

IN THE CIRCUIT COURT OF THE STATE OF OREGON
FOR THE COUNTY OF LANE
125 E. 8th Ave. Eugene, Oregon 97401

STATE OF OREGON,

Plaintiff,

v.

RANDALL DE WITT SIMONS,

Defendant.

Case No. 19CR43543
SUPPLEMENTAL
OPINION AND ORDER
RE: DEFENDANT'S MOTION TO
CONTROVERT AND SUPPRESS

The parties are before the Court on Defendant's Motion to Supplement the Court's Findings in Defendant's Motion to Controvert the Search Warrant, and Motion to Suppress. The Court having reviewed the following pleadings, Defendant's Motion to Controvert and Suppress, Defendant's Memorandum in Support of Motion, State's Response to Defendant's Motion to Controvert and Suppress, Defendant's Amended Motion to Controvert and Suppress, and State's Supplemental Brief in Support of Response to Defendant's Amended Motion to Controvert and Suppress, Defendant's Supplemental Memorandum in Support of Defendant's Amended Motion to Suppress.

I. Relevant Facts

The facts presented are those provided in Affidavit in Support of Search Warrant, Grand Jury Testimony, and testimony presented through witnesses at the pretrial Motion to Controvert and Suppress. The Court finds the relevant facts as follows:

At the time of the criminal investigation in this matter, Mr. Rodney Porteous owned the A&W Restaurant on Highway 58, Oakridge, in Lane County Oregon. Mr. Porteous employed private consultant, Kenneth Sanders, to assist him with installation and maintenance of a wireless internet platform to allow his restaurant patrons access to the internet. The A&W wireless network signal strength was sufficiently strong to allow public users, not within the restaurant, to also access the internet. All users to the A&W Wi-fi network were granted access only after acknowledging and accepting (by clicking) the "terms of use." (Exhibit 1).

Mr. Sanders assisted Mr. Porteous in establishing a firewall for the A&W wireless network. As part of establishing the safety protocols for the A&W wireless network, Mr. Sanders utilized a program (Untangle) that listed all the sites that any user of the network visited. Such sites were catalogued by category.

On July 2, 2018, while performing routine maintenance of the computer for Mr. Porteous, Mr. Sanders displayed the catalogued information and Mr. Porteous questioned him about the category showing "child abuse/child pornography" (Exhibit 102). Mr. Sanders testified that when he sees that category, he feels he is required to report that to law enforcement. Mr.

Sanders and Mr. Porteous then had contact with Officer Larson at Oakridge Police Department. Mr. Sanders reported to Officer Larson that the computer that was accessing child pornography was called "Ian Anderson-PC" and had a specific address assigned to the device. Such addresses are called "MAC" (Media Access Control) addresses that are unique to each device.

From July 2018 until June 2019, Mr. Sanders and Officer Larson worked collaboratively to identify when the "Ian Anderson PC" was logging into child abuse/pornography websites. Mr. Sanders indicated that he established an alert system that would send an email to Officer Larson (at an email provided by Officer Larson) any time a child abuse/pornography site was accessed. Mr. Sanders indicated that he offered this service to Officer Larson to assist with the investigation. Officer Larson indicated he felt he and Mr. Sanders were working together to get the information for the investigation. During this period of time, A&W network continued to log all websites visited by all users including those catalogued as child abuse/pornography.

From October 2018 until June 2019, Officer Larson focused his investigation on Phillip Thomas, a registered sex offender living in Oakridge, who uses an alias of Ian Anderson within the community. In May 2019, a search warrant was issued regarding Mr. Thomas' house, car, person, and electronics. Mr. Thomas was found to be a felon in possession of firearms and was subsequently lodged in jail. Detective Robert Weaver questioned Mr. Thomas about the "IanAndersonPC" laptop and Mr. Philips disclosed that he had given his laptop to a "Randy" and knew him to be living across from A&W on Highway 58. Detective Weaver was able to ascertain that Mr. Thomas had purchased a Toshiba Laptop with the same MAC address as the IanAndersonPC address that had been catalogued by A&W. While Mr. Thomas was detained in Lane County Jail, someone using IanAndersonPC, same MAC address, had accessed the child abuse/pornography websites.

