the City of New York</u>, 607 F.3d 923 (2nd Cir. 2010). Here there is no specific secret observation post to protect nor an undercover car to protect for future use by law enforcement. The location of this or any pole camera is NOT a secret vantage point. There are available poles in almost every location. This (and the traditional pole camera) are disguised to give no clue to targets that a camera is operating. Neither <u>U.S. v. Roviaro</u>, nor its

DEFENDANT'S REPLY MEMORANDUM- 3

proginy support withholding the capabilities of the subject technology. The capability of the technology here should not be secret simply because law enforcement wants it so. There is no specific information which "destroys their present utility, compromises their present utility, compromises their future use, and potentially endangers law enforcement officers who seek to employ them." Governments Reply, Doc. 99, page4. This court, this defendant and the public have the right and the need to know the secret capability to assess the appropriateness of this warrantless surveillance.

The right to privacy is impacted by any search. In <u>Johnson v. United States</u>, 333 US 10, 13-14, 68 S. Ct. 367 (1948), the court states:

The point of the Fourth Amendment... is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers...When the right to privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. (Footnotes omitted).

The technical capability of the technology employed by the government is relevant for the court to determine whether (1) the surveillance intruded on a protected space, like a home and curtilage; (2) did the surveillance last so long that it created a picture of the person's life; and (3) does it feel "creepy and un-American?". See *Beyond Jones*: Electronic Surveillance and the Fourth Amendment; AFPD Lisa Hay, District of

Oregon, June 2012. Hay cites <u>US v. Maynard</u>, 615 F. 3d 544 (D.C. Cir. 2010), aff'd sub. nom, <u>US v. Jones</u>, 132 S. Ct. 945 (2011), and Judge Kozinski's eloquent dissent from denial of rehearing en bank, <u>US v. Pineda-Moreno</u>, 617 F.3d 1120 (9th Cir. 2010), cert. granted, judgment vacated, 132 S. Ct. 1533 (February 21, 2012).

Judge Kozinski criticizes the panel for allowing installation of GPS tracking devices under cars parked in driveways of homes. He notes that access to growing databases and prolonged surveillance (by GPS tracking device) reveals types of cumulative information not revealed by short-term surveillance, a permanent electronic record "to deduce all manner of private information about individuals." Id. at 1124-26.

At 617 F.3d 1124 -1125 he states:

The Supreme Court has recognized that advances in "police technology [can] erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). To guard against this, courts "must take the long view, from the original meaning of the Fourth Amendment forward." *Id.* at 40, 121 S.Ct. 2038. *Kyllo* followed a line of cases going back to *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), *Katz*, 389 U.S. at 353, 88 S. Ct. 507, and *Silverman v. United States*, 365 U.S. 505, 512, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961), which stemmed the erosion of personal privacy wrought by technological advances.

In *Kyllo*, the Court held that use of a thermal imager to detect the heat emanating from defendant's home was a search for purposes of the Fourth Amendment because the then-new technology enabled police to detect what was going on inside the home-activities the homeowner was entitled to consider private. Any other conclusion, the Court noted, "would leave the homeowner at the mercy of advancing technology-including imaging technology that could discern all human activity in the home." *Kyllo*, 533 U.S. at 35-36, 121 S.Ct. 2038 (citing *Karo*, 468 U.S. at 705, 104 S.Ct. 3296). "While the technology used in the present case was relatively crude," the Court continued, "the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Id.* at 36,

121 S.Ct. 2038. In determining whether the tracking devices used in Pineda-Moreno's case violate the Fourth Amendment's guarantee of personal privacy, we may not shut our eyes to the fact that they are just advance ripples to a tidal wave of technological assaults on our privacy.

At 1126

But there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention....Most targets won't know they need to disguise their movements or turn off their cellphones because they will have no reason to suspect that Big Brother is watching them.

The Supreme Court in *Knotts* expressly left open whether "twenty-four hour surveillance of any citizen of this country" by means of "dragnet-type law enforcement practices" violates the Fourth Amendment's guarantee of personal privacy. 460 U.S. at 283-84, 103 S.Ct. 1081.

