

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](mailto: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

13 STATE OF OREGON, )  
14 )  
15 Plaintiff, )  
16 vs. )  
17 RANDALL DE WITT SIMONS, )  
18 )  
19 Defendant. )  
20 \_\_\_\_\_ )

Case No. 19CR43543

MEMORANDUM OF POINTS  
AND AUTHORITIES IN  
SUPPORT OF DEFENDANT’S  
MOTION TO CONTROVERT  
AND SUPPRESS

Oral Argument and Evidentiary  
Hearing Requested  
Time: Approximately 4 hours

21 **I. Introduction**

22 The search of defendant Randall Simons’s home, car, person, and effects including his  
23 computer and other electronic devices was unlawful, because the application in support of the search  
24 warrant included information that was illegally obtained, and without the illegally obtained evidence,  
25 the warrant is not supported by probable cause. Specifically, the police located a computer in Mr.  
26 Simons’s home by intercepting the wireless signal from that computer. Searching the home by  
intercepting the wireless signal of the computer located in the house was illegal, because it was  
without a court order in violation of ORS 133.724, and because it was made without warrant in

1 violation of article 1, section 9 of the Oregon Constitution and the Fourth Amendment to the United  
2 States Constitution.

3         Once this illegally obtained information is stricken from the affidavit in support of the warrant  
4 in this case, the warrant is not supported by probable cause. All evidence obtained from the warrant  
5 and the fruits thereof should be suppressed.

6         Separately and in addition, the defense submits that internet activity gathered by a private  
7 party at the direction of the police was also illegally obtained, because the internet activity was  
8 gathered without a warrant. That evidence should be stricken from the application for warrant, and  
9 should be suppressed. Without that evidence, the warrant is not supported by probable cause.

10  
11   **II.         Statement of the Case and Relevant Facts**

12             A. Statement of the Case

13             Mr. Simons is charged by indictment with 15 counts of Encouraging Child Sexual Abuse in  
14 the First Degree, in violation of ORS 163.684. The conduct in counts 1-14 of the indictment  
15 allegedly occurred before June 27, 2019, the day the court issued the search warrant at issue in this  
16 motion. Count 15 is alleged to have occurred on June 27, 2019.

17             Mr. Simons has entered not guilty pleas. Trial in this matter is set for April 15, 2020.

18             B. The Investigation<sup>1</sup>

19             On July 2, 2018, Oakridge Police Officer Loren Larsen contacted Rodney Porteous and Ken  
20 Sanders. Exhibit A at 32. Mr. Porteous owns the A&W restaurant on Highway 58 in Oakridge. *Id.*  
21 The A&W restaurant offers free wireless internet access to the public. *Id.* at 33. Mr. Sanders is an  
22 independent contractor who maintains the wireless network at the A&W. *Id.* at 33. When accessing  
23

24 <sup>1</sup> These facts are taken from the reports and data provided in discovery in this case, the affidavit in  
25 support of the warrant in this case and from the grand jury testimony in this case. The search warrant  
26 and affidavit are attached hereto as Exhibit A, and incorporated by reference herein. A transcript of  
the grand jury testimony is attached hereto as Exhibit B, and incorporated by reference herein.

1 the network, a user must “agree to terms and conditions related to the monitoring and prohibition of  
2 illegal activity.”<sup>2</sup> Mr. Sanders and Mr. Porteous reported to Officer Larsen that someone was using  
3 the public WiFi provided by the A&W to access websites suspected to contain child pornography.  
4 *Id.* at 32-33. Officer Larsen determined that a computer accessing these sites was named  
5 “IanAnderson-PC.” *Id.* at 33.

6 From July of 2018 through June of 2019, Mr. Sanders tracked all of the internet activity, legal  
7 and illegal, of IanAnderson-PC and an Android device called “Android-f278c8e04f5e02a4.”<sup>3</sup> The  
8 A&W uses Untangle NG Firewall software to monitor and categorize the websites being accessed on  
9 its WiFi network.<sup>4</sup> This software can also block access by specific users or to specific websites or  
10 categories of websites. *NG Firewall Apps*, Untangle, [https://www.untangle.com/untangle-ng-](https://www.untangle.com/untangle-ng-firewall/applications/#Filter)  
11 [firewall/applications/#Filter](https://www.untangle.com/untangle-ng-firewall/applications/#Filter) (last visited Nov. 14, 2019). Each time either IanAnderson-PC or the  
12 Android device accessed a website that contained suspected child pornography, Officer Larsen  
13 received an email at [lorenlarsen@ci.oakridge.or.us](mailto:lorenlarsen@ci.oakridge.or.us). Larsen’s e-mail address is not available  
14 publicly. Declaration of Counsel at 2.

15 The subject line of each email is “Untangle Server event! [untangle.example.com.]” The  
16 sender’s email address is [Subway.AandW@untangle.com](mailto:Subway.AandW@untangle.com). The body of the email contains  
17 information regarding the flagged internet activity, including the date and time of the activity and the  
18 name of the device accessing the website. *Id.*

19 //

20 //

---

22 <sup>2</sup> The warrant does not provide the language of the terms and conditions, and does not aver whether  
23 a user consents to monitoring by the police or any government agency with or without a warrant and  
24 with or without probable cause.

25 <sup>3</sup> The defense has received in discovery spreadsheets containing browsing history from both devices.  
26 It is unclear from the discovery whether this Android is associated with Mr. Simons.

<sup>4</sup> *See* Declaration of Counsel at 2.

1 Starting in October, 2018, and continuing through June, 2019, Officer Larsen focused his  
2 investigation on Phillip Thomas, a registered sex offender living in Oakridge, who uses the name Ian  
3 Anderson. Exhibit A at 34-36.

4 In May of 2019, Officer Larsen enlisted the help of Detective Robert Weaver of Springfield  
5 Police. Discovery at 000064. In June of 2019, Officer Larsen obtained a warrant to search the  
6 house, car, person and electronic devices of Phillip Doyle Thomas.<sup>5</sup> After the search of his house,  
7 Mr. Thomas told Det. Weaver that he had given the computer identified as IanAnderson-PC to  
8 Randy Simons who lived in Westfir at the time. *Id.* at 15. Mr. Thomas told Det. Weaver that he  
9 knew that Randy Simons had moved to Oakridge and lives at the southeast corner of Rock Road and  
10 Highway 58, across the street from the A&W. *Id.* at 15. Mr. Thomas said that he had “become  
11 upset” with Mr. Simons and has not had contact with him in the “last couple years.” *Id.*

12 Mr. Sanders, the contractor who maintains the A&W wireless network, also provided Officer  
13 Larsen with a spreadsheet showing web addresses viewed using IanAnderson-PC between the dates  
14 May and June, 2019. Exhibit A at 33. The defense does not know when Mr. Sanders provided that  
15 information to Officer Larsen.<sup>6</sup>

16 Detective Weaver confirmed that in 2009 Mr. Thompson had purchased a Toshiba laptop that  
17 had the same MAC address as Ian Anderson-PC. *Id.* at 16.

18 The detective then received from Mr. Sanders a spreadsheet showing the web pages and  
19 images accessed by Ian Anderson-PC, and confirmed that some of those websites contained child  
20 pornography. *Id.* at 16-17. Spreadsheets received by the defense in discovery includes web  
21 browsing history for July, August, October and November of 2018 and March, April, May and June  
22 of 2019. Declaration of Counsel at 2. There is not web activity every day of every month, and  
23 appears to include all web browsing activity, not just activity related to child pornography. *Id.*

---

24 <sup>5</sup> That warrant and the affidavit in support are an exhibit to Detective Weaver’s warrant in this case,  
25 and can be found at pages 23-39 of Exhibit A.

26 <sup>6</sup> The defense has requested all reports from Oakridge Police regarding its investigation in this case.  
That request is pending.

1 On June 23, 2019, Det. Weaver ran Mr. Simons's name through a law enforcement database.  
2 Exhibit A at 17. He confirmed that Mr. Simons lived at 47816 Highway 58, Unit 1 in Oakridge, and  
3 that Mr. Simons had been associated with that address since July of 2018. *Id.*

4 On June 24, 2019, Det. Weaver and Officer Larsen used a laptop using the Kali Linux  
5 operating system, Kismet software and an external directional wireless network antenna to intercept  
6 and analyze the WiFi traffic of every device connected to the wireless router at the A&W. *Id.* at 18-  
7 19. Detective Weaver focused on the traffic from IanAnderson-PC, and walked around Mr.  
8 Simons's address to determine in which residence the computer was located. *Id.* at 19. The detective  
9 tracked the computer to Mr. Simons's home, which is approximately 140 yards from the A&W.<sup>7</sup> *Id.*  
10 at 19.

11 On June 26, 2019, Det. Weaver ran Mr. Simons's name through the DMV database. The  
12 DMV records indicated that Mr. Simons's address was 47816 Highway 58 Unit 1, Oakridge,  
13 Oregon. *Id.* at 17. Officer Larson told Det. Weaver that he had contacted Mr. Simons at his  
14 residence while working patrol. *Id.* at 18. The affidavit does not give a date of that contact.

15 On June 27, 2019, Detective Weaver applied for and was granted the search warrant that is the  
16 subject of this motion. In Mr. Simons's home, the detective found the laptop known as  
17 IanAnderson-PC. After searching the laptop, the detective found contraband.

### 18 C. Using WiFi Networks

19 WiFi networks originate at a single location, such as a restaurant, home or business, and  
20 connect to all devices in the immediate vicinity. WiFi networks can connect to devices up to 300  
21 feet away, including over nearby structures and properties, and can have over a hundred devices  
22 connected to them. Bradley Mitchell, *What Is the Range of a Typical WiFi Network?*, Lifewire (Oct.  
23 28, 2019), <https://www.lifewire.com/range-of-typical-wifi-network-816564> (last visited November  
24 21, 2019); Bradley Mitchell, *How Many Devices Can Connect to One Wireless Router?*, Lifewire  
25

---

26 <sup>7</sup> This distance was calculated with the "Measure Distance" tool on Google Maps.

1 (July 23, 2019), <https://www.lifewire.com/how-many-devices-can-share-a-wifi-network-818298>  
2 (last visited November 21, 2019). Internet-enabled devices often automatically connect to nearby  
3 wireless networks. AT&T and Comcast customers, for example, must take affirmative steps to  
4 prevent auto-connection to the companies' respective "hotspots." *Manage WiFi on Your Mobile*  
5 *Device*, AT&T, <https://www.att.com/esupport/article.html#!/wireless/KM1010177> (last visited Nov.  
6 11, 2019); *How Do I Stop My Device from Auto-connecting to Xfinity WiFi Hotspots?*, XFINITY,  
7 <https://www.xfinity.com/mobile/support/article/stop-phone-autoconnecting-wifi-hotspots> (last  
8 visited Nov. 11, 2019). When a modern device connects to any WiFi network even once, the device  
9 saves the network information and will auto-connect to it unless the device user takes affirmative  
10 steps to prevent it. Bradley Mitchell, *How to Prevent WiFi From Connecting Automatically*,  
11 Lifewire (June 28, 2019), [https://www.lifewire.com/avoid-automatic-connection-to-wifi-networks-](https://www.lifewire.com/avoid-automatic-connection-to-wifi-networks-818312)  
12 [818312](https://www.lifewire.com/avoid-automatic-connection-to-wifi-networks-818312).

13           Devices connected to a WiFi network transmit and receive packets of information through  
14 the local router. These packets make up the "personal emails, usernames, passwords, videos, and  
15 documents" that people send over the internet. *See Joffe v. Google, Inc.*, 746 F3d 920, 923 (9th Cir.  
16 2013) *cert. denied Google Inc. v. Joffe*, 573 US 947 (2014). The router connects to the Internet  
17 Service Provider's ("ISP") gateway, which in turn connects to the broader internet. *See Shaina*  
18 *Hyder, The Fourth Amendment and Government Interception of Unsecured Wireless*  
19 *Communications*, 28 Berkeley Tech. LJ 937, 940-42 (2013).

#### 20           D. Kismet

21           Kismet, the application used by Det. Weaver, is a type of software called a packet sniffer. A  
22 packet sniffer allows a person to intercept all communications and data sent or received by any  
23 computer, phone or other device that is connected to a wireless network. It is a broad and  
24 comprehensive tool. It can capture all of the communications of a particular device, and it can  
25 capture the communications of many devices connected to a network at a time. In addition to  
26

1 capturing communications, a packet sniffer can also pinpoint the physical location of connected  
2 devices.

3 Using packet sniffer software, a person collects and displays the packets in transit,<sup>8</sup> capturing  
4 all of the communications of anyone using the network, without interfering with the packet  
5 transmission or notifying the surveilled devices. *See In re Innovatio IP Ventures, LLC Patent*  
6 *Litigation*, 886 F Supp 2d 888, 890 (ND Illinois, 2012) (describing the potential collection of packets  
7 from “any devices that may be communicating with [a router], such as a customer's laptop,  
8 smartphone, or tablet computer.”); *see also id.* at 890 (describing the potential collection of “e-mails,  
9 pictures, videos, passwords, financial information, private documents, and anything else a customer  
10 could transmit to the internet.”)

11 In addition, a packet sniffer can discover and monitor the location of people connected to a  
12 wireless network. By pairing a packet sniffer with a directional antenna, the person viewing the  
13 packets can also measure signal strength. By observing the change in signal strength while moving  
14 around, rotating the antenna, and “circling the suspected location,” the person using the packet  
15 sniffer can accurately estimate the location of devices connected to the WiFi and their respective  
16 users. *GPS, Kismet*, <https://www.kismetwireless.net/docs/readme/gps/> (last visited Nov. 11, 2019).