Law enforcement expanded their investigation to include Mr. Simons. Detective Weaver was able to review DMV records, and utility records to confirm Mr. Simons residence at 47816 Highway 58 Unit 1 in Oakridge. On June 24, 2019, Detective Weaver and Officer Larsen used a laptop with the Linux operating system and the Kismet Software together with an external directional wireless network antennae to intercept and analyze data of every wireless device broadcasting in the area at or near Mr. Simons residence, such antennae and programs are called "packet sniffers". While utilizing the device Detective Weaver focused on identifying radio traffic associated with the MAC address assigned to IanAndersonPC. He paced the area near A&W Restaurant and Mr. Simons' home to ascertain 1) whether the signal was broadcasting, and 2) the signal strength both of which are accomplished by intercepting data packets broadcast by that computer. Detective Weaver determined that the IanAndersonPC was broadcasting, and through the additional functions of his directional antennae he was able to narrow the scope of the location from which the broadcast was occurring.

Detective Weaver then applied for and was granted a Search Warrant for Mr. Simons personally and for his property. Officers located the Toshiba laptop with MAC address and identifying information of Ian AndersonPC within Mr. Simons' home. When officers searched the laptop they located child pornography.

II. Legal Analysis

Should the Court strike from the affidavit in the search warrant information obtained using the packet sniffer because the information was illegally obtained and without the location of the Ian Anderson PC the affidavit is not supported by probable cause.

An affidavit in support of a search warrant may not be based on illegally-obtained information. State v. McKee, 89 Or App 94, 99 (1987). If an affidavit in support of a search warrant contains illegally-obtained information, the reviewing court excises that information from the warrant and determines whether the affidavit still establishes probable cause. State v. Binner, 128 Or App 639, 646 (1994).

Intercepting electronic communications without authorization from a court is illegal. *See* ORS 133.724 (outlining the requirements for obtaining a court order for the interception of wire, electronic or oral communications); *See also* 18 USC § 2510. Evidence obtained in violation of Oregon's wiretapping law is inadmissible in any proceeding. ORS 133.735(2).

Before intercepting electronic communications, a district attorney or deputy district attorney must apply to the court for an order allowing the interception. ORS 133.724. The application must include the name of the attorney applying for the order; the name of the law enforcement officer making the application; a statement demonstrating that there is probable cause that an individual is committing or is about to commit one of the crimes listed in the statute; a description of the crime alleged; a description of the nature and location of the facilities from which the electronic communication is to be intercepted; the identity of the suspect; and "[a] full and complete statement as to whether or not other investigative procedures have been tried and failed or why other investigative procedures reasonably appear to be likely to succeed if tried or are likely too dangerous." ORS 133.724(1)(a)-(h). All intercepted communications must be recorded and delivered to the court. *Id.* at 133.729.

For the purposes of Oregon's wiretapping statute, an electronic communication "*means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a radio, electromagnetic, photoelectronic or photo-optical system, or transmitted in part by wire, but does not include any oral communication or any communication that is completely by wire; or (b) any communication made through a tone-only paging device.*" ORS 133.721

Oregon's wiretapping law is based on the federal wiretap statutes, known by the shorthand "Title III," and found at 18 USC sections 2510-2520. Oregon's wiretapping law is more restrictive than Title III. State v. Stockfleth, 311 Or 40, 49 (1991). The court in Stockfleth examined the legislative history of ORS 133.724 et seq. and noted that the legislature's "strong, express effort to conform Oregon law to the perceived mandates of federal law implies that prior binding federal precedent was included in the legislature's design." *Id.* at 52. The court also noted that "Oregon adopted its cognate provisions generally to conform to the 1968 amendments to the federal law. Accordingly, it is particularly appropriate to review cases interpreting the

federal statutes in applying their Oregon counterparts.” Id. at 46-47 citing Computer Concepts, Inc. v. Brandt, 310 Or 706 10 (1990).

Title III has a similar definition of “electronic communication” as the comparable Oregon statute. Compare 18 USC 2510(12) with ORS 133.721(3). The only difference in these definitions is that the federal statute excludes from the definition of electronic communication any communication from a tracking device and electronic funds transfer information stored by a federal institution. 18 USC §§ 2510 (12)(C), (D). However, under the federal statute, it is not illegal to intercept radio communications that are “readily accessible to the general public.” 18 USC § 2511(1)(g)(i).

