

1 Rosalind M. Lee (OSB 055566)
2 Rosalind Manson Lee, LLC
3 474 Willamette St., Ste 302
4 Eugene, OR 97401
5 Tel: (541) 485-5110
6 Fax: (541) 485-5111
7 ros@mansonlee.com

8 Of Attorneys for Defendant
9 RANDALL DE WITT SIMONS

10
11 IN THE CIRCUIT COURT OF THE STATE OF OREGON
12 LANE COUNTY

11	STATE OF OREGON,)	Case No. 19CR43543
12)	
13	Plaintiff,)	REPLY TO STATE’S RESPONSE TO
14	vs.)	DEFENDANT’S MOTION TO
15)	CONTROVERT AND SUPPRESS
16	RANDALL DE WITT SIMONS,)	Oral Argument and Evidentiary Hearing
17)	Requested
18	Defendant.)	Time: Approximately 4 Hours
19	_____)	

20 **I.**

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

26 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,

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

10 II.

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

12 The Oregon Supreme Court recognizes that data contained in computers is different than
13 other personal property, and that article 1, section 9 of the Oregon Constitutions protects that data
14 from unreasonable searches and seizures. In *State v. Mansor*, 363 Or 185 (2018) the Oregon
15 Supreme Court considered, *inter alia*, whether a warrant to search a computer for the defendant’s
16 internet browsing history on a single day allowed the police to search the computer for all of the
17 defendant’s internet browsing history. Relying on *State v. Munro*, 399 Or 545 (2005), the state
18 argued that because the computer was in the lawful possession of the police at the time they searched
19 the browsing history, the defendant no longer had a privacy interest in its contents. *Mansor, supra*,
20 363 Or at 209. The court rejected that argument, distinguishing the contents of a computer from the
21 videotape seized by the police in *Munro*, because of the nature of contents of a computer, including a
22 person’s internet browsing history. *Id.* at 210. The court in *Mansor* held that the police exceeded
23 the scope of the warrant by searching for internet history on days other than the one specified in the
24 warrant. *Id.* at 221.

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

1 browsing history without a warrant supported by probable cause that specifies the scope of the
2 search. Notably, the court in *Mansor* recognized the particular privacy interest in data contained in
3 electronic devices affirmed by the United States Supreme Court in *Riley v. California*, 573 US 373
4 (2014).¹

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

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

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

23 //

24 //

25
26 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).

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

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, propert 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

1 electronic communication was recorded by the detective when he took what appears to be screen
2 shots of the packet sniffer software as it was searching for IanAnderson-PC. *See* Discovery at
3 000074-75.

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

11 The state further argues that items seized in violation of a statute are not subject to suppression
12 “unless the legislature has created an express exclusionary remedy for a statutory violation.” State’s
13 Response at 6-7 *quoting State v. Silbernagel*, 229 Or App 688, 690-91 (2009). Oregon’s
14 wiretapping statute has an express exclusionary remedy for a statutory violation. ORS 133.735,
15 which is titled “Suppression of intercepted communications; procedure; grounds; appeal”
16 specifically requires suppression of information unlawfully seized under ORS 133.724. The statute
17 particularly requires that if the motion to suppress evidence seized in violation of the wiretapping
18 statute is granted, then “the contents of the intercepted wire, electronic or oral communication, *or*
19 *evidence derived therefrom*, shall be treated as having been unlawfully obtained.” ORS
20 133.735(c)(2) (emphasis added.)

21 In its response, the state does not address the defense argument that in using the packet sniffer,
22 Det. Weaver violated the federal wiretapping statutes. Rather than restating the Title III arguments
23 here, the defense respectfully refers the Court to Defendant’s Motion to Controvert and Suppress at
24 10-11.

25 //

26 //

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

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

8 1. *Article 1, section 9.*

9 Article 1, section 9 of the Oregon Constitution recognizes privacy interests outside the
10 curtilage of one’s home. For example, placing a radio transmitter on a person’s car and tracking the
11 car’s movements in public is a search under article 1, section 9. *State v. Campbell*, 306 Or 157
12 (1998). While unaided observations from public places are not searches, use of technology in
13 making observations can constitute searches when “the practice, if engaged in wholly at the
14 discretion of the government will significantly impair ‘the people’s’ freedom from scrutiny. *Id.* at
15 170.