### 17 **III. Law and Argument**

#### 18 **A. The Court Should Strike from the Affidavit the Information Obtained Using the Packet** 19 **Sniffer, because that Information was Illegally Obtained, and Without the Location of** 20 **IanAnderson-PC the Affidavit is not Supported by Probable Cause.**

21 An affidavit in support of a search warrant may not be based on illegally-obtained  
22 information. *State v. McKee*, 89 Or App 94, 99 (1987). If an affidavit in support of a search warrant  
23 contains illegally-obtained information, the reviewing court excises that information from the  
24 warrant and determines whether the affidavit still establishes probable cause. *State v. Binner*, 128 Or  
25 App 639, 646 (1994). This memorandum presents arguments first based on relevant statutes, then

---

26 <sup>8</sup> Technological methods to protect packets from surveillance – such as WiFi passwords, HTTPS, or  
VPNs - are generally not fully secure, universally used, nor free.

1 under Article I, section 9 of the Oregon Constitution and the Fourth Amendment to the United States  
2 Constitution.

3 1. *The Location of “IanAnderson-PC” in Mr. Simons’s Home was Unlawfully*  
4 *Obtained, because Detective Weaver Violated ORS 133.724 when he Intercepted*  
5 *Data from the Computer Using Packet-Sniffing Software*

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

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

21 For the purposes of Oregon’s wiretapping statute, an electronic communication

22 “means any transfer of signs, signals, writing, images, sounds, data or  
23 intelligence of any nature transmitted in whole or in part by a radio,  
24 electromagnetic, photoelectronic or photo-optical system, or transmitted in  
25 part by wire, but does not include [a]ny oral communication or any  
26 communication that is completely by wire; or (b) [a]ny communication  
made through a tone-only paging device.”

ORS 133.721. WiFi signals travel over radio frequencies. *Hyder, supra*, at 939.



1 Oregon’s wiretapping law is based on the federal wiretap statutes, known by the shorthand  
2 “Title III,” and found at 18 USC sections 2510-2520. Oregon’s wiretapping law it is more restrictive  
3 than Title III. *State v. Stockfleth*, 311 Or 40, 49 (1991). The court in *Stockfleth* examined the  
4 legislative history of ORS 133.724 et seq. and noted that the legislature’s “strong, express effort to  
5 conform Oregon law to the perceived mandates of federal law implies that prior binding federal  
6 precedent was included in the legislature’s design.” *Id.* at 52. The court also noted that “Oregon  
7 adopted its cognate provisions generally to conform to the 1968 amendments to the federal law.  
8 Accordingly, it is particularly appropriate to review cases interpreting the federal statutes in applying  
9 their Oregon counterparts.” *Id.* at 46-47 citing *Computer Concepts, Inc. v. Brandt*, 310 Or 706  
10 (1990).

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

17 Federal courts that have considered the use of packet sniffers in the context of Title III  
18 wiretaps have found that intercepting wireless data without a court order violates Title III. Like the  
19 Oregon wiretapping statute, federal law allows a civil cause of action for damages for violating Title  
20 III. *See* ORS 133.739; 18 USC §2520.

21 In *Joffe v. Google*, Google was sued for collecting data from unencrypted WiFi networks  
22 when photographing neighborhoods for its Street View feature.<sup>9</sup> *Joffe, supra*, at 922-23. When  
23 Google sent cars to photograph streets, the cars were equipped to with antennas and software that  
24

---

25 <sup>9</sup> Street View is a feature of Google Maps that shows images from a particular location on a map. It  
26 allows the user to see what a particular location looks like as if the person were standing in the street  
in front of the location.

1 collected data transmitted by WiFi networks in homes and businesses. *Id.* at 923. Google collected  
2 all data transmitted by any device connected to a network, including emails, usernames, passwords,  
3 videos and documents. *Id.* The issue in *Joffe* was whether Title III’s exception for “electronic  
4 communications [that are] readily accessible to the general public” applied to Google’s collection of  
5 this data. *Id.* at 926. The court found that the exception did not apply. *Id.* *Joffe* stands for the  
6 proposition that content of communications sent over WiFi are protected by federal law and cannot  
7 be intercepted without a court order. *Id.* By extension, data transmitted via WiFi signal are protected  
8 by Oregon law, and may not be interception without an order issued under ORS 133.724.

9 Detective Weaver intercepted the electronic communications coming from Mr. Simons’s  
10 computer that was in his home. He did so without first obtaining an order under ORS 133.724.  
11 Therefore, the data obtained by Det. Weaver was obtained in violation of ORS 133.724, and should  
12 be stricken from the search warrant affidavit and suppressed. *See McKee, supra*, at 99 (striking from  
13 a search warrant application information seized in violation of statute requiring a court order before  
14 obtaining bank records.)

15  
16 *2. Using a Packet-Sniffer to Locate Mr. Simons’s Computer in his Home by  
Intercepting His Data Violated 18 U.S.C. 2511*

17 Title III protects the privacy of our communications with one another by allowing  
18 wiretapping only when specific requirements are met. *United States v. Gonzalez, Inc.*, 412 F.3d  
19 1102, 1110 (9th Cir. 2005) (quoting S.Rep. No. 90–1097, at 66 (1968), reprinted in 1968  
20 U.S.C.C.A.N. 2122, 2153), *amended on denial of reh'g*, 437 F.3d 854 (9th Cir. 2006). Those seeing  
21 to lawfully intercept wire or oral communications must strictly adhere to the procedural  
22 requirements of Title III. *U.S. v. Kalustian*, 529 F.2d 585, 588 (9th Cir. 1975).

23 Title III generally prohibits the intentional interception of “any wire, oral or electronic  
24 communication.” 18 U.S.C. § 2511(1)(a). Information transmitted by a WiFi network are electronic  
25 communications within the meaning of Title III because, “Wi-Fi networks transmit information  
26 using radio waves (which are a type of electromagnetic radiation), and thus transmit ‘electronic

1 communications.” *Innovatio*, 886 F. Supp. 2d at 890. Although Title III’s definition of “electronic  
2 communication” exempts “any communication from a tracking device,” this exemption does not  
3 apply to packet sniffers. Tracking devices are defined as “an electronic or mechanical device which  
4 permits the tracking of the movement of a person or object.” 18 U.S.C. §§ 2510(12)(C), 3117(b).  
5 Packet sniffers do not intercept communication[s] from a tracking device: they intercept the content  
6 of internet communications, *see Joffe*, 746 F.3d at 923 (describing packet sniffer’s collection of  
7 “personal emails, usernames, passwords, videos, and documents” that people send over the internet).

8 While law enforcement’s primary use of the packet sniffer here was to locate and track Mr.  
9 Simons, they intercepted his communications to do so. Prohibited interception under Title III occurs  
10 “when the contents of [an electronic] communication are captured or redirected *in any way*.” *See*  
11 *Noel v. Hall*, 568 F.3d 743 (9th Cir. 2009) (internal quotations and citations omitted) (emphasis  
12 added). It should not matter whether they “[have] been recorded in a permanent medium . . . because  
13 that requirement is nowhere found in [Title III].” *See Innovatio*, 886 F. Supp. 2d at 892.

14 Lastly, as noted above, *Joffe* held that Title III’s exemption for “electronic communication[s]  
15 [that are] readily accessible to the general public,” 18 U.S.C. § 2511(2)(g)(i), “excludes payload data  
16 transmitted over a Wi-Fi network.” *Joffe*, 746 F.3d at 926.

17 In sum, Detective Weaver unlawfully intercepted Mr. Simons’s electronic communications  
18 with a packet sniffer, an internet wiretap, without obtaining permission from the court. *See*  
19 *Kalustian*, 529 F.2d at 588. The fruits of this unauthorized wiretap must be stricken from the warrant  
20 application and suppressed. 18 U.S.C. § 2518(10)(a).

21 //

22 //

23 //

24 //

25 //

26 //

3. *Using a Packet-Sniffer to Locate Mr. Simons's Computer in his Home Violated Article 1 Section 9 of the Oregon Constitution*

Using a computer and specialized software, police searched the inside of Mr. Simons's home for a particular computer without a warrant. The state has the burden of establishing that the search "did not violate a protected interest of the defendant." *State v. Tucker*, 330 Or 85, 89 (2000); see ORS 133.693(4).

Article 1, section 9 of the Oregon Constitution protects the privacy to which one has a right. *State v. Campbell*, 306 Or 157, 164 (1988) (citations omitted). To determine whether the government invaded a person's protected privacy interest the court considers, "whether the government's conduct would significantly impair an individual's interest in freedom from scrutiny, *i.e.*, his privacy." *State v. Carle*, 255 Or App 102, 107 (2014) (citations and internal quotations omitted). The "privacy protected by Article I, section 9 is the freedom from scrutiny as determined by social and legal norms of behavior, such as trespass laws and conventions against eavesdropping." *State v. Lien*, 364 Or 750, 760 (2000) (citations and internal quotations omitted).

In *Lien* the court considered whether a person retains a privacy interest in garbage in an opaque container left at the curb for regular pick up by the garbage company. The court weighed "general social norms of behavior," and whether "most Oregonians would consider their garbage to be private and deem it highly improper for others—curious neighbors, ex-spouses, employers, opponents in a lawsuit, journalists, and government officials \*\*\*to take away their garbage bin and scrutinize its contents." *Id.* at 761. In finding that the defendants retained an interest in their garbage—even after they left it at the curb—the court explained, "we recognize, given the realities of living in modern society, which is experiencing its own significant social and technological changes, that privacy norms exist notwithstanding some limited public exposure of information." *Id.* at 764.

A person has a privacy interest in the location of his belongings in his or her home. By using the packet sniffer, the police searched Mr. Simons's home for a particular item—IanAnderson-PC—without a warrant. Oregonians have a fundamental privacy right in the contents of our homes.

1 Detective Weaver was searching Mr. Simons’s house for a particular computer. But for the packet-  
2 sniffing software, he would not have been able to “see” inside Mr. Simons’s home.

3 Most Oregonians would be outraged to learn that the government was monitoring what kind  
4 of electronic devices were present in a home, and when they were being used. The suit in *Joffe* was  
5 class action lawsuit. People were aghast that Google was gathering information about them from  
6 their wireless networks, even if the data from their wireless networks was accessible outside of their  
7 homes.

8 Consider the response if a person looked out the window of his or her home and saw a police  
9 officer with a laptop and antenna walking up and down the sidewalk in front of that person’s home.  
10 Now consider that the police officer is intercepting all of the wireless data coming from all of the  
11 electronic devices in that home and inventorying the devices. People would be outraged that their  
12 electronic devices, devices upon which we rely for our day-to-day activities, could be tracked by the  
13 police without a warrant, without a court order or without probable cause. Put another way, people  
14 would be outraged to learn that the government can search our homes at any time of the day or night  
15 without a warrant, without probable cause and without our knowledge merely because we use  
16 internet-connected devices. Surely the Oregon Constitution protects us in our homes from such  
17 intrusions.

18 This case is not an instance akin to the police merely magnifying an image visible through an  
19 open window. *See State v. Louis*, 296 Or 57 (1983). The computer was not visible from the street.  
20 Nor is this case similar to obtaining text messages from the recipient’s phone. *See Carle, supra*.  
21 When looking for the computer in Mr. Simons’s house, Det. Weaver was not, at that time, searching  
22 information received by the wireless router at A&W. Rather, Det. Weaver was searching for  
23 transmissions from the computer in the house.

24 Nothing in the search warrant indicates that use of the public WiFi at the A&W was  
25 conditioned on consent for the police monitor, track and locate a user’s electronic devices in his or  
26 her home. If the terms of use accepted by the user of IanAnderson-PC contained such a broad

1 waiver, there is no averment of that in the warrant. Indeed, counsel is aware of no standard terms of  
2 use for free WiFi where the user consents to unrestricted monitoring by the police.

3 In attempting to locate IanAnderson-PC in Mr. Simons’s home, Det. Weaver conducted a  
4 warrantless search of Mr. Simons’s home without a warrant in violation of article 1, section 9 of the  
5 Oregon Constitution. The evidence obtained as a result of that search should be stricken from the  
6 search warrant affidavit and suppressed.

7  
8 *4. Using a Packet-Sniffer to Locate Mr. Simons’s Computer in his Home Violated  
the Fourth Amendment to the United States Constitution*

9 In recent years, the United States Supreme Court has repeatedly reexamined old Fourth  
10 Amendment doctrines grounded in the constraints of the physical world, finding in each instance that  
11 the realities of the digital age compel a different outcome. In *United States v. Jones* the Court held  
12 that 28 days of GPS tracking a vehicle required a warrant, despite the traditional rule that there is no  
13 expectation of privacy on public streets. *United States v. Jones*, 565 US 400 (2012). The Court  
14 determined that the tracking was a search because of the “unique attributes of GPS surveillance,”  
15 such as the ability to generate “a precise, comprehensive record of a person’s public movements that  
16 reflects a wealth of detail about her familial, political, professional, religious, and sexual  
17 associations.” *Id.* at 415 (Sotomayor J., concurring); *see also id.* at 429 (Alito, J., concurring).