Federal courts that have considered the use of packet sniffers in the context of Title III wiretaps have found that intercepting wireless data without a court order violates Title III. Like the Oregon wiretapping statute, federal law allows a civil cause of action for damages for violating Title III. See ORS 133.739; 18 USC §2520. See Joffe v. Google, Inc, 746 F3d 920, 923 (9th Cir. 2013) cert. denied Google Inc. v. Joffe, 573 US 947 (2014).

In this case, Detective Weaver intercepted radio wave communications of IanAndersonPC device as they were broadcast from a location on Highway 58 and Rock Rd. Such broadcast was a voluntary effort of the user of IanAndersonPC to attempt to engage with a publicly offered WiFi system at A&W Restaurant intended for restaurant patrons. The user of IanAndersonPC was not attempting to keep his computer’s radio wave/wifi communications private or confined to the privacy of his abode but instead, was reaching out, to attempt public contact. In this way, the Court distinguishes the actions of the Defendant from the affected parties in the Joffe case.

When Detective Weaver scanned the airwaves on or near the location of the A&W Restaurant, he did not initially limit his search of airwaves to only IanAndersonPC’s identifying MAC address, he received information about all users broadcasting in the area. Detective Weaver testified that he then targeted specifically his software to look for the IanAndersonPC MAC address, which he found. The specially equipped law enforcement devices used by Detective Weaver were capable (although Detective Weaver testified that he disregarded the function) of ascertaining specifically which sites IanAndersonPC was actively downloading information. Defense argument that we maintain a privacy interest in our devices when we affirmatively direct our devices to reach out and seek public access overstates the breadth of the law regarding privacy expectations. See United States v. Forrester, 512 F3d 500 (2008). Also, the State’s argument that once someone is broadcasting outside of their home they forgo privacy interests attempts to oversimplify what the courts have grappled with for decades. It ignores the nuance presented to us in the rapidly evolving technology realm that people expect privacy where perhaps none currently exists under law.

In this case Detective Weaver not only used a computer with a unique operating system (Linux), his system also required the use of specialized programs and a directional antennae to enhance observations that are not readily apparent to the general public. It is for this reason, this case is more similar to Kyllo v. United States, 533 U.S. 27 (2001). The police in Kyllo used a device to measure the infrared radiation that was coming from Defendant’s home. Such

radiation is not visible to the naked eye and the court found 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 where the technology in question is not in general public use.” Id at 34. However, in Kyllo, unlike this case, the parties were not attempting to reach outside their home to access a third party’s private, yet publicly available, wireless network.

I find that the limited use of the Kismet software to intercept generalized radio waves (akin to a cloud over an area of space) not attributed to any particular location, that solely identify the MAC address and title of IanAndersonPC does not violate a privacy interest held by Defendant. That information was intentionally broadcast by Defendant in this case to seek out a publicly available but privately owned wi-fi network at A&W restaurant. Mr. Simons’ radio wifi waves were not an incidental overflow of radio transmission from his private property into the public domain but rather a purposeful display of radio waves to the public.

However, I find that the law enforcement use of Kismet (an enhanced device) and the associated technology to ascertain the intensity of a signal resulting in directional identifiers/location is a search specifically designed yield admissible evidence in a criminal case. Further, the Kismet device was capable of capturing the specific content of communications of IanAndersonPC as it attempted to download information from A&W Restaurant. (Although Det. Weaver testified that he disregarded this function of the program). Such searches require a court order under both Oregon and Federal Wiretapping laws. That did not occur in this case.

Using a packet sniffer device to identify the specific location of Mr. Simons’ computer in his home by searching with an enhanced device violated Article 1 Section 9 of the Oregon Constitution. The Court adopts Mr. Simons’ arguments in support specifically the legal rationale stated in State v. Tucker 330 Or 85 (2000), State v. Campbell 306 Or 157 (1988), State v. Carle 255 or App 102 (2014), and State v. Lien 364 Or 750 (2000). The Court distinguishes, in this case, the willful broadcast of the radio waves emitting from Mr. Simons’ home while the computer (and presumably its user) attempts to access a privately held but publicly available network. When law enforcement captures the general basic MAC address and name identifier from the cloud of radio waves, that identification of use/broadcasting does not constitute a search in violation of Article 1 Sect. 9, but rather when law enforcement uses the enhanced device to access specific location, intruding on the privacy interest one holds in their home, that is where the violation of Article 1, Sect 9 occurs. Oregon Constitution affords its citizens more protections than have been historically contemplated by the scope of the US Constitution 4th Amendment.

