Rosalind M. Lee (OSB 055566)
Rosalind Manson Lee, LLC
474 Willamette St., Ste 302
Eugene, OR 97401
Tel: (541) 485-5110
Fax: (541) 485-5111
ros@mansonlee.com

Of Attorneys for Defendant
RANDALL DE WITT SIMONS

IN THE CIRCUIT COURT OF THE STATE OF OREGON

LANE COUNTY

STATE OF OREGON, Plaintiff, vs. RANDALL DE WITT SIMONS, Defendant.	Case No. 19CR43543 REPLY TO STATE'S RESPONSE TO DEFENDANT'S MOTION TO CONTROVERT AND SUPPRESS Oral Argument and Evidentiary Hearing Requested Time: Approximately 4 Hours

I.

A&W's Actions were Those of the State and Subject to the Restrictions of Article 1, section 9 of the Oregon Constitution, because Someone at A&W Configured A&W's Firewall to Seize all Internet Traffic from IanAnderson-PC for 11 Months, and Configured A&W's Firewall Software to Send Alerts to Oakridge Police Officer Larsen.

The state argues that A&W employees "acted on their own" when they reported to law enforcement evidence on their server of searches for child pornography. State's Response to Defendant's Motion to Controvert and Suppress at 3, 4 (hereinafter "State's Response.") A&W employees did more than report contraband found on the server, which they did in July of 2018,

almost one year before the search warrant in this case. Someone configured the A&W firewall to automatically notify the police when any device using the A&W WiFi connected to a website containing suspected child pornography. Someone, at the behest of the police, also collected all of the internet browsing history of IanAnderson-PC and provided it to the police. Indeed, Detective Weaver testified at the grand jury in this case that "they [the A&W server] were *keeping track for us* of every website he was going to." Defendant's Motion to Controvert and Suppress Exhibit B at 6 (emphasis added). When A&W was downloading the browsing history for IanAnderson-PC, they were working at the behest of the police.

II.

Mr. Simons has a Privacy Interest in his Web Browsing History.

The Oregon Supreme Court recognizes that data contained in computers is different than other personal property, and that article 1, section 9 of the Oregon Constitutions protects that data from unreasonable searches and seizures. In *State v. Mansor*, 363 Or 185 (2018) the Oregon Supreme Court considered, *inter alia*, whether a warrant to search a computer for the defendant's internet browsing history on a single day allowed the police to search the computer for all of the defendant's internet browsing history. Relying on *State v. Munro*, 399 Or 545 (2005), the state argued that because the computer was in the lawful possession of the police at the time they searched the browsing history, the defendant no longer had a privacy interest in its contents. *Mansor*, *supra*, 363 Or at 209. The court rejected that argument, distinguishing the contents of a computer from the videotape seized by the police in *Munro*, because of the nature of contents of a computer, including a person's internet browsing history. *Id*. at 210. The court in *Mansor* held that the police exceeded the scope of the warrant by searching for internet history on days other than the one specified in the warrant. *Id*. at 221.

Mansor stands for the proposition that even if the police have lawful possession of a computer that contains internet browsing history, the police cannot search that computer for internet

browsing history without a warrant supported by probable cause that specifies the scope of the search. Notably, the court in *Mansor* recognized the particular privacy interest in data contained in electronic devices affirmed by the United States Supreme Court in *Riley v. California*, 573 US 373 (2014).[1]

Here, the police were seizing internet browsing history without a warrant and without probable cause. The A&W "server" is akin to the lawfully-obtained computer like the one in *Mansor*. The police cannot seize the internet browsing history of a particular person without a warrant supported by probable cause.

In addition, under the Fourth Amendment, law enforcement may not obtain electronic data about a person's location collected by way of the person's cell phone signal, and retained by a third party without a warrant. *See Carpenter v. United States*, 138 SCt 2206 (2018). If we assume for the sake of argument that A&W was collecting all of the web browsing history of a specific computer for close to one year in the ordinary course of business—just like the third party in *Carpenter*—and the police had nothing to do with A&W's collection of that evidence, then the rule in *Carpenter* applies. The police needed a warrant before seizing the web browsing history from A&W.