18 Two years after *Jones*, the Court declined to extend lawful searches incident to arrest “to  
19 digital content on cell phones.” *Riley v. California*, 573 US 373, 386 (2014). The Court in *Riley*  
20 recognized that “[m]odern cell phones, as a category, implicate privacy concerns far beyond those  
21 implicated by the search of a cigarette pack, a wallet, or a purse.” *Id.* at 393. The Court explained  
22 that equating a typical physical search with a search of all data stored on a cell phone “is like saying  
23 a ride on horseback is materially indistinguishable from a flight to the moon.” *Id.*

24 //

25 //

1           Finally, in 2018, the Court held that tracking data of a cell phone collected in the normal  
2 course of business by the cell phone provider can only be obtained with a search warrant. *Carpenter*  
3 *v. United States*, \_\_ US \_\_, 138 S Ct 2206 (2018). In *Carpenter*, the Court declined to extend the so-  
4 called “third-party doctrine” to cell phone location data. For the last 40 years, the doctrine has meant  
5 that there is no reasonable expectation of privacy in personal information voluntarily shared with a  
6 third party such as a bank. See *United States v. Miller* 425 US 435 (1976); *Smith v. Maryland*, 442  
7 US 735 (1979). But in *Carpenter*, the Court declined to extend the rule to cell phone location records  
8 maintained by third-party service provider. Like GPS information in *Jones*, the Court found that  
9 such data “provides an all-encompassing record of the holder’s whereabouts” that “hold for many  
10 Americans the ‘privacies of life.’” *Carpenter, supra*, at 2217 quoting *Riley, supra*, at 403. In short,  
11 the Court’s message from *Jones, Riley, and Carpenter* is clear: when it comes to the Fourth  
12 Amendment, digital is different.

13           Keeping in mind the law as it applies to the portable computers that are cell phones, using a  
14 packet sniffer is a Fourth Amendment search for at least three reasons. First, in addition to  
15 intercepting communications data, packet sniffers can pinpoint the location of connected devices  
16 within constitutionally protected spaces, such a home, because it allows police to learn information  
17 about the interior of a space that they would have otherwise needed a warrant to enter. *Kyllo v.*  
18 *United States*, 533 US 27, 40 (2001); *United States v. Karo*, 468 US 706, 719 (1984).

19           Second, the Supreme Court has recently and repeatedly affirmed that individuals have a  
20 reasonable expectation of privacy in their computers, laptops, phones, and the information that they  
21 contain, and that the government’s capture of this information without a warrant violates the Fourth  
22 Amendment. See *Carpenter, supra*, at 2221; *Riley, supra*, at 403.

23           Finally, with a packet sniffer the government gathers the communications itself and some of  
24 the communications are modern-day papers and effects under the Fourth Amendment, so the third-  
25 party doctrine does not apply. See *Carpenter*, 138 S Ct at 2220; see *id.* at 2222 (citing *Warshak*, 631  
26 F3d 266, 283-88 (6th Cir. 2010); see *id.* at 2230 (Kennedy, J., dissenting).

1 Each of these reasons are addressed separately below.

2  
3 a. Using a Packet Sniffer to Intrude on a Constitutionally Protected  
4 Space is a Search

5 Packet sniffers gather information about constitutionally protected spaces, including the  
6 home, which is “presumptively unreasonable in the absence of a search warrant.” *Katz*, 389 U.S. at  
7 361. In our homes “*all* details are intimate details.” *Kyllo*, 533 US at 37 (2001); *see also id.* at 40  
8 (Recognizing that “the Fourth Amendment draws ‘a firm line at the entrance to the house’”) (citing  
9 *Payton v. New York*, 445 US 573, 590 (1980)); *Knotts*, 460 US 276, 282 (1983) (noting “the  
10 traditional expectation of privacy within a dwelling place”); *United States v. Karo*, 468 US 705, 715  
11 (1984) (stating that “[w]e cannot accept the Government’s contention that it should be completely  
12 free from the constraints of the Fourth Amendment to determine by means of an electronic device,  
13 without a warrant and without probable cause or reasonable suspicion, whether a particular article—  
14 or a person, for that matter—is in an individual’s home at a particular time”).

15 *Kyllo* and *Karo* are particularly instructive. In *Kyllo* the police used a device to measure  
16 infrared radiation coming from the defendant’s home. The police were trying to determine whether  
17 the defendants were using high-intensity heat lamps to grow marijuana at their home in Florence,  
18 Oregon. *Kyllo*, *supra* at 29. Infrared radiation is not visible to the naked eye. *Id.* at 30. The Court  
19 found that “obtaining by sense-enhancing technology any information regarding the interior of the  
20 home that could not otherwise have been obtained without physical intrusion into a constitutionally  
21 protected area constitutes as search where the technology in question is not in general public use.”  
*Id.* at 34.

22 In *Karo*, DEA agents placed tracking device, a beeper, on a cannister of ether. *Karo*, *supra*,  
23 at 708. The agents followed the cannister as the defendants moved it to and from various locations.  
24 *Id.* at 708-09. The final location was a home owned by one of the defendants. *Id.* at 711. A day after  
25 agents tracked the cannister to the defendant’s home, the agents confirmed that the cannister was in  
26 the home by using the tracking device. *Id.* The Court found that looking for the cannister in the



1 home using the beeper was a search that required a warrant. The Court reasoned that because the  
2 agents could not have simply entered the house without a warrant to confirm the presence of the  
3 cannister, the agents could not “surreptitiously employ[] an electronic device to obtain information  
4 that it could not have obtained by observation from outside the curtilage of the house.” *Id.* at 715.

5 Packet sniffers grant the government a significant new power to obtain information that it  
6 otherwise could not obtain by outside of the curtilage of a home. People compulsively carry cell  
7 phones and other internet-enabled devices, and these devices are almost always connected to the  
8 internet, because they can “display data stored on remote servers rather than on the device itself,”  
9 *Riley, supra*, at 397; *see also Carpenter, supra*, at 2218. To find a person or a device law  
10 enforcement need only use a packet sniffer to locate their WiFi-connected device. When law  
11 enforcement seeks to use new technology, courts have the important duty to “take the long view,  
12 from the original meaning of the Fourth Amendment forward.” *Kyllo, supra*, at 40. A packet sniffer  
13 should be seen as the kind of tool that “risks Government encroachment of the sort the Framers, after  
14 consulting the lessons of history, drafted the Fourth Amendment to prevent.” *Carpenter, supra*, at  
15 2223 citations and internal quotations omitted.

16 The invasive nature of a packet sniffer is made even more dangerous because the surveillance  
17 is “inescapable and automatic.” *See Id.* Internet-enabled devices will generally automatically connect  
18 to WiFi, unless a user takes affirmative steps to prevent it.<sup>10</sup> “Apart from disconnecting the [device]  
19 from the network, there is no way to avoid leaving behind a trail of location data” and internet  
20 communications. *Id.* at 2220. However, cell phones and other internet-enabled devices are “such a  
21 pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern  
22 society.” *See id.* (quoting *Riley*, 573 US at 385); *see also Innovatio, supra*, at 894 (noting the  
23 public’s “strong expectation of privacy in its communications on an unencrypted WiFi network.”) It  
24 is unreasonable to expect people to not use WiFi. Packet sniffers, in turn, operate on these

---

25  
26 <sup>10</sup> *See* section II(C), *supra*.

1 indispensable WiFi networks, making their surveillance “inescapable.” *See Carpenter, supra*, at  
2 2220.

3 When law enforcement uses a packet sniffer, it not only risks piercing the wall of one  
4 individual’s home, but of hundreds or thousands of homes, without anyone ever learning that their  
5 privacy was invaded. The sheer volume of users that might be captured by a packet sniffer search  
6 creates a high probability that the device will surveil an internet-enabled device inside a home “at the  
7 moment” it passes by. *See Joffe, supra*, at 923. This is far too expansive an invasion of the “sanctity  
8 of the home” or any other constitutionally protected area. *Kyllo, supra*, at 37.

9 *United States v. Norris* does not compel a different conclusion. No. 17-10354 at 12, 14 (9th  
10 Cir., Nov. 4, 2019) (holding that when an individual “gains access to the internet through the  
11 *unauthorized use* of a third-party’s password-protected router,” they do not have a reasonable  
12 expectation of privacy in “the signal strength of the MAC address emanating from outside his  
13 apartment.”) (emphasis added). The court reasoned that society is not prepared to recognize as  
14 reasonable a subjective expectation of privacy in the content of property obtained through  
15 unauthorized means.” *Id.* at 13 (citing *United States v. Caymen*, 404 F3d 1196, 1197-98 (9th Cir.  
16 2005)). Here, A&W’s WiFi was open to the public and not password-protected in any way.  
17 Furthermore, the Supreme Court’s decision in *Carpenter* was not decided until after briefing in  
18 *Norris* was almost complete, and not discussed by the three-judge panel in its opinion. Under  
19 *Carpenter*, Mr. Simons’ reasonable expectation of privacy includes the “trail of location data”  
20 resulting from his use of the WiFi. *See Carpenter, supra*, at 2220.

21 Detective Weaver’s use of a packet sniffer to search Mr. Simons’s home for a specific  
22 computer is effectively the same as searching for the canisters using a beeper. The detective could  
23 not have entered Mr. Simons’s home without a warrant to look for the computer. Similarly, using  
24 the packet sniffer was an unreasonable search, because Det. Weaver used an electronic device to  
25 obtain information that could not have obtained by standing outside of the curtilage of Mr. Simons’s  
26 home.

1                                    b. Using a Packet Sniffer to Intercept Communication Content and  
2                                    Metadata is a Search

3                    Intercepting the wireless communications from IanAnderson-PC itself was a search that  
4 required a warrant, because the content of the communications, like the content of cell phones,  
5 contain “a digital record of nearly every aspect of [a person’s] li[fe]—from the mundane to the  
6 intimate,” such as “Internet search and browsing history.” *See Riley, supra*, at 395. The  
7 government’s acquisition of the cell-site records is a search because of “the deeply revealing nature”  
8 of cell site location data, noting that “its depth, breadth, and comprehensive reach, and the  
9 inescapable and automatic nature of its collection.” *Carpenter, supra*, at 2223. The government’s use  
10 of a packet sniffer similarly collects personal information such as internet search and browsing  
11 history and should similarly demand Fourth Amendment protection. *See Riley, supra*, at 395.

12                    Prior to the internet age, in order to capture a person’s communications and learn  
13 comprehensive information about them, the government had to physically search their person,  
14 effects, and home. *See Riley, supra*, at 393-94 (discussing how “[m]ost people cannot lug around  
15 every piece of mail they have received for the past several months, every picture they have taken, or  
16 every book or article they have read.”). In contrast, by using a packet sniffer to monitor an internet-  
17 enabled device, law enforcement can capture all of this information when it is communicated online.  
18 *See id.* at 394 (acknowledging that “[t]he sum of an individual’s private life can be reconstructed  
19 through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be  
20 said of a photograph or two of loved ones tucked into a wallet.”) As the Supreme Court has  
21 acknowledged with regard to cell phones, it is commonplace for this information to be  
22 communicated online (and thus vulnerable to packet sniffing). *See id.* at 397 (discussing the  
23 “increasing frequency” of cloud computing on cell phones, which is “the capacity of Internet-  
24 connected devices to display data stored on remote servers rather than on the device itself.”).  
25 Moreover, the Court noted that “a cell phone’s capacity allows even just one type of information to  
26 convey far more than previously possible.” *Id.* at 394. E-mails, in particular, can contain an

1 individual’s “entire business and personal life.” *United States v. Warshak*, 631 F3d 266, 284 (6th  
2 Cir. 2010).

3 The government’s use of a packet sniffer in this case amounts to a “dragnet-type law  
4 enforcement practice[]” that the Court feared in *Knotts*, sweeping up the internet communications of  
5 all internet-enabled devices in its path in the hopes of finding one lead. *Knotts, supra*, at 284. The  
6 Court has always been “careful to distinguish between [] rudimentary tracking . . . and more  
7 sweeping modes of surveillance,” *Carpenter, supra*, at 2215 (citing *Knotts*, 460 U.S. at 284), in  
8 deciding whether a search is entitled to heightened protection under the Fourth Amendment. A  
9 packet sniffer falls on the sweeping end of this spectrum due to its capability to surveil everyone on  
10 a wireless network. *See Ybarra v. Illinois*, 444 US 85, 86 (1979) (noting that “a person’s mere  
11 propinquity to others independently suspected of criminal activity does not, without more, give rise  
12 to probable cause to search that person.”); *Knotts, supra*, at 284 (stating that a dragnet search would  
13 be held unconstitutional).

14 Regardless of how a packet sniffer is configured in a particular case, the Fourth Amendment  
15 requires that a search has precise limits established by a warrant supported by probable cause. *See*  
16 *Katz, supra*, at 356. It is not enough for government agents to voluntarily “confine[] their  
17 surveillance.” *Id.* at 354, 356-57. The Fourth Amendment requires meaningful judicial oversight  
18 involving the disclosure of the government’s exact plan for the length of time and location it plans to  
19 use the device, and how it plans to minimize the collection and retention of non-targeted individuals’  
20 internet communications.

21  
22 c. The Third-Party Doctrine Does Not Apply to Use of a Packet  
Sniffer

23 The third-party doctrine, defines a reduced expectation of privacy in items held by third  
24 parties, does not apply to the government’s use of a packet sniffer for two reasons. First, the  
25 government obtains location information and internet communication directly from the device user,  
26

1 not from a third party. And second, the doctrine does not apply to internet communications such as  
2 emails that are modern-day ‘papers’ or ‘effects’ under the Fourth Amendment.

3 Even before the Supreme Court clarified the scope of the third-party doctrine to digital-age  
4 searches in *Carpenter*, the third party doctrine could not apply to the use of a packet sniffer device  
5 because the government obtains the information directly from the tracked individual(s), as opposed  
6 to through a third party. The third-party doctrine may apply when the government makes a “garden-  
7 variety request for information” that is “created and maintained by the [third party].” *See Carpenter*,  
8 *supra*, at 2219. But with a packet sniffer, unlike a phone company’s network transiting dialed phone  
9 numbers in *Smith* or where information is “exposed to [a third-party] in the ordinary course of  
10 business,” in *Miller*, law enforcement is obtaining internet communications and local information  
11 directly from Mr. Simons’ device itself. When the police seek information by directly interacting  
12 with a suspect’s device, no third party is involved, so “in no meaningful sense does the user  
13 voluntarily ‘assume[] the risk’ of turning over a comprehensive dossier of his physical movements”  
14 or internet communications. *See Carpenter, supra*, at 2220 (citing *Smith, supra*, at 745).