I don't think that most people in the United States would agree with the panel that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something creepy and un American about such clandestine and unheralded behavior. To those of us who have lived under a totalitarian regime, there is an eery feeling of de'ja' vu. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourself and our children may be dire and irreversible. Some day, soon, we may wake up and find we are living in Oceania.

Privacy and advancements in the technology of cell phones were recently considered by the Supreme Court in <u>Riley v. California</u>, slip opinion No. 1-32, decided June 25, 2014, 573 U.S. ____ (2014). The Court held that police generally may not search digital information on a cell phone seized from an individual who has been arrested under the search incident to arrest exception.

DEFENDANT'S REPLY MEMORANDUM- 6

Like infrared or cell phone technology, advancements in the technology of digital photography require this court to consider the technical capability of the subject pole camera. Kyllo v. US, 533 US 27, 34 (2001) acknowledges the need to protect privacy from advancing infrared technology. It is apparent that capabilities of the subject "camera" far exceed the traditional pole cam, including the ability to operate and record continuously and indefinitely, and to (at least) remotely control pan and zoom from the police station, which permit far more intense surveillance. United States v. Cuevas-Sanchez, 821 F.2d 248, 5th Cir. 1987 (video surveillance of home constituted a search and a warrant is required. The continuous intense surveillance captures a picture of the person's life in a digital recording which intensifies the intrusion.

Defendant acknowledges that traditional analysis would deny that a reasonable expectation of privacy exists here because (the government asserts) the camera was (is) incapable of viewing inside the house and could only observe those things any passerby could easily observe. <u>US v. Jackson</u>, 213 F.3d 1269 (10th Cir. 2000). <u>US v. Vankesteren</u>, 553 F.3d 286 (4th Cir. 2009) (camera installed to record open fields does not implicate Fourth Amendment). <u>US v. McIver</u>, 186 F.3d 1119 (9th Cir. 1999) (warrant not required if the defendant did not have a reasonable expectation of privacy in a public area). These cases do not address surveillance of the curtilage of this intensity undertaken for a police investigation without a warrant. The technical capability of this equipment bears directly on the intensity of the surveillance and the reasonableness of police actions.

Police targeted the house and curtilage (for a month of continuous 24 hours a day digital video recording with off site manipulation of pan and zoom) until a status crime, possession of a firearm by an undocumented alien, was detected which led to the subject search warrant. Had the defendant not chosen to target practice when he did, how much longer would the surveillance have continued? This secret long term spying undertaken in the unfettered discretion of the officers, without prior judicial consideration of its propriety, falls within the "dragnet- type" invasive clandestine law enforcement practices of "Big Brother" and is akin to the general warrant at the heart of protection afforded under the Fourth Amendment guarantee of personal privacy. The government's claim to keep it's technology secret compounds the fact that the known capability of this surveillance equipment has that "Oceania" feeling, something "creepy and un-American".

As noted in Riley at 27-28, 573 U.S. ____(2014):

Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.

And at 28 concludes:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." *Boyd, supra*, at 630. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple--get a warrant.

DEFENDANT'S REPLY MEMORANDUM-8

CONCLUSION

Here, disclosure of the technical capability of the surveillance technology employed here is critical to a consideration of the intensiveness and invasiveness of the search and its propriety. If agents want to employ this "dragnet-type" surveillance technology directed at an individual's home and curtilage, they should "get a warrant." What other or further unknown capability does this equipment provide to the police in their unfettered rummaging? Whether or how it is or may be connected to the ever growing governmental data collection increases the intensity of the search and the necessity for both disclosure and for judicial oversight.

DATED this 14th day of August, 2014.

s/John S. Matheson JOHN S. MATHESON, WSBA No. 8288 Attorney for Defendant

DEFENDANT'S REPLY MEMORANDUM- 9

CERTIFICATE OF SERVICE

I hereby certify that on August 14, 2014, I electronically filed the foregoing with the Clerk of the Court using the CM/EDF System which will send notification of such filing to the following: Alex Ekstrom, Assistant United States Attorney

s/John S. Matheson John S. Matheson, WSBA No. 8288 Attorney for Defendant