The police obtained months of web browsing history—the majority of which contained entirely legal content—from a third party without a warrant. *See* Declaration of Counsel in Support of Defendant's Motion to Suppress and Controvert at 2. Although the data in this case is of a different type than that obtained in *Carpenter*, the intrusion into Mr. Simons's privacy is of a similar nature. The government's warrantless seizure of 11 months of internet activity violated Mr. Simons's reasonable expectation of privacy. It is this type of intrusion into a person's privacy that the Supreme Court prohibited in *Carpenter*.

//

//

[1] In *Riley* the United States Supreme Court held that a cell phone may not be searched incident to arrest. *Riley v. California*, 573 US 373, 386 (2014).

III.

Using Technology to Search Mr. Simons's Home for a Specific Computer Required either a Court Order under ORS 133.721 or 18 U.S.C. § 2518 or a Search Warrant.

The state makes three arguments regarding the detective's use of the packet sniffer to locate IanAnderson-PC: first, that use of the packet sniffer does not violate the Oregon Wiretapping statute; State's Response at 6; second, that even if the use of the packet sniffer violated that statute, it is not subject to suppression; *Id*. at 7; and third, that using the packet sniffer violated no privacy interest, because the WiFi signal from the computer in Mr. Simons's home exceeded the curtilage of his property. *Id*. at 6, 8. Each argument is addressed separately below.

A. The State Misconstrues State Wiretapping Law

The state argues that Det. Weaver's use of the packet sniffer does not violate the Oregon wiretapping statute, because the packet sniffer "does not intercept content of communication" within the meaning of ORS 133.721(2) and (5). State's Response at 6. The Oregon wiretap statute defines "contents" as "any information concerning the identity of the parties to such communication *or the existence*, substance, proport or meaning of that communication." ORS 133.721(2)(emphasis added.) Using the packet sniffer, Det. Weaver confirmed the existence of a communication between the A&W WiFi router and IanAnderson-PC. In addition, when using the packet sniffer, Det. Weaver determined that IanAnderson-PC was viewing a website with suspected child pornography. Motion to Controvert and Suppress, Exhibit B at 7:22-25. In so doing, Det. Weaver intercepted the content of the signal between IanAnderson-PC and the wireless router.

The state also argues that because the police did not listen to or record the communication between the computer and the router, the wiretap statute does not apply. State's Response at 6. A packet sniffer collects and displays packets in transit. Kismet, the software used by Det. Weaver, displayed a view of signal strength and packet rate among other information about the electronic communication between IanAnderson-PC and the WiFi router. The information about this

electronic communication was recorded by the detective when he took what appears to be screen shots of the packet sniffer software as it was searching for IanAnderson-PC. *See* Discovery at 000074-75.

In addition, in order to function properly the software records the electronic communications and displays them on the computer screen. The software does not act like a telescope: the user is not looking at magnified images of the packets of data that make up the electronic communication between the computer and the router. The communications are recorded, processed, and analyzed by the software and presented to the user in the form of graphs and other data. Detective Weaver recorded electronic communications when he used the Kismet software to search for IanAnderson-PC.

The state further argues that items seized in violation of a statute are not subject to suppression "unless the legislature has created an express exclusionary remedy for a statutory violation." State's Response at 6-7 *quoting State v. Silbernagel*, 229 Or App 688, 690-91 (2009). Oregon's wiretapping statute has an express exclusionary remedy for a statutory violation. ORS 133.735, which is titled "Suppression of intercepted communications; procedure; grounds; appeal" specifically requires suppression of information unlawfully seized under ORS 133.724. The statute particularly requires that if the motion to suppress evidence seized in violation of the wiretapping statute is granted, then "the contents of the intercepted wire, electronic or oral communication, *or evidence derived therefrom*, shall be treated as having been unlawfully obtained." ORS 133.735(c)(2) (emphasis added.)

In its response, the state does not address the defense argument that in using the packet sniffer, Det. Weaver violated the federal wiretapping statutes. Rather than restating the Title III arguments here, the defense respectfully refers the Court to Defendant's Motion to Controvert and Suppress at 10-11.

//

//

B. Mr. Simons has a Constitutionally-Protected Interest in the Contents of his Home, Even if Items in his Home Emit Invisible Signals that Exceed the Curtilage of his Home

The state argues that Mr. Simons has no privacy interest in the wireless signal coming from a computer in his home, because it emanated outside of the curtilage of his home. State's Motion at 6. Both the Oregon and United States Constitutions protect individuals from warrantless searches of their homes by tracking invisible signals—even those that can be detected from outside of a constitutionally-protected space.