15 Second, when device users communicate to the internet, they are sharing confidential and  
16 personal content, not creating ordinary business records. The Court has cautioned against  
17 “mechanically applying the third-party doctrine” to situations involving new technology and  
18 information. *Carpenter, supra*, at 2219. Rather, courts must “consider[] ‘the nature of the particular  
19 documents sought’ to determine whether ‘there is a legitimate expectation of privacy concerning  
20 their contents.’” *Id.* (quoting *Miller, supra*, at 442). As described above, the internet communications  
21 that law enforcement can capture with a packet sniffer are “deeply revealing” in fundamentally  
22 different ways than pre-digital information. *Id.* at 2223. Both the majority and Justice Kennedy’s  
23 dissent in *Carpenter* favorably cited *Warshak* for the proposition that “modern-day equivalents of an  
24 individual’s own ‘papers’ and ‘effects,’ even when those papers or effects are held by a third party”  
25 present “a sensible exception” to the third-party doctrine. *Id.* at 2222 (citing *Warshak, supra*, at 283-  
26 288); *id.* at 2230 (Kennedy, J., dissenting). E-mail, for example, “is the technological scion of

1 tangible mail” and it would “defy common sense to afford emails lesser Fourth Amendment  
2 protection.” *Warshak, supra*, at 285-86. In sum, “[t]here is a world of difference between the limited  
3 types of personal information addressed in *Smith and Miller*” and the internet communications that  
4 law enforcement can acquire with a packet sniffer, and this Court should decline to create “a  
5 significant extension of [the third-party doctrine]” to this information. *See Carpenter, supra*, at 2219.

6  
7 d. Detective Weaver’s Use of the Packet Sniffer was a Search of  
Mr. Simons

8 The police searched Mr. Simons when they used the Kismet packet sniffer to collect his  
9 internet communications and locate him inside his home. “There was nothing ... that would point the  
10 finger at [Mr. Simons]” by linking him to the suspected device, so they decided they would “have to  
11 try to track him.” Exhibit B at 6. In doing so, they violated the “sanctity of [his] home,” *see Kyllo,*  
12 *supra*, at 37. Because Det. Weaver did not have a warrant, this search was presumptively  
13 unreasonable. *See Katz, supra*, at 361. The packet sniffer use by Det. Weaver was precise enough to  
14 locate Mr. Simons’ device in the south part of his home without having to “visually track [him] from  
15 some starting location,” *see Jones v. United States*, 168 A3d 703, 714 (DC 2017)(finding that using a  
16 cell-site simulator, known as a StingRay device, was a search under the Fourth Amendment and  
17 required a warrant). The mere fact that the police monitored his activities inside his home – his use  
18 of WiFi – was an intrusion. The police monitored the packets being transmitted by every device on  
19 the network in order to identify the suspect device, capturing the “deeply revealing” information that  
20 is often shared over the internet. Det. Weaver admitted that they observed the content of the real-  
21 time internet browsing by the suspect device, violating Mr. Simons’ reasonable expectation of  
22 privacy. Exhibit B at 7.

23 The packet sniffer captured the packets of not just Mr. Simons but everyone on the WiFi  
24 network. As Det. Weaver described in his affidavit, the WiFi network was easily accessible from  
25 Mr. Simons’s street, which is 140 yards from the A&W. Exhibit A at 19. While Weaver and Larsen  
26 were moving from place to place with the packet sniffer, eventually reaching Mr. Simons’ street,

1 they potentially invaded the “sanctity” of many people’s homes. *See Kyllo, supra*, at 37. Because  
2 internet-enabled devices, especially home computers, may be used by multiple people, there is an  
3 additional multiplier to how many bystanders may have been swept up. Even if Weaver and Larsen  
4 confined their surveillance by configuring the packet sniffer to not capture and display every packet,  
5 these precise limits were not established in advance by a warrant, as required by the Fourth  
6 Amendment. *See Katz, supra*, at 356. This kind of tool risks Government encroachment on the  
7 bounds of the Fourth Amendment. *See Carpenter, supra*, at 2223.

8 The third-party doctrine does not apply here because Weaver and Larsen captured these  
9 packets directly from WiFi users’ devices, not from a third party. The content of Mr. Simons’  
10 device’s internet browsing, for example, was intercepted by law enforcement before it reached the  
11 router, much less the third-party ISP, so “in no meaningful sense [did Mr. Simons] voluntarily  
12 ‘assume[] the risk’ of turning over a comprehensive dossier of his physical movements” or internet  
13 communications. *See Id.* at 2220 (citing *Smith*, 442 U.S. at 745).

14  
15 e. Using a Packet Sniffer Requires a Warrant based on Probable Cause

16 When the police violate someone’s reasonable expectation of privacy by searching them,  
17 they generally must first get a warrant based on probable cause. *Id.* (holding that “a warrant is  
18 required . . . where the suspect has a legitimate privacy interest in the records”); *Riley, supra*, at 2493  
19 (citing *Coolidge v. New Hampshire*, 403 U.S. at 481) (explaining that “[o]ur cases have historically  
20 recognized that the warrant requirement is ‘an important working part of our machinery of  
21 government,’ not merely ‘an inconvenience to be somehow ‘weighed’ against the claims of policy  
22 efficiency”’). Since none of the recognized exceptions to the warrant requirement apply here, the  
23 government’s failure to get a warrant requires suppression of the fruits of the unconstitutional  
24 search.

25 When the government uses new technology with new capabilities, it is critical that courts be  
26 able to exercise their constitutional oversight function through, at minimum, the requirement of a



1 warrant. *Cf. Kyllo, supra*, at 34 (holding that “obtaining by sense-enhancing technology any  
2 information regarding the interior of the home that could not otherwise have been obtained without  
3 physical ‘intrusion into a constitutionally protected area,’ constitutes a search—at least where (*as*  
4 *here*) the technology in question is not in general public use.”) (internal citations omitted) (emphasis  
5 added); *Carpenter, supra*, at 2223 (citing *Olmstead v. United States*, 277 US 438, 473–74 (1928)  
6 (Brandeis, J., dissenting)) (concluding that “the Court is obligated—as ‘[s]ubtler and more far-  
7 reaching means of invading privacy have become available to the Government’—to ensure that the  
8 ‘progress of science’ does not erode Fourth Amendment protections”).

9  
10 f. The Good Faith Exception Should Not Apply to the  
Government’s Warrantless Use of a Packet Sniffer.

11 The government knew or should have known that a packet sniffer raises unique privacy  
12 concerns that at minimum require a warrant. By failing to seek judicial authorization to use the  
13 device in this manner, the government prevented the court from exercising its constitutional  
14 oversight function, and the good-faith exception should not apply. This conclusion is bolstered by  
15 the Court’s recent holdings in *Riley* and *Carpenter*. Both cases emphasize the general principle that  
16 precise electronic location tracking of this type requires a warrant because it intrudes on reasonable  
17 expectations of privacy. *Carpenter, supra*, at 2217 (explaining, “[w]hether the Government employs  
18 its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an  
19 individual maintains a legitimate expectation of privacy in the record of his physical movements as  
20 captured through CSLI”); *Riley, supra*, at 2490 (noting Fourth Amendment implications of cell  
21 phone location data that can “reconstruct someone’s specific movements down to the minute, not  
22 only about town but also within a particular building”); *see also United States v. Jones, supra*, at 429  
23 (Alito, J., concurring) (“[T]he use of longer term GPS monitoring in investigations of most offenses  
24 impinges on expectations of privacy.”)

25 Here, the police failed to get a warrant to use a packet sniffer despite *Carpenter* having been  
26 decided a year previously and *Riley* five years previously. *See Davis v. US*, 564 U.S. 229, 240



1 (2011)(holding that the exclusionary rule does not apply when the police “acted in *strict compliance*  
2 *with binding precedent*”) (emphasis added). These cases should have alerted the government to the  
3 privacy interests at stake when it employs modern technology that permits it to track an individual  
4 extensively, precisely, and within the confines of constitutionally-protected spaces, and monitor their  
5 communications. When the government has engaged in such intrusive searches, courts have  
6 repeatedly given the same response: “get a warrant.” *Carpenter, supra*, at 2221; *Riley, supra*, at  
7 2495.

8  
9 B. Without the Location of IanAnderson-PC, the Warrant Lacked Probable Cause

10 A warrant is supported by probable cause when “the facts set out in the warrant lead a  
11 reasonable person to believe that things subject to seizure will probably be found in the location to  
12 be searched.” *State v. Goodman*, 348 Or 318, 325 (1999).

13 Without the location of IanAnderson-PC, the search warrant affidavit contained the following  
14 information: that a computer known as IanAnderson-PC was accessing websites containing child  
15 pornography; that the computer was purchased in 2009 by someone other than the defendant; that  
16 the purchaser of the computer told the police that he gave the computer to Mr. Simons, but that he  
17 had not seen Mr. Simons in several years; that Mr. Simons was associated with a residence near the  
18 A&W restaurant, and been associated with it for 11 months prior to obtaining the search warrant.

19 What is not included in the search warrant affidavit is that when police searched Mr.  
20 Thompson’s residence, they found firearms. Mr. Thompson is a felon and may not possess firearms.  
21 Police also failed to include in the search warrant affidavit that when Mr. Thompson spoke to them,  
22 he was in custody on this open firearms possession case, and may have been expecting a benefit in  
23 his current criminal case in exchange for his information to Det. Weaver.

24 Once the information obtained using the packet-sniffer is stricken, the affidavit now lacks Mr.  
25 Simons’s possession of the computer during the time the computer was accessing the websites that  
26 contain child pornography. At the time of the warrant, IanAnderson-PC was 10 years old, and had

1 been given to Mr. Simons at least a few years before. There is no evidence that Mr. Simons still  
2 owned the laptop known as IanAnderson-PC. Indeed, Det. Weaver testified as much to the grand  
3 jury: “There was nothing ... that would point the finger at [Mr. Simons]” by linking him to the  
4 suspected device, so they decided they would “have to try to track him.” Exhibit B at 6.

5 Without tracking the computer to the inside of Mr. Simons’s home, there is insufficient  
6 evidence linking that computer to Mr. Simons and his residence. According to the affidavit, Mr.  
7 Simons must have received the computer at least a few years prior to the application of the search  
8 warrant, because Mr. Thomas said that he had not seen Mr. Simons in a few years. In addition,  
9 according to Mr. Thomas, Mr. Simons was living in Westfir, not in Oakridge, when he received the  
10 computer. The police needed to link the computer to Mr. Simons at his residence in Oakridge before  
11 obtaining the warrant for Mr. Simons’s home, car, person and effects.

12  
13 C. Tracking the Internet Browsing History of Mr. Simons’s PC by Ken Sanders Was Illegal,  
14 because it was Done at the Direction of the Police and Without a Warrant, and Should be  
15 Stricken from the Warrant and Suppressed.

16 The burden is on the state to justify a warrantless search under article 1, section 9 of the  
17 Oregon Constitution. The internet browsing history of IanAnderson-PC and another Android device  
18 was collected by Mr. Sanders and given to the police without a warrant. The burden is on the state  
19 to justify this warrantless search.

20 1. *Mr. Sanders was Working as an Agent of the Police within the Meaning of Article*  
21 *1, section 9*

22 To determine whether a private actor is working on behalf of the government such that article  
23 1, section 9 protections apply, courts consider whether the private actor had an agency relationship  
24 with the government agent. *State v. Sines*, 359 Or 41, 59 (2016) The court in *Sines* noted:

25 “situations can and do arise in which a private citizens’ conduct in pursuing  
26 his or own search and seizure may become so intertwined with the conduct  
of a state actor that the private citizen’s actions are essentially those of the  
state and should be subject to constitutional restrictions on state searches  
and seizures.”

*Id.* at 50.

1           When Mr. Sanders first noticed evidence that someone was accessing child pornography  
2 using the A&W WiFi, he may not have been working for the police. However, after his contact with  
3 Officer Larsen, Mr. Sanders intercepted the entire internet browsing history of IanAnderson-PC for  
4 over 11 months. According to the discovery in this case, the intercepted browsing history contained  
5 over 200,000 contacts with web sites. *See* Declaration of Counsel at 2. Many of the websites  
6 accessed including banking and other private activities. *Id.* Because the firewall was configured to  
7 notify Officer Larsen of certain activity conducted with IanAnderson-PC, it is reasonable to infer  
8 that Mr. Sanders was collecting all of the internet data from IanAnderson-PC at the behest of the  
9 police.

10           Finally, and significantly, Detective Weaver testified to the grand jury that “they were  
11 keeping track for us of every website he was going to...” Exhibit B at 6. Mr. Sanders was working  
12 for the police.

13  
14                           2. *Mr. Sanders was Working as an Agent of the Police within the Meaning of the  
                                  Fourth Amendment*

15           The Fourth Amendment “was intended as a restraint upon the activities of sovereign  
16 authority,” *Burdeau v. McDowell*, 256 US 465, 475 (1921), which includes “protect[ion] against [...]”  
17 intrusions [by a private party] if the private party acted as an instrument or agent of the  
18 Government.” *Skinner v. Ry. Labor Executives’ Ass’n*, 489 US 602, 614.

19           The Ninth Circuit has established a two-part test “for determining whether a private  
20 individual is acting as a governmental instrument or agent for Fourth Amendment purposes.” *United*  
21 *States v. Reed*, 15 F3d 928, 931 (9th Cir. 1994). A court must determine: “(1) whether the  
22 government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing  
23 the search intended to assist law enforcement efforts or further his own ends.” *Id.* at 931 (citing  
24 *United States v. Miller*, 688 F2d 652, 657 (9th Cir.1982)). The private actor need not have been  
25 compelled by the police to perform the search. *Skinner, supra*, at 614-15. The idea to conduct the  
26

1 search did not have to come from the police. *Lustig v. United States*, 338 US 74, 79 (1949). Rather,  
2 the police engaged in the search if the officer “had a hand in it.” *Id.* For the second part of the test,  
3 “a private carrier's interest in preventing criminal activity [is] not a legitimate independent  
4 motivation.” *Reed*, 15 F3d at 932 (citing *United States v. Walther*, 652 F2d 788, 792 (9th Cir.1981).  
5 In other words, there must be a “legitimate motive *other than crime prevention.*” *Id.* at 932  
6 (emphasis in original).