Using a packet sniffer device to identify the specific location of Mr. Simons’ computer in his home by searching with an enhanced device violated the U.S. Constitution 4th Amendment right regarding being free of unreasonable searches and seizures. The Court adopts the Defendant’s argument in support specifically the legal rationale outline in United States v. Jones 565 US 400 (2012). Riley v. California 573 US 373 (2014). Kyllo v. United States 533 US 21 (2001) and United States v. Karo 468 US 706 (1984). The Court distinguishes, in this case, the willful broadcast of the radio waves emitting from Mr. Simons’ home while the computer (and presumably its user) attempts to access a privately held but

publicly available network. When law enforcement captures the general basic MAC address and name identifier from the cloud of radio waves, that identification of use/broadcasting does not constitute an unreasonable search in violation of the 4th Amendment, but rather when law enforcement uses the enhanced device to access specific location, intruding on the privacy interest one holds in their home, that is where the violation of 4th Amendment right to be free of unreasonably search and seizure exists.

Using a packet sniffer device to intercept actual communications of a device is a search. I find that the MAC addresses and name identifier (IanAnderson PC) is not a communication (meaning data packet transfers) but rather a label given the device as it attempts to exchange the data packets. The use of the packet sniffer to access radio waves in an open space to track and monitor the exchange of data packets (including information about sites that are visited and downloaded) is a search under both Article 1 Sect 9 and the 4th Amendment and unless there is a supported warrantless exception, which the Court does not find in this case, a warrant was required to use the packet sniffer for any information exceeding the initial identifiers. Again, in this case the user of IanAndersonPC was attempting to send his particular information into the open space of a public wifi network hosted by a private third party. Had the government used the packet sniffer to ascertain MAC address and name identifier for a closed networking system within the home, that too, would be a violation of both Article 1 Sect. 9 and the 4th Amendment. But that was not the circumstance in this case.

Defendant argues that the tracking the internet browsing history of Mr. Simons' computer by Mr. Sanders was illegal, because it was done at the direction of the police and without a warrant, and should be stricken from the warrant and suppressed.

The court finds that Mr. Sanders and Mr. Porteous contacted law enforcement and that together with law enforcement, they developed a plan to exchange information such that Officer Larsen would receive instantaneous email alerts when someone was accessing a child abuse and pornography site on the A&W restaurant network. I find that Mr. Sanders was an agent of the state, acting on behalf of the state in gathering information for a criminal investigation for child abuse and child pornography viewers.

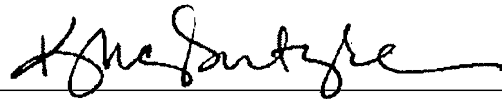
However, I find that when a member of the public seeks out to access another's privately owned but publicly available network (such as A&W's) where the restaurant offered the network to patrons, free of charge, they accept the terms of use with that network. Further, they can have no reasonable expectation of privacy when utilizing such network in this way, particularly when not a patron of the business. Therefore, in this public access to a third party private network setting there can be no privacy interest held by Mr. Simons in what the A&W network provider is reviewing, logging, sharing, and forwarding to law enforcement. Therefore, although Mr. Sanders was an agent of the state through his consulting employment with A&W and following Mr. Porteous directives to assist law enforcement, I find the evidence of the browsing history of IanAndersonPC was lawfully obtained by A&W and that the information was lawfully shared with law enforcement. One cannot expect to access, for free, a third party's open/public access wi-fi and tell that third party "not to look" at what they are doing. I distinguish this from

circumstances when one accesses their own wireless network, or access their privately paid for wireless connection. This circumstance is different. One cannot expect to actively seek to join another's free wi-fi and commit criminal acts and then claim that the third party cannot share that information with law enforcement.

3. Ruling

Therefore, the information about the location and strength of signal that Detective Weaver used in the affidavit in support of the search warrant shall be excised from the warrant and further that the evidence regarding this portion of the search shall be suppressed. Defendant asserts that without the location of IanAnderson-PC derived from the Kismet Software search, the warrant lacked probable cause. I find that the affidavit in support of the search warrant outlines specific and sufficient probable cause despite the suppression of the Kismet evidence outlined above. Det. Weaver's search of the computer for its browsing history did not exceed the scope of the warrant.

Signed: 9/1/2021 09:33 AM



Karrie K. McIntyre, Circuit Court Judge