1. *Article 1, section 9.*

Article 1, section 9 of the Oregon Constitution recognizes privacy interests outside the curtilage of one's home. For example, placing a radio transmitter on a person's car and tracking the car's movements in public is a search under article 1, section 9. *State v. Campbell*, 306 Or 157 (1998). While unaided observations from public places are not searches, use of technology in making observations can constitute searches when "the practice, if engaged in wholly at the discretion of the government will significantly impair 'the people's' freedom from scrutiny. *Id*. at 170.

The detective used the packet sniffer to look for a particular item in Mr. Simons's home. The detective did not have a warrant to search the house, and could not see into the house, unaided, from a lawful vantage point. The detective used specialized technology to look inside the house. Using packet sniffers without any judicial oversight through the use of a warrant or a wiretapping order will significantly impair our freedom from scrutiny, because the police will be able to look into anyone's home at any time for internet connected devices, and download payload data, or merely inventory electronic devices in the residence. The WiFi signal from a device present in a home that is connected to a router also located in the home is detectable with a packet sniffer. *See generally Joffe v. Google, Inc*. 746 F3d 920, 923 (9th Cir. 2013) *cert. denied Google v. Joffe*, 573 US 947 (2014)(describing how Google downloaded payload data from residential WiFi networks using a

packet sniffer.) One cannot use WiFi without having the signal broadcast from the curtilage of one's home.

2. *Fourth Amendment*

In 1967, the Supreme Court held that the Fourth Amendment protects "people" and not simply "places"—against unreasonable searches and seizures." *Katz v. United States*, 389 US 347, 351 (1967). This includes "surveillance . . . without any 'technical trespass under local property law.'" *Id.* at 353. According to *Katz* and the more than fifty years of Supreme Court precedent that have followed it, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" so long as there is a "reasonable expectation of privacy." *Carpenter*, *supra*, at 2217 *citing Katz*, at 351-52) (alteration in original); *see* Defendant's Motion to Suppress and Controvert at 19-23 (arguing that Mr. Simons has a reasonable expectation of privacy in his internet communications).

The state's response ignores *Katz* and its progeny, arguing that Mr. Simons has no "personal privacy right" when connecting to the internet "beyond his constitutionally protected curtilage." State's Response at 4, 6. The state's argument is the very one that *Katz* rejected in holding that eavesdropping on a telephone conversation made from a public telephone booth was a Fourth Amendment search, despite the fact that no physical trespass occurred. *See Katz*, *supra*, at 389. Even though the defendant in *Katz* was using a public payphone, he had closed the telephone booth door behind him in an effort to exclude the "uninvited ear" and preserve the privacy of his conversation. *Id.* at 352. Thus, when the government listened in on that conversation using a recording device attached to the outside of the booth, they violated the privacy "upon which he justifiably relied." *Id.* at 353. It made no difference that the phone conversation was being transmitted through wires that went beyond the four walls of the booth. Following *Katz*, it is the expectation of privacy that matters.

Consequently, the Supreme Court has repeatedly held that law enforcement engages in a search when they use new technology to learn information about activities inside a home, even when they commit no trespass and are positioned well outside the curtilage. In *United States v. Karo*, for

example, the Court considered the use of an electronic tracking beeper hidden inside a drum of chemicals, which police used to determine whether the drum was inside a residence or had been transported elsewhere. *See United States v. Karo*, 468 US 706, 709-10 (1984). The Court held that a Fourth Amendment search had occurred, despite the absence of a physical trespass involving the residence or its curtilage. *Id.* at 716. The Court reasoned that, "We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time." *Id*.