7 Here, Mr. Sanders acted as a government agent. Officer Larsen met with Sanders on July 2,  
8 2018. Three days after that meeting, Off. Larsen began receiving emails at his police email address  
9 from the Firewall with alerts describing alleged “Child Abuse Images.” Declaration of Counsel at 3.  
10 Officer Larsen received emails from the Firewall over the course of a year. Officer Larsen’s email  
11 address was not available publicly. Officer Larsen “personally navigated” through the monitored  
12 internet browsing history, Exhibit A at 33.

13 Second, Mr. Sanders performed the search to “assist law enforcement efforts.” *See Reed*,  
14 *supra*, at 931. The only action he configured the Firewall to take upon detecting the alleged “Child  
15 Abuse Images” was to alert Off. Larsen. Even if Off. Larsen “ha[d] not compelled” Mr. Sanders to  
16 do so and Mr. Sanders himself wished to “prevent[] criminal activity,” this would still qualify as  
17 state action. *See Skinner, supra*, at 614-15; *Reed, supra*, at 932. If Mr. Sanders had a different  
18 motive, such as protecting the WiFi network from illegal or dangerous material, he would have taken  
19 appropriate action, such as blocking access to the material or by the suspected users. He did not. In  
20 fact, he did the opposite – Mr. Sanders knowingly allowed the access to continue for almost one  
21 year, apparently so that Off. Larsen could monitor it. Mr. Sanders acted to assist Larsen’s  
22 investigation, and thus acted as a government agent.

3. *Without the Information from the Browsing History of IanAnderson-PC, the Warrant is not Supported by Probable Cause*

Mr. Sanders spoke to Off. Larson for the first time in June of 2018. Without the browsing history of that PC reviewed by Officer Larson and by Det. Weaver, there was no reason to believe that there would be contraband on a computer one year after Mr. Sanders's initial contact with the police.

**IV. Conclusion**

For the above-stated reasons, defendant Randall Simons respectfully request that the court controvert the warrant, and suppress the evidence seized pursuant to the warrant, in addition to suppressing all of the intercepted web activity obtained prior to the search warrant.

DATED: February 12, 2020

Respectfully Submitted,  
ROSALIND MANSON LEE, LLC

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

1                                   **IN THE CIRCUIT COURT FOR THE STATE OF**  
2                                   **OREGON FOR LANE COUNTY**

3   **STATE OF OREGON**                                    )  
4    ) **ss.**            **SEARCH WARRANT**  
5   **County of Lane**                                    )

6  
7   To any police officer, greetings:

8           Information on oath having this day been laid before me that evidence of the  
9   crimes of Encouraging Child Sexual Abuse in the First, Second and Third Degree  
10   (ORS 163.684, 163.686, and 163.687), and other crimes of a sexual nature involving  
11   children committed in Lane County, Oregon to wit:

- 12       • A Toshiba brand Satellite laptop, model L505-S6951
- 13       • Computer records, documents, and materials, including computer towers  
14       (desktop) and notebook computers (laptops); tablets; cellular phones or other  
15       electronic devices capable of accessing the internet via wireless or cellular  
16       signal and running mobile applications; commercial software and hardware;  
17       computer disks; disk drives; solid state flash drives; computer printers;  
18       modems; tape drives; disk application programs; data disks; system disk  
19       operating systems; magnetic media floppy disks; tape systems and hard  
20       drives and other computer related operation equipment; in addition to  
21       computer photographs, slides or other equipment capable of storing digital  
22       images, and all system and user sign-on password codes.
- 23       • Any image or movie file containing or displaying child sexual abuse contained  
24       within any media storage device. To include any computer media storage  
25       device, electronic device, video tape, CD/DVD, and/or any other media

1 storage including but not limited to thumb drives, SD cards, I devices,  
2 cameras, digital cameras, and cellular phones.

- 3 • Any digital artifacts showing the connection to or use of the wireless network  
4 association with the A & W restaurant in Oakridge, Lane County, Oregon,  
5 between July 2, 2018 and June 25, 2019.
- 6 • Any and all diaries, notebooks, notes, writings, documents, day-planners and  
7 any other records reflecting activities indicating the sexual abuse of children.
- 8 • Communications related to the acquiring and trading of sexually explicit  
9 images of children between July 2, 2018, and June 25, 2019.
- 10 • Any evidence related to ownership, control, or use of residence, storage  
11 facilities, computer system(s), media files, programs, telephone number, and  
12 Internet accounts.
- 13 • Any documentation, written or electronic, showing the use of, possession of,  
14 or affiliation with any file-sharing or storage applications.
- 15 • Any and all documents tending to show the occupancy of 47816 Highway 58  
16 Unit #1 Oakridge, Lane County, Oregon including personal identification, bills,  
17 receipts, canceled mail, utility bills, rent receipts and bank statements.
- 18 • The biometric information for Randall Dewitt Simons (date of birth October 13,  
19 1952) to include fingerprint read through device fingerprint sensor, iris or  
20 retinal scans, and facial recognition images collected through device digital  
21 camera.

22  
23 is currently located in the real property of **47816 Highway 58 Unit #1 Oakridge,**  
24 **Lane County, Oregon** including the curtilage, any associated storage or  
25 outbuildings, in a gray **Dodge Journey (VIN 3D4GG57VX9T551841)** baring

1 **Oregon license "N0LRJ"** registered to Randall Dewitt Simons (date of birth  
2 October 13, 1952) and on the person of **Randall Dewitt Simons (date of birth**  
3 **October 13, 1952)** regardless of their location in the state of Oregon.

4 **Real Property Description:**

5 The involved property of 47816 Highway 58 Oakridge, Lane County, Oregon  
6 is a series of multiple dwellings located at the southeast corner of Rock St and  
7 Highway 58. The main building is a single story, tan building with brown trim that  
8 contains three residences. The numbers "47816" are affixed to the north side of this  
9 building in black numbers on gold colored rectangles. Unit #1 is the northern most  
10 residence, with the main door facing to the west. The number "1" is located on the  
11 wall just to the left of this northernmost door. No outbuildings or storage for the  
12 apartment is visible from the road.

13 **Vehicle Description:**

14 A gray Dodge Journey (VIN 3D4GG57VX9T551841) bearing Oregon license  
15 "N0LRJ" registered to Randall Dewitt Simons (date of birth October 13, 1952).

16 **Person To Be Searched:**

17 Randall Dewitt Simons (date of birth October 13, 1952).

18 **YOU ARE HEREBY COMMANDED** to search the above-described residence,  
19 including curtilage and associated storage buildings, at **47816 Highway 58 Unit #1**  
20 **Oakridge, Lane County, Oregon.** You are also command to search the gray  
21 Dodge Journey (VIN 3D4GG57VX9T551841) bearing Oregon license "N0LRJ"  
22 registered to Randall Dewitt Simons (date of birth October 13, 1952) and the person  
23 Randall Dewitt Simons (date of birth October 13, 1952) regardless of their location in  
24 the State of Oregon. You are further commanded to search and seize the evidence  
25 listed of the above said crimes.



1 You are further authorized to employ any qualified forensic technician, analyst  
2 or other forensic expert you deem necessary to analyze the evidence you seize.

3 You are also further authorized to employ any forensically sound process to analyze  
4 such evidence you seize in this case.

5 You are further authorized to utilize, by means reasonably necessary, the  
6 biometric information for Randall Dewitt Simons (date of birth October 13, 1952) to  
7 unlock digital devices. This biometric information can include a fingerprint read  
8 through a device fingerprint sensor, iris or retinal scans, and facial recognition  
9 images collected through a device digital camera.

10 Return of this warrant and an inventory of the item(s) seized shall be made to  
11 me at my office in the Lane County Courthouse, Eugene, Oregon, no later than five  
12 days following the execution of this warrant.

13  
14 <sup>du</sup>  
(X) This warrant to be executed between 7:00 A.M. and 10:00 P.M. within five  
15 days.

16 Dated this 27 day of June, 2019 at 1:30 a.m./p.m.

17  
18 

19 Circuit Court Judge  
D. Velure

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

IN THE CIRCUIT COURT FOR THE STATE OF  
OREGON FOR LANE COUNTY

STATE OF OREGON                    )  
  ) ss. AFFIDAVIT FOR SEARCH WARRANT  
County of Lane                     )

I, Robert Weaver, being first duly sworn on oath, do depose and say that I am employed as a police officer in the State of Oregon by the City of Springfield and have been so employed for over twenty years. I am currently assigned to the Investigative Services Bureau division of the Springfield Police Department working as the Digital Forensic Investigator. As part of my responsibilities, I investigate a wide variety of crimes, which includes Encouraging Child Sexual Abuse. I have received specific training in the investigation of crimes involving digital evidence including classroom training by experts in the field and on the job training by experienced detectives. I am a Certified Computer Examiner (CCE certification) through the International Society of Forensic Computer Examiners and also a Certified Forensic Computer Examiner (CFCE certification) through the International Association of Computer Investigative Specialist. I hold professional Information Technology (IT) certifications through CompTIA for digital equipment (A+ Certification), networking (Network+ certification), as well as digital security and encryption (Security+ certification). I have attended over 500 hours of digital forensics training to include training on data extraction and analysis for cellular devices, more specifically cellular devices containing Android operating systems and Apple devices running iOS operating systems. I am a duly sworn peace officer as defined in ORS 133.005. I am authorized pursuant to ORS 133.545, to apply for

1 search warrants and hereby make application to this Court for a search warrant as  
2 further described below.

3 I am familiar with the information contained in this affidavit because I have  
4 reviewed relevant documents and other evidence related to this case. Because this  
5 affidavit is being submitted for the limited purpose of establishing probable cause to  
6 search/obtain and seize specific evidence, I have not included herein the details of  
7 every aspect of the investigation. Where actions, conversations and statements of  
8 others are related herein, they are related in substance and in part except where  
9 otherwise indicated.

10  
11 **TRAINING AND EXPERIENCE:**

12 That based on my experience and training, I know that people who are  
13 sexually attracted to children, and engage in sexual acts with children, often  
14 maintain and collect photos, which in today's age of technology, are commonly  
15 stored on memory devices such as personal computers, laptop computers, tablets,  
16 cellular phones, digital media storage, CDs, DVDs, flash drives, spare hard drives,  
17 etc. In addition, based on my experience and training, I've learned that suspects  
18 attracted to children also maintain collections of hard copy photos as well as books,  
19 magazines, articles, and other writings on the subject of sexual activity. That these  
20 books and materials on the topics of human sexuality and sexual education may  
21 consist of sex manuals discussing or showing various sexual acts, positions and/or  
22 sexual activities. That these materials are used for the personal sexual arousal on  
23 the part of the offender, particularly, when naked children are shown or depicted  
24 within the materials.

1 That based on my experience and training, I know that the offender will often  
2 store/keep these materials within close proximity in order to ensure they're readily  
3 available for viewing and use. That an offender's residence, vehicle and/or person  
4 would be the most convenient and likely place where an offender would keep these  
5 materials in order to keep them readily accessible and to ensure that they are not  
6 discovered, lost, or removed by someone else. That the offender values these  
7 materials and as such often keeps such digital storage media on their person in  
8 order to keep the pornography readily accessible and to ensure they are not  
9 discovered, lost, or removed by someone else.

10 That based on my experience and training regarding persons who have an  
11 expressed interest in the sexual molestation of children and child pornographers,  
12 your affiant knows that such suspects are collectors of child pornography and value  
13 their material as prized possessions and that suspects are very secretive about their  
14 collections of child pornography. That suspects rarely, if ever, dispose of child  
15 pornography they have acquired, as it is relatively difficult to obtain. I have also  
16 learned through my experience and training that suspects will often keep their child  
17 pornography at their residence, on their person, or at a secure location convenient to  
18 them to ensure that the material is readily available and protected. I also know that  
19 persons predisposed to collecting child pornography will frequently maintain  
20 collections of visual depictions of adults made to appear as minors engaged in  
21 sexually explicit conduct as a surrogate of child pornography. I also know that film  
22 negatives as well as photo sets, slides, video tapes and computer software, are  
23 offered for sale and exchanged domestically and internationally along with  
24 magazines and films.  
25

1 That based on my experience and training concerning individuals who are  
2 interested in the sexual molestation and/or exploitation of minors engaged in  
3 sexually explicit conduct will often correspond with others who express the same  
4 interest. That as a result of these contacts, these persons will often retain  
5 correspondence received and that some of these persons may keep records e.g.  
6 card files, computer files, digital application messages, address books, diaries,  
7 notebooks, and/or electronic communications (emails and application messaging) of  
8 such correspondence. I have also found that persons who obtain and/or disseminate  
9 child pornography through the United States Mail and/or other common carrier  
10 and/or computer mediums, will frequently retain advertisements and list of sources  
11 of such material;

12 That based on my experience and training regarding criminal investigations, I  
13 know that corroborating facts asserted by a reporting party is important in a criminal  
14 prosecution, and that locating network activity and sexually explicit evidence  
15 involving minors on a suspect's electronic devices, and any other digital storage  
16 media, would tend to corroborate facts asserted by the complainant.