16 The detective used the packet sniffer to look for a particular item in Mr. Simons’s home. The
17 detective did not have a warrant to search the house, and could not see into the house, unaided, from
18 a lawful vantage point. The detective used specialized technology to look inside the house. Using
19 packet sniffers without any judicial oversight through the use of a warrant or a wiretapping order
20 will significantly impair our freedom from scrutiny, because the police will be able to look into
21 anyone’s home at any time for internet connected devices, and download payload data, or merely
22 inventory electronic devices in the residence. The WiFi signal from a device present in a home that
23 is connected to a router also located in the home is detectable with a packet sniffer. *See generally*
24 *Joffe v. Google, Inc.* 746 F3d 920, 923 (9th Cir. 2013) *cert. denied Google v. Joffe*, 573 US 947
25 (2014)(describing how Google downloaded payload data from residential WiFi networks using a
26

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

3 2. *Fourth Amendment*

4 In 1967, the Supreme Court held that the Fourth Amendment protects “people” and not
5 simply “places”—against unreasonable searches and seizures.” *Katz v. United States*, 389 US 347,
6 351 (1967). This includes “surveillance . . . without any ‘technical trespass under local property
7 law.’” *Id.* at 353. According to *Katz* and the more than fifty years of Supreme Court precedent that
8 have followed it, “what [one] seeks to preserve as private, even in an area accessible to the public,
9 may be constitutionally protected” so long as there is a “reasonable expectation of privacy.”
10 *Carpenter, supra*, at 2217 *citing Katz*, at 351-52) (alteration in original); *see* Defendant’s Motion to
11 Suppress and Controvert at 19-23 (arguing that Mr. Simons has a reasonable expectation of privacy
12 in his internet communications).

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

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

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

10 Finally, in *Kyllo v. United States*, the Court examined police use of a thermal-imaging device
11 to determine, from a distance, whether a particular home was operating grow lights indicative of
12 marijuana production. *See Kyllo v. United States*, 533 US 27, 29-30 (2001). Once again, the Court
13 found that a Fourth Amendment search had occurred even though the government had committed no
14 physical trespass. *See id.* at 32-33. The Court held that, “obtaining by sense-enhancing technology
15 any information regarding the interior of the home that could not otherwise have been obtained
16 without physical intrusion into a constitutionally protected area, constitutes a search—at least where
17 (as here) the technology in question is not in general public use.” *Id.* at 34 (citations and internal
18 quotations omitted.) Such a rule is necessary when new technology upsets expectations of privacy,
19 the Court explained, in order to “assure[] preservation of that degree of privacy against government
20 that existed when the Fourth Amendment was adopted.” *Id.*

21 Legislative protections for electronic communications also recognize the need to protect
22 information in transit. The whole point of the telephone, of course, was to be able to communicate
23 with individuals located outside of one’s home. Legislatures therefore recognized the need to protect
24 the privacy of these communications. One year after *Katz*, for example, Congress passed Title III of
25 the Omnibus Crime Control and Safe Streets Act of 1968 (*i.e.*, the “Wiretap Act”), Pub. L. 90-351,
26 82 Stat 212 (1968), which specifically prohibited obtaining wire communications contemporaneous

1 with transmission *See Konop v. Hawaiian Airlines, Inc.*, 302 F3d 868, 878 (9th Cir. 2002). Again in
2 1986, Congress passed the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848
3 (1986), to include protections for electronic communications while they are being made, are in
4 transit, and stored on computers.

5 In this case, law enforcement used new technology—the packet sniffer—to gain information
6 about the inside of Mr. Simons’s home that they did not and could not have learned from visual
7 surveillance alone. As in *Karo*, “there is no gainsaying that the [packet sniffer] was used to locate
8 the [computer] in a specific house..., and that that information was in turn used to secure a warrant
9 for the search of the house.” *Karo, supra*, at 714. Under *Katz, Karo*, and *Kyllo*, the relevant question
10 is whether Mr. Simons had an expectation of privacy in his WiFi traffic and internet
11 communications, not whether those signals crossed his property line. The state does not
12 acknowledge this binding case law, but instead seeks to revive an argument that has been thoroughly
13 and repeatedly rejected. This Court should likewise reject such a mechanical interpretation of the
14 Fourth Amendment and not “leave the homeowner at the mercy of advancing technology.” *Kyllo*,
15 533 US at 35-36.

17 IV.

18 **The Doctrine of Inevitable Discovery Does Not Purge the Taint of the 19 Officer’s Illegal Seizure of the Computer Known as IanAnderson-PC.**

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

24 Under Oregon law, if the state obtains evidence seized in violation of article 1, section 9 of
25 the Constitution, “it is presumed that the evidence was tainted by the violation and must be
26 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

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

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

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

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

1 **V. Conclusion**

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

6 DATED: May 29, 2020

7 Respectfully Submitted,

8 ROSALIND MANSON LEE, LLC

9 By: /s/Rosalind M. Lee
10 Rosalind M. Lee
11 Of Attorneys for Defendant Simons
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26