Finally, in *Kyllo v. United States*, the Court examined police use of a thermal-imaging device to determine, from a distance, whether a particular home was operating grow lights indicative of marijuana production. *See Kyllo v. United States*, 533 US 27, 29-30 (2001). Once again, the Court found that a Fourth Amendment search had occurred even though the government had committed no physical trespass. *See id.* at 32-33. The Court held 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 where (as here) the technology in question is not in general public use." *Id.* at 34 (citations and internal quotations omitted.) Such a rule is necessary when new technology upsets expectations of privacy, the Court explained, in order to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.*

Legislative protections for electronic communications also recognize the need to protect information in transit. The whole point of the telephone, of course, was to be able to communicate with individuals located outside of one's home. Legislatures therefore recognized the need to protect the privacy of these communications. One year after *Katz*, for example, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (*i.e.*, the "Wiretap Act"), Pub. L. 90-351, 82 Stat 212 (1968), which specifically prohibited obtaining wire communications contemporaneous

with transmission *See Konop v. Hawaiian Airlines, Inc.*, 302 F3d 868, 878 (9th Cir. 2002). Again in 1986, Congress passed the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986), to include protections for electronic communications while they are being made, are in transit, and stored on computers.

In this case, law enforcement used new technology—the packet sniffer—to gain information about the inside of Mr. Simons's home that they did not and could not have learned from visual surveillance alone. As in *Karo*, "there is no gainsaying that the [packet sniffer] was used to locate the [computer] in a specific house..., and that that information was in turn used to secure a warrant for the search of the house." *Karo*, *supra*, at 714. Under *Katz*, *Karo,* and *Kyllo*, the relevant question is whether Mr. Simons had an expectation of privacy in his WiFi traffic and internet communications, not whether those signals crossed his property line. The state does not acknowledge this binding case law, but instead seeks to revive an argument that has been thoroughly and repeatedly rejected. This Court should likewise reject such a mechanical interpretation of the Fourth Amendment and not "leave the homeowner at the mercy of advancing technology." *Kyllo*, 533 US at 35-36.

IV.
The Doctrine of Inevitable Discovery Does Not Purge the Taint of the Officer's Illegal Seizure of the Computer Known as IanAnderson-PC.

The state argues that even if the application for the warrant in this case had been denied "based on the inclusion of the Kismet software," police would have been able, through lawful police procedures, to connect Mr. Simons to his residence and show that he downloaded child pornography, and obtain a search warrant with that information. State's Response at 11-12.

Under Oregon law, if the state obtains evidence seized in violation of article 1, section 9 of the Constitution, "it is presumed that the evidence was tainted by the violation and must be suppressed." *State v. Miller*, 267 Or App 382, 398 (2014) *citing State v. Unger*, 356 Or 59, 84 (2014). The state may "rebut that presumption by establishing that the disputed evidence 'did not

derive from the preceding illegality'" *Id*. *quoting State v. Hall*, 339 Or 7 (2005). The doctrine of inevitable discovery is an exception to the exclusionary rule. *State v. Miller*, 300 Or 203 (1985) *superseded by statute on other grounds Powers v. Cheeley*, 307 Or 585, n 13 (1989).

The analysis begins with the premise that evidence was illegally obtained. In this case, the illegally-obtained evidence is the evidence from the packet sniffer regarding the location of IanAnderson-PC, and the evidence seized from the execution of the warrant at Mr. Simons's residence. IanAnderson-PC was seized during the execution of the warrant. The police seizure of IanAnderson-PC was the fruit of the unlawful search of Mr. Simons's home using the packet sniffer.

At the time the state obtained its warrant to search Mr. Simons's residence, they had evidence that a PC identified as IanAnderson-PC had connected to websites that contained suspected child pornography. They also had information that a known felon facing new charges told them during a jailhouse interview that he gave a computer identified as IanAnderson-PC to Mr. Simons at least two years before the application for the search warrant, when they both lived in Westfir. Defendant's Motion to Suppress and Controvert, Exhibit A at 15. What the police were unable to do without the unlawful use of the packet sniffer, was determine whether Mr. Simons still owned IanAnderson-PC, and whether the PC was present in Mr. Simon's home in June of 2019. The state will be unable to prove that the police would have been able to determine the location of IanAnderson-PC in Mr. Simons's home by lawful, predicable police procedures.

//

//

//

//

//

//

//

//

V. Conclusion

For the above-stated reasons, and for the reasons set forth in Defendant's Motion to Controvert and Suppress, the defense respectfully requests that the court suppress the web-browsing history obtained without a warrant, and suppress the items seized from Mr. Simons's residence as a result of the search warrant.

DATED: May 29, 2020

Respectfully Submitted,

ROSALIND MANSON LEE, LLC

By: /s/Rosalind M. Lee
Rosalind M. Lee
Of Attorneys for Defendant Simons