17 I know in any investigation and prosecution it is important to establish that the  
18 suspect had the opportunity to be at the location of the crime at the times described.  
19 This can be established in a variety of ways. One way would be via location,  
20 network data and other data stored within a suspect's cell phone, computer and/or  
21 tablet that corroborates and matches the suspect's activity presented by the  
22 complainant.

23 That based on my experience and training, preferential child molesters,  
24 pedophiles and child pornographers receive sexual gratification, stimulation and  
25 satisfaction from actual physical contact with children, from fantasies they have

1 viewing children engaged in sexual activity or in sexually suggestive poses (whether  
2 in person, photographs, or other visual media), and from literature describing such  
3 activity.

4 That I am a Certified Computer Examiner through the International Society of  
5 Forensic Computer Examiners and a Certified Forensic Computer Examiner with the  
6 International Association of Computer Investigative Specialist. I have hundreds of  
7 hours of training in information technology, electronics, digital forensics for  
8 computers and cellular phones. I have also forensically processed almost a  
9 thousand digital devices.

10 That I know based on training and experience that a wide assortment of data  
11 is commonly stored on memory devices such as personal computers, laptop  
12 computers, tablets, cellular phones, digital media storage, CDs, DVDs, flash drives,  
13 spare hard drives, etc. This data can include digital artifacts of identifying  
14 information of the owner of the device, internet activity, digital photographs, and  
15 correspondence with others including, messaging and chat application data, emails,  
16 text messages and call logs. Network information, such as router, IP addresses,  
17 and network Service Set Identifiers (SSID or network names) is often stored on  
18 digital devices. That networking devices, such as routers, modems and other items  
19 that connect to the internet can maintain usage logs and user information.

20 That I know based on experience and training concerning searches and  
21 seizures of evidence from computers commonly requires law enforcement to seize  
22 all computer items (hardware, software, digital storage devices and media, and  
23 instructions) to be processed at a later date by a qualified computer expert in a  
24 laboratory or other controlled environment. This is almost always true because  
25 computer storage devices (hard disks, diskettes, data tapes, laser disks, compact

1 flash drives, thumb drives, SD disks, and other removable media used in cellular  
2 phones, hand held computers, laptop computers, tablets, personal digital assistant  
3 (PDA) devices and cameras) can store the equivalent of millions of pages of  
4 information. These small devices are commonly carried on the person using these  
5 devices. This is especially when the user wants to conceal criminal evidence.  
6 Further, consumers of this type of contraband often stores files in random order with  
7 deceptive file names. This requires searching authorities to examine all of the  
8 stored data to determine whether it is included in the warrant. This sorting process  
9 can take weeks or months depending on the volume of data stored and it would be  
10 impractical to attempt this kind of data search except for within a digital forensics  
11 laboratory. Searching computer systems, cellular phones and other digital storage  
12 devices for criminal evidence is a highly technical process requiring expert skill and  
13 a properly controlled environment. The vast array of computer hardware and  
14 software available requires even computer experts to specialize in some systems  
15 and applications, so it is difficult to know before a search which expert(s) should  
16 analyze the system and its data. The search of a computer system is an exacting  
17 scientific procedure which is designed to protect the integrity of the evidence and to  
18 recover even "hidden," erased, compressed, password-protected, or encrypted files.  
19 Since computer evidence is extremely vulnerable to tampering or destruction (either  
20 from external sources or from destructive codes imbedded in the system as a "booby  
21 trap"), the controlled environment of a laboratory is essential to its complete and  
22 accurate analysis;

23 That I know based on his training and experience processing digital evidence  
24 that digital artifacts (including pictures, internet history, digital correspondence and  
25 filenames) can remain on a device even after being "deleted." Remnants of activity

1 on a computer can remain on the hard disk drive in an unallocated space for years.  
2 He knows that on a digital storage device, when data is "deleted" it often is only  
3 flagged by the system for deletion and to be written over at a later date, placing the  
4 "deleted" data into unallocated space on the drive. This data can remain on a  
5 computer hard drive for an indefinite amount of time until the data is written over by  
6 the system and often loses any associated date/time stamp information.

7 That I know based on training and experience that file names can be easily  
8 manipulated by a user to hide the files true content. Files can also be compressed  
9 or encrypted to hide their true content. This requires the searching of all files  
10 determine if they are the ones specifically sought.

11 That I know based on training and experience that cellular phones often are  
12 passcode locked and the data on them is often not retrievable by external, non-  
13 destructive means. This requires law enforcement to use other processes in which  
14 the phone is disassembled, including ones that consume the cellular phone, to  
15 retrieve the data stored on the cellular phone's memory chips. I know that flash  
16 memory chips used in cellular phones regularly copy data around on the memory  
17 chip in a process called "wear leveling". This is a technique for avoid overuse and  
18 ultimate failure of a portion of the memory and prolong the service life of the device.  
19 This process can leave data (including but not limited to photographs, text message,  
20 call log and other databases) virtually anywhere on the memory chip.

21 I know based on training and experience that many modern personal  
22 electronic devices for sale to the public by major brands (including Apple Motorola,  
23 HTC, Samsung and other companies) use personal biometric information to unlock  
24 the devices. This can include fingerprint information when a fingerprint is read  
25 through a touch sensor, iris or retinal information and facial recognition through the



1 device's digital camera. Most of these newer devices store the user data in an  
2 encrypted form, requiring the user passcode or biometric unlock to be able to access  
3 them. Modern devices' data is often heavily encrypted utilizing the hardware specific  
4 to that individual device and the passcode set by the user. Both Android and Apple  
5 iOS operating system phones typically disable biometric unlocking if a set time has  
6 passed since the device was unlocked, the device has been powered off, if the  
7 device has been remotely locked or several attempts to unlock the device have  
8 failed. With this, many times the only way to readily access the user data on the  
9 device is through biometric information taken from the user.

10 That I know based on experience, training and communications with fellow  
11 law enforcement officers that computers, the internet, email providers and computer  
12 technology have introduced a new method in which pedophiles and child  
13 pornographers may interact with one another. That digital correspondence related  
14 to the trading of child pornography can occur through text messaging, application  
15 chat messaging, email and other forms of digital communication.

16 That I know that breakthroughs in technology have made it possible for large  
17 amounts of data to be digitally stored on small devices that can easily be concealed  
18 on one's person, within a residence, within a vehicle, within a cellular phone, within a  
19 computer, within a duffel bag or backpack, or any other type of container. I also  
20 know that small digital devices can be quickly and easily discarded out of a window  
21 and that it is imperative to search the area directly surrounding a residence;

22 That with the development of the computer, cellular and associated  
23 technologies, such as the internet, pornographers may now connect their computer  
24 or cellular phone to other computers or cellular phones via high speed data lines,  
25 and that connecting to a host computer, electronic contact can be made to literally

1 millions of computers around the world. That a host computer is one that is attached  
2 to a dedicated network that serves many users and information and files can easily  
3 be electronically transferred from one user to another.

4 That these internet service providers allow electronic mail service (email)  
5 between subscribers, and sometimes between their own subscribers and those of  
6 other networks. That some of these systems, including Microsoft, Google, Yahoo,  
7 etc., and cellular phone applications (apps) offer their subscribers the ability to  
8 communicate publicly or privately with each other in real time in the form of "chat  
9 rooms." That contact with others utilizing this online format is very open and  
10 anonymous and that the communication can also be quite private in the form of  
11 person-to-person instant or immediate messages. That based on the nature and  
12 structure of these types of systems, they pose as an ideal communication system for  
13 pedophiles and persons involved in child pornography;

14 That I know a computer or other digital devices ability to store images in  
15 digital form makes them an ideal repository for child pornography as single USB  
16 portable flash drive can store thousands of images and millions of pages of text.  
17 That the size of the electronic storage media (commonly referred to as a drive) used  
18 in home computers, cellular phones and other devices has grown tremendously  
19 within the last few years and that drives with a capacity of several Terabytes  
20 (1,000,000,000,000 bytes of information) or more is not uncommon. That these  
21 drives can store thousands of images at a very high resolution, and that it is only  
22 with careful laboratory examination of electronic storage devices, that it may be  
23 possible to recreate the evidence trail;

24 That I know the ability to produce child pornography easily, reproduce it  
25 inexpensively, and market it anonymously (through electronic communications) has

1 drastically changed the method of distributing child pornography and that this  
2 pornography can now be electronically mailed to anyone with access to a computer  
3 and modem, or anyone with a cellular phone that is able to access the internet. That  
4 computerized depictions of child pornography can take the form of still digital images  
5 or digital movie files. Compressed file containers can contain multiple image file  
6 types.

7  
8 **BASIS OF KNOWLEDGE:**

9 That I was asked by Oakridge Police Officer Loren Larson to assist in a  
10 criminal investigation regarding the use of the open, Wifi wireless internet at the A &  
11 W restaurant in Oakridge at 47841 Highway 58. Beginning in July of 2018, it was  
12 discovered that someone was consistently connecting to the network and  
13 downloading sexually explicit images of children and has periodically done so since  
14 that time to as recently as June 25, 2019.

15 That on June 14, 2019, Oakridge Police Officer Loren Larsen obtained a Lane  
16 County Circuit Court search warrant for Philip Doyle Thomas (date of birth  
17 [REDACTED]), his residence at [REDACTED]  
18 [REDACTED] and Thomas' associated vehicles. The probable cause connecting  
19 Philip Thomas and for the search of him, his residence and vehicle is detailed in the  
20 affidavit for this search warrant which is attached and incorporated herein as **Exhibit**  
21 **A.**

22 On Tuesday, June 18, 2019, I assisted the Oakridge Police Department in  
23 serving the search warrant on Philip Thomas at his residence. I assisted in  
24 collecting computer equipment and other digital devices from the home and took  
25

1 them back to the Springfield Police Department Digital Forensics Laboratory for  
2 processing.

3 I spoke to Philip Thomas, after he had been advised of his Miranda rights,  
4 and he was adamant that he had not been connecting to the A & W Wifi network and  
5 downloading images of child pornography. He seemed rather overwhelmed at the  
6 time but told me he had given away computers in the past that may have his  
7 information still on them. He briefly mentioned someone by the name of "Randy."

8 That on June 19, 2019, I began forensically processing Philip Thomas'  
9 cellular phone, laptop and other devices. I did not locate evidence of child  
10 pornography or network artifacts showing his laptop computer had connected with  
11 the A & W wireless network.

12 That on Friday, June 21, 2019, I met with Philip Thomas and his Attorney  
13 David Saydack while he was at the Lane County Jail on a separate charge. Philip  
14 Thomas informed me that years ago he had purchased several computers on-line.  
15 He sold several of them but began using one, setting up the computer with his  
16 information. He ultimately gave this computer to Randy Simons, who lived in Westfir  
17 at the time. Philip Thomas explained that he became upset with Randy Simons and  
18 has not had contact with him in the last couple years. He knows that Randy Simons  
19 moved into the town of Oakridge and lives at the southeast corner of Rock Road and  
20 Highway 58, across the street from the A & W restaurant.

21 Philip Thomas later explained that the computer he gave Randy Simon was a  
22 laptop computer. He confirmed that he put the name Ian Anderson on the computer  
23 as this is the name he regularly uses.

24 Philip Thomas gave me permission to log into his online accounts to review  
25 his order purchases. I ultimately logged into his and his mother's account on the on-

1 line retailer Tigerdirect.com. I saw several purchases for laptops, two of which  
2 (dated July 28, 2009 and August 10, 2009) show to be for Toshiba Satellite laptop  
3 computers (model number L505-S6951). I later checked the specifications for these  
4 laptops through the manufacturer and confirmed that they contain an Intel brand  
5 wireless adaptor (model 5100AGN) for connecting to Wifi wireless networks.

6 That I contacted Kenneth Sanders (date of birth [REDACTED]), whose  
7 company (KS Consulting) installed the wireless network for the A & W restaurant.  
8 Ken Sanders provided information that he Media Access Control (MAC) Address for  
9 the device used by the suspect was "00:1E:65:13:70:B2" and that the device listed  
10 the name "lanAnderson-PC". I checked this MAC address, knowing that the first  
11 three hexadecimal characters identify the manufacturer and 00:1E:65 shows to be  
12 Intel corporation.

13 Ken Sanders provided me a spreadsheet showing the Uniform Resource  
14 Locator (URL) web addresses for pages and images viewed on the internet by this  
15 user and that the user continued to access the A & W wireless network from this  
16 same device while Philip Thomas was in custody at the Lane County Jail. I saw in  
17 logs provided from the server the activity related to child pornography continued all  
18 the way until as recently as June 25, 2019. I personally navigated to many of the  
19 web sites and saw they showed young females, many of which were prepubescent,  
20 posing in sexual positions. I personally viewed the following listed websites and saw  
21 they showed sexually explicit images of children, exposing their genitals:

- 22 • <http://bestnn.win/bans/v/9/daphne2.jpg>

23 Image labeled as a "10 y.o. model" showing a prepubescent female  
24 spreading her legs for the camera. She is wearing very small, thin  
25

1 underwear, showing her labia. The logs showing the site was visited  
2 on 6/24/2019 at 00:45:12 hours.

- 3 • <http://pics.youngadult.biz/streamrotator/thumbs/Dq/913215.jpg>

4 Image of an apparent teenage girl naked, with her legs spread,  
5 exposing her vagina. The logs showing the site was visited on  
6 6/23/2019 at 00:03:14 hours.

- 7 • <http://lustteens.net/?id=crazy-holiday.biz>

8 Site showing numerous pornographic images of females. At least one  
9 photograph shows a naked, young teenage girl (based on  
10 development) spreading her legs, exposing her vagina. The logs  
11 showing the site was visited on 6/22/2019 at 22:46:02 hours

- 12 • <http://medudabe.top>

13 Website showed it was suspended when I attempted to view it but the  
14 thumbnail images it had contained were still accessible. Several of the  
15 images were of girls under ten years old (based on development)  
16 exposing their breast and/ or naked. The logs showing the site was  
17 visited on 6/21/2019 at 01:59:05 hours

18 That on June 26, 2019 I checked the Department of Motor Vehicle's database  
19 and confirmed Randall Dewitt Simons (date of birth October 13, 1952) shows to  
20 have a valid driver's license (Oregon number 2541303) and lists the residence  
21 address of 47816 Highway 58 Unit 1 Oakridge, Lane County, Oregon. I also saw  
22 that the vehicle license "N0LRJ" shows to be registered to a 2009 Dodge Journey  
23 (Vehicle Identification Number 3D4GG57VX9T551841) to the same Randall Dewitt  
24 Simons (date of birth October 13, 1952).

1 That I personally viewed the real property of 47816 Highway 58 Unit #1  
2 Oakridge, Lane County, Oregon. The involved property of 47816 Highway 58  
3 Oakridge, Lane County, Oregon is a series of multiple dwellings located at the  
4 southeast corner of Rock St and Highway 58. The main building is a single story,  
5 tan building with brown trim that contains three residences. The numbers "47816"  
6 are affixed to the north side of this building in black numbers on gold colored  
7 rectangles. Unit #1 is the northern most residence, with the main door facing to the  
8 west. The number "1" is located on the wall just to the left of this northernmost door.  
9 No outbuildings or storage for the apartment is visible from the road. However, I  
10 know that apartment units commonly have associated with them storage units that  
11 can take the form of a room accessed from the exterior of the unit or an entirely  
12 separate outbuilding.

13 That Officer Loren Larson stated he personally has contacted Randall Dewitt  
14 Simons at the residence at 47816 Highway 58 Unit 1 in Oakridge, Lane County,  
15 Oregon while working patrol. He confirmed that this was in fact Simons' residence  
16 where he currently lives by himself.

17 That on June 23, 2019, I checked one of the informational databases used by  
18 Law Enforcement and it showed Randall Dewitt Simons using the 47816 Highway 58  
19 Unit 1 in Oakridge, Oregon address beginning in July of 2018.

20 That on June 24, 2019, I went to the area of the A & W restaurant with  
21 Oakridge Officer Loren Larsen. I used a laptop computer with the Linux operating  
22 system (specifically the Kali Linux distribution version 2018.4), the Kismet wireless  
23 software, and an Alfa external, directional wireless network antenna. Placing the  
24 wireless adaptor in monitor mode, I could see the wireless traffic in the area  
25

1 including that to the A & W public, wireless network with the Service Set Identifier  
2 (SSID or network name) "AandWSubwayGuest".

3 That at approximately 2336 hours, I saw the suspect device (IanAnderson-  
4 PC) with the MAC address 00:1E:65:13:70:B2 connect to the A & W network. Upon  
5 adjusting the direction of my wireless antenna, I could see based on signal strength  
6 that the client device "IanAnderson-PC" was located on the south side of Highway  
7 58. I moved to the south side of Highway 58 moving down some of the roads  
8 perpendicular to the highway. I found that the client signal from the suspect device  
9 was strongest at the corner of Rock St and Highway 58. As I walked away from  
10 47816 Highway 58 Unit 1, the device signal decreased. As I approached 47816  
11 Highway 58 Unit 1, walking on the street, I saw the signal increase and then  
12 decrease as I passed by.

13 That I personally checked the signal strength of the AandWSubwayGuest  
14 wireless network and it was easily accessible from Rock St.

15  
16 WHEREFORE your Affiant has probable cause to believe, and does believe  
17 that evidence of the crimes of Encouraging Child Sexual Abuse in the First, Second  
18 and Third Degree (ORS 163.684, 163.686, and 163.687), and other crimes of a  
19 sexual nature involving children is currently located on the person of Randall Dewitt  
20 Simons, in the real property located at 47816 Highway 58 Unit #1 and the vehicle  
21 registered to Randall Simons, more specifically described as follows:

22 **Real Property Description:**

23 The involved property of 47816 Highway 58 Oakridge, Lane County, Oregon  
24 is a series of multiple dwellings located at the southeast corner of Rock St and  
25 Highway 58. The main building is a single story, tan building with brown trim that



1 contains three residences. The numbers "47816" are affixed to the north side of this  
2 building in black numbers on gold colored rectangles. Unit #1 is the northern most  
3 residence, with the main door facing to the west. The number "1" is located on the  
4 wall just to the left of this northernmost door. No outbuildings or storage for the  
5 apartment is visible from the road.

6 **Vehicle Description:**

7 A gray Dodge Journey (VIN 3D4GG57VX9T551841) bearing Oregon license  
8 "N0LRJ" registered to Randall Dewitt Simons (date of birth October 13, 1952).

9 **Person To Be Searched:**

10 Randall Dewitt Simons (date of birth October 13, 1952).

11 This evidence consists of:

- 12 • A Toshiba brand Satellite laptop, model L505-S6951
- 13 • Computer records, documents, and materials, including computer towers  
14 (desktop) and notebook computers (laptops); tablets; cellular phones or other  
15 electronic devices capable of accessing the internet via wireless or cellular  
16 signal and running mobile applications; commercial software and hardware;  
17 computer disks; disk drives; solid state flash drives; computer printers;  
18 modems; tape drives; disk application programs; data disks; system disk  
19 operating systems; magnetic media floppy disks; tape systems and hard  
20 drives and other computer related operation equipment; in addition to  
21 computer photographs, slides or other equipment capable of storing digital  
22 images, and all system and user sign-on password codes.
- 23 • Any image or movie file containing or displaying child sexual abuse contained  
24 within any media storage device. To include any computer media storage  
25 device, electronic device, video tape, CD/DVD, and/or any other media

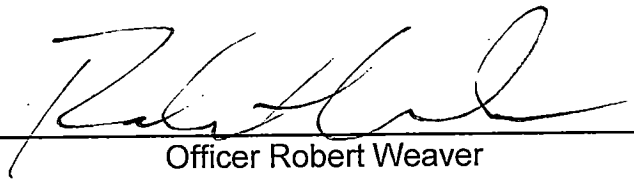
1 storage including but not limited to thumb drives, SD cards, I devices,  
2 cameras, digital cameras, and cellular phones.

- 3 • Any digital artifacts showing the connection to or use of the wireless network  
4 association with the A & W restaurant in Oakridge, Lane County, Oregon,  
5 between July 2, 2018 and June 25, 2019.
- 6 • Any and all diaries, notebooks, notes, writings, documents, day-planners and  
7 any other records reflecting activities indicating the sexual abuse of children.
- 8 • Communications related to the acquiring and trading of sexually explicit  
9 images of children between July 2, 2018, and June 25, 2019.
- 10 • Any evidence related to ownership, control, or use of residence, storage  
11 facilities, computer system(s), media files, programs, telephone number, and  
12 Internet accounts.
- 13 • Any documentation, written or electronic, showing the use of, possession of,  
14 or affiliation with any file-sharing or storage applications.
- 15 • Any and all documents tending to show the occupancy of 47816 Highway 58  
16 Unit #1 Oakridge, Lane County, Oregon including personal identification, bills,  
17 receipts, canceled mail, utility bills, rent receipts and bank statements.
- 18 • The biometric information for Randall Dewitt Simons (date of birth October 13,  
19 1952) to include fingerprint read through device fingerprint sensor, iris or  
20 retinal scans, and facial recognition images collected through device digital  
21 camera.


22 THEREFORE, your affiant prays this court issue a warrant authorizing and  
23 commanding any police officer to search the above described premises, person, and  
24 vehicles for the above described evidence, to seize such evidence, and for any  
25 search, seizure, analysis, and processing of the evidence by a qualified examiner by

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

whatever forensic means necessary and documentation of those items of evidence necessary to the investigation. I also pray this court authorize for the use of Randall Dewitt Simons' biometric information to unlock electric devices by placing his fingers or thumb onto any device's fingerprint sensor and or allowing the imaging of his eyes or face with any device digital camera for the purposes of unlocking the device.

  
\_\_\_\_\_  
Officer Robert Weaver

SUBSCRIBED AND SWORN before me 27 day of June, 2019.

Time 1:30pm  
  
\_\_\_\_\_  
Circuit Court Judge  
Dvelure

IN THE CIRCUIT COURT FOR THE STATE OF  
OREGON FOR LANE COUNTY

STATE OF OREGON                    )  
  ) ss. AFFIDAVIT FOR SEARCH WARRANT  
County of Lane                    )

I, Loren Larsen, being first duly sworn on oath, do depose and say that I am employed as a police officer in the State of Oregon by the City of Oakridge and have been so employed for approximately four and a half years. As a patrol officer my responsibilities include the investigation of a wide variety of crimes, which includes the production, dissemination and distribution of child pornography as well as the sexual abuse and exploitation of children. I have received assistance and on the job training from experienced detectives who have received specific training in the investigation of crimes involving digital evidence and internet-based crimes. I am a duly sworn peace officer as defined in ORS 133.005. I am authorized pursuant to ORS 133.545, to apply for search warrants and hereby make application to this Court for a search warrant as further described below.

I am familiar with the information contained in this affidavit because I have reviewed relevant documents and other evidence related to this case. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search/obtain and seize specific evidence, I have not included herein the details of every aspect of the investigation. Where actions, conversations and statements of others are related herein, they are related in substance and in part except where otherwise indicated.

## TRAINING AND EXPERIENCE:

Based on my experience and training, preferential child molesters, pedophiles and child pornographers receive sexual gratification, stimulation and satisfaction from actual physical contact with children, from fantasies they have viewing children engaged in sexual activity-or in sexually suggestive poses (whether in person, photographs, or other visual media), and from literature describing such activity.

Based on my experience and training, I know that people who are sexually attracted to children, and engage in sexual acts with children, often maintain and collect photos, which in today's age of technology, are commonly stored on memory devices such as personal computers, laptop computers, tablets, cellular phones, digital media storage, CDs, DVDs, flash drives, spare hard drives, etc. In addition, based on my experience and training, I've learned that suspects attracted to children also maintain collections of hard copy photos as well as books, magazines, articles, and other writings on the subject of sexual activity. I know that these books and materials on the topics of human sexuality and sexual education may consist of sex manuals discussing or showing various sexual acts, positions and/or sexual activities. I know that these materials are used for the personal sexual arousal on the part of the offender, particularly, when naked children are shown or depicted within the materials.

Based on my experience and training, I know that the offender will often store/keep these materials within close proximity in order to ensure they're readily available for viewing and use and to show to their victims for grooming purposes. I know that an offender's residence and/or person would be the most convenient and likely place where an offender would keep these materials in order to keep them readily

accessible and to ensure that they are not discovered, lost, or removed by someone else. I know that because these offenders' value these materials they often keep such digital storage media on their person in order to keep the pornography readily accessible and to ensure they are not discovered, lost, or removed by someone else.

Based on my experience and training regarding persons who have an expressed interest in the sexual molestation of children and child pornographers, I know that suspects are collectors of child pornography and value their material as prized possessions and that suspects are very secretive about their collections of child pornography. Suspects rarely, if ever, dispose of child pornography they have acquired, as it is relatively difficult to obtain. I have also learned through my experience and training that suspects will often keep their child pornography at their residence, on their person, or at a secure location convenient to them to ensure that the material is readily available and protected. I also know that persons predisposed to collecting child pornography will frequently maintain collections of visual depictions of adults made to appear as minors engaged in sexually explicit conduct as a surrogate of child pornography. I also know that film negatives as well as photo sets, slides, video tapes and computer software, are offered for sale and exchanged domestically and internationally along with magazines and films.

Based on my experience and training I know that people will often store items that are valuable to them in secured locations, including vehicles and outbuildings. These locations can provide some security for the suspects' evidence being found by roommates, family members, or others residing with them at their residence.

Based on my experience and training concerning individuals who are interested in the sexual molestation and/or exploitation of minors engaged in sexually explicit conduct will often correspond with others who express the same interest. I know that as a result of these contacts, these person(s) will often retain correspondence received and that some of these person(s) may keep records e.g. card files, computer files, digital application messages, address books, diaries, notebooks, and/or electronic communications (emails and application messaging) of such correspondence. I have also found that person(s) who obtain and/or disseminate child pornography through the United States Mail and/or other common carrier and/or computer mediums, will frequently retain advertisements and list of sources of such material;

Based on my experience and training regarding criminal investigations, I know that corroborating facts asserted by a reporting party is important in a criminal prosecution, and that locating sexually explicit evidence involving minors on Philip Thomas' electronic devices, and any other digital storage media, would tend to corroborate facts asserted by the complainant.

I know in any investigation and prosecution it is important to establish that the suspect had the opportunity to be at the location of the crime at the times described. This can be established in a variety of ways. One way would be via location, network data and other data stored within Philip Thomas' cell phone, computer and/or tablet that corroborates and matches the suspect's activity as reported by a witness or complainant.

I know that accessing a wireless network at the business would mean needing to bring a device capable of accessing the network within the range of the wireless signal.

Portable devices can easily be brought within range in a vehicle. I know that when multiple vehicles are available to a suspect, they may use a vehicle other than their own.

I have spoken with Springfield Police Digital Forensic Investigator, Detective Robert Weaver, about this case along with the process and complications that go along with searching and analyzing electronic data. Detective Robert Weaver is a Certified Computer Examiner through the International Society of Forensic Computer Examiners and a Certified Forensic Computer Examiner with the International Association of Computer Investigative Specialist. Detective Robert Weaver has hundreds of hours of training in information technology, electronics, digital forensics for computers and cellular phones. He has also forensically processed almost a thousand digital devices. Detective Robert Weaver has provided me the following information regarding cases where digital devices information is extracted.

Detective Robert Weaver knows based on training and experience that a wide assortment of data is commonly stored on memory devices such as personal computers, laptop computers, tablets, cellular phones, digital media storage, CDs, DVDs, flash drives, spare hard drives, etc. This data can include digital artifacts of identifying information of the owner of the device, internet activity, digital photographs, and correspondence with others including, messaging and chat application data, emails, text messages and call logs. Network information, such as router, IP addresses, and network Service Set Identifiers (SSID or network names) is often stored on digital devices. That networking devices, such as routers, modems and other items that connect to the internet can maintain usage logs and user information.



Detective Weaver knows based on experience and training concerning searches and seizures of evidence from computers commonly requires law enforcement to seize all computer items (hardware, software, digital storage devices and media, and instructions) to be processed at a later date by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because computer storage devices (hard disks, diskettes, data tapes, laser disks, compact flash drives, thumb drives, SD disks, and other removable media used in cellular phones, hand held computers, laptop computers, tablets, personal digital assistant (PDA) devices and cameras) can store the equivalent of millions of pages of information. Further, persons who possess evidence of criminal conduct in the form of digital files will often stores those files in random order with deceptive file names. This in turn requires searching authorities to examine all of the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months depending on the volume of data stored and it would be impractical to attempt this kind of data search except for within a digital forensics' laboratory. Additionally, searching computer systems, cellular phones and other digital storage devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert(s) should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to

tampering or destruction (either from external sources or from destructive codes imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis;

Detective Robert Weaver knows based on his training and experience processing digital evidence that digital artifacts (including pictures, internet history, digital correspondence and filenames) can remain on a device even after being "deleted." Remnants of activity on a computer can remain on the hard disk drive in an un-allocated space for years. He knows that on a digital storage device, when data is "deleted" it often is only flagged by the system for deletion and to be written over at a later date, placing the "deleted" data into un-allocated space on the drive. This data can remain on a computer hard drive for an indefinite amount of time until the data is written over by the system and often loses any associated date/time stamp information.

Detective Weaver know based on training and experience that file names can be easily manipulated by a user to hide the files true content. Files can also be compressed or encrypted to hide their true content. This requires the searching of all files determine if they are the ones specifically sought.

Detective Robert Weaver knows based on training and experience that cellular phones often are passcode locked and the data on them is often not retrievable by external, non-destructive means. This requires law enforcement to use other processes in which the phone is disassembled, including ones that consume the cellular phone, to retrieve the data stored on the cellular phone's memory chips. He knows that flash memory chips used in cellular phones regularly copy data around on the memory chip in a process called "wear leveling". This is a technique for avoid overuse and ultimate

failure of a portion of the memory and prolong the service life of the device. This process can leave data (including but not limited to photographs, text message, call log and other databases) virtually anywhere on the memory chip.

Detective Weaver knows based on training and experience that many modern personal electronic devices for sale to the public by major brands (including Apple, Motorola, HTC, Samsung and other companies) use personal biometric information to unlock the devices. This can include fingerprint information when a fingerprint is read through a touch sensor, iris or retinal information and facial recognition through the device's digital camera. Most of these newer devices store the user data in an encrypted form, requiring the user passcode or biometric unlock to be able to access them. Modern devices' data is often heavily encrypted utilizing the hardware specific to that individual device and the passcode set by the user. Both Android and Apple iOS operating system phones typically disable biometric unlocking if a set time has passed since the device was unlocked, the device has been powered off, if the device has been remotely locked or several attempts to unlock the device have failed. With this, many times the only way to readily access the user data on the device is through biometric information taken from the user.

Detective Weaver knows based on experience, training and communications with fellow law enforcement officers that computers, the internet, email providers and computer technology have introduced a new method in which pedophiles and child pornographers may interact with one another. That digital correspondence related to the trading of child pornography can occur through text messaging, application chat messaging, email and other forms of digital communication.

Detective Weaver knows that breakthroughs in technology have made it possible for large amounts of data to be digitally stored on small devices that can easily be concealed on one's person, within a residence, within a vehicle, within a cellular phone, within a computer, within a duffel bag or backpack, or any other type of container. He also knows that small digital devices can be quickly and easily discarded out of a window and that it is imperative to search the area directly surrounding a residence;

With the development of the computer, cellular and associated technologies, such as the internet, pornographers may now connect their computer or cellular phone to other computers or cellular phones via high speed data lines, and that connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network that serves many users and information and files can easily be electronically transferred from one user to another.

These internet service providers allow electronic mail service (email) between subscribers, and sometimes between their own subscribers and those of other networks. That some of these systems, including Microsoft, Google, Yahoo, etc., and cellular phone applications (apps) offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms." That contact with others utilizing this online format is very open and anonymous and that the communication can also be quite private in the form of person-to-person instant or immediate messages. Based on the nature and structure of these types of systems, they pose as an ideal communication system for pedophiles and persons involved in child pornography;

Detective Weaver knows the computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography a single USB portable flash drive can store thousands of images and millions of pages of text. That the size of the electronic storage media (commonly referred to as a drive) used in home computers, cellular phones and other devices has grown tremendously within the last few years and that drives with a capacity of several Terabytes (1,000,000,000,000 bytes of information) or more is not uncommon. These drives can store thousands of images at a very high resolution, and that it is only with careful laboratory examination of electronic storage devices, that it may be possible to recreate the evidence trail;

Detective Weaver knows the ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distributing child pornography and that this pornography can now be electronically mailed to anyone with access to a computer and modem, or anyone with a cellular phone that is able to access the internet. Computerized depictions of child pornography can take the form of still digital images or digital movie files. Compressed file containers can contain many multiple image file types.

**BASIS OF KNOWLEDGE:**

On July 2, 2018, I contacted Ken Sander (DOB [REDACTED]) and Rodney Porteous (DOB [REDACTED]) when they filed a complaint regarding someone downloading pornographic material involving children. Rodney Porteous is the owner of the A&W restaurant located at [REDACTED]. Ken

Sanders is the owner of the Information Technology company (KS Consulting Services) that implements the wireless internet (WIFI) for the A&W business.

I was informed by them that the business provides free, wireless internet to the public but that anyone using the wireless internet must agree to terms and conditions related to the monitoring and prohibition of illegal activity.

Ken Sanders informed me that the server at the business had alerted to user activity that the server detected and automatically classified as related to child abuse and/or child pornography. Ken Sanders explained that the server retrieves and stores information about the computer as well as the internet sites visited by the user. He informed me that the Media Access Control (MAC) Address for the device used by the suspect was "00:1E:65:13:70:B2" and that the device listed the name "IanAnderson-PC".

Ken Sanders provided me a spreadsheet showing the Uniform Resource Locator (URL) web addresses for pages and images viewed on the internet by this user. I personally navigated to the following listed websites and saw they showed sexually explicit images of children, some exposing their genitals or engaged in sexual acts:

<http://kansasgirls.top/cont/g.php?f=192.jpg>

Suspect Visited on 6-7-2019 @ 23:31

<http://eroticgf4you.com/>

Suspect Visted on 6-1-2019 @ 00:10

<http://hotsharing.net/>

Suspect Visted on 5-30-2019 @ 02:19

<http://archive-teen.ru/>

Suspect Visted on 5-28-2019 @ 00:44

I saw the activity related to child pornography began in July of 2018 and continued all the way until as recently as June 7th, 2019. I was provided lists of other websites visited by the user which included a Facebook account in the name of "Ian Anderson" with Facebook id 100012317230419 (<https://www.facebook.com/profile.php?id=100012317230419>). I viewed the items on this Facebook profile page and saw a "like" for the Gear Peddler bicycle shop in Bend, Oregon.

On 10-31-2018 I viewed Philip Thomas' (AKA Ian Anderson) Facebook page and saw that he listed employment as a shuttle driver working out of the Willamette Mountain Mercantile-Oakridge Bike Shop at 48080 Highway 58 Oakridge, Lane County, Oregon. I went to the Mercantile bicycle shop and contacted Kerri Vandenberg (DOB [REDACTED]) and showed them photographs printed of the person identifying themselves as "Ian Anderson" on the Facebook account. They told me that the person is actually named Philip Thomas and goes by the name Ian Anderson for some unknown reason.

On June 3, 2019 I checked the Department of Motor Vehicle's database and confirmed Philip Doyle Thomas (DOB [REDACTED]) shows to have a valid driver's license (Oregon number 1968004) and lists the residence address of [REDACTED]. I looked at the DMV photograph for Philip Thomas and confirmed it matched the photograph of the male identifying himself as "Ian Anderson" on the Facebook account (Facebook ID number 100012317230419). I also saw that the vehicle license "030EMB" shows to be

registered to a 1999 Chevrolet Tahoe Sport Utility Vehicle (Vehicle Identification Number 1GEK13R4XJ493497) to the same Philip Doyle Thomas (DOB [REDACTED]).

On 5-30-2019 I personally contacted Philip Doyle Thomas at the residence at [REDACTED] on an unrelated case. I confirmed with him that this was in fact his residence where he lives with his mother, Sally Ann Thomas (DOB [REDACTED]). I also saw Philip Thomas' Tahoe parked at the residence along with other vehicles, including a blue Honda CRV bearing Oregon license "205CKY".

I checked the Department of Motor Vehicles database and the vehicle license "205CKY" shows to be registered to a 2006 Honda CRV (Vehicle identification Number JHLRD78886C031473) to Sally Ann Thomas (DOB [REDACTED]).

On 06-06-2019 I contacted Shiela Keller (DOB [REDACTED]), a neighbor of Philip Thomas that lives at 49365 Mountain View Rd (across the street from Philip Thomas). They stated they know Philip Thomas and have seen him driving multiple vehicles including his Chevrolet Tahoe (Oregon license "030EMB") and his mother's Honda CRV (Oregon license "205CKY"). They told me Thomas and his mother Sally live at the residence and had bought the property from the previous owner. She thought they had lived there for about 12 years now.

On June 3, 2019, I checked Philip Thomas through the Law Enforcement Data System and he showed to be a registered sexual offender with the registered address of [REDACTED]. Upon doing a full Criminal History check



of Philip Thomas, he shows to have been convicted of two counts of Lewd or Lascivious acts with a child under age 14.

**REAL PROPERTY DESCRIPTION:**

The real property at [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED] n, is a plot of land over six acres in size on the south side of Mountain View Road approximately one-half mile west of the intersection with High Prairie Road. The entrance to the property is a gravel road blocked by a metal tube gate. A mailbox to the right of the driveway has the numbers [REDACTED]" in black affixed to the side. The residence on the property is a manufactured home that is light blue with white trim located at the end of the gravel driveway. At least two, separate, small outbuildings are visible from the road.

**VEHICLE DESCRIPTIONS:**

A white 1999 Chevrolet Tahoe (Vehicle Identification Number 1GEK13R4XJ493497) registered with Oregon license "030EMB" to Philip Doyle Thomas (DOB [REDACTED]).

A blue 2006 Honda CRV (Vehicle identification Number JHLRD78886C031473) registered to license "205CKY" to Sally Ann Thomas (DOB [REDACTED]).

**PERSON TO BE SEARCHED:**

Philip Doyle Thomas (DOB [REDACTED])

WHEREFORE, your Affiant has probable cause to believe, and does believe, that evidence of the crimes of Encouraging Child Sexual Abuse in the First, Second and

Third Degree (ORS 163.684, 163.686, and 163.687), and other crimes of a sexual nature involving children is currently located on the person, in and on the real property, in outbuildings on the real property, and in the vehicles described above. This evidence consists of the following:

- Computer records, documents, and materials, including computer towers (desktop), notebook computers (laptops), tablets, cellular phones, commercial software and hardware, computer disks, disk drives, solid state flash drives, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive and other computer related operation equipment, in addition to computer photographs, slides or other equipment capable of digital images, and all system and user sign-on password codes.
- Any image or movie file containing or displaying child sexual abuse contained within any media storage device, to include any computer media storage device, electronic device, video tape, CD/DVD, and/or any other media storage including but not limited to thumb drives, SD cards, I devices, cameras, digital cameras, and cellular phones.
- Any digital artifacts showing the connection to or use of the wireless network association with the A & W restaurant in Oakridge, Lane County, Oregon, between July 2, 2018 and June 8, 2019.
- Any and all diaries, notebooks, notes, writings, documents, day-planners and any other records reflecting activities indicating the sexual abuse of children.

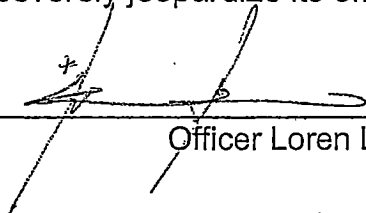
**EMERSON A**

- Communications related to the acquiring and trading of sexually explicit images of children occurring between July 2, 2018, and June 8, 2019.
- Any evidence related to ownership, control, or use of residence, storage facilities, computer system(s), media files, programs, telephone number, and Internet accounts.
- Any documentation, written or electronic, showing the use of, possession of, or affiliation with any file-sharing or storage applications.
- Any and all documents tending to show the occupancy of [REDACTED] [REDACTED] [REDACTED] including but not limited to personal identification, bills, receipts, canceled mail, utility bills, rent receipts and bank statements.
- The biometric information for Philip Doyle Thomas' person (DOB [REDACTED] [REDACTED]) to include fingerprint read through device fingerprint sensor, iris or retinal scans, and facial recognition images collected through device digital camera.

THEREFORE, your affiant prays this court to issue a warrant commanding any police officer to search the above described premises, person, and vehicles for the above described evidence, to seize such evidence, and for any search, seizure, processing, analysis, processing by a qualified examiner by whatever forensic means necessary and documentation of those items of evidence necessary to the investigation. I also pray this court authorize for the use of Philip Doyle Thomas' biometric information to unlock electric devices by placing his fingers or thumb onto any device's fingerprint sensor and/or allowing the imaging of his eyes or face with any device digital camera for the purposes of unlocking the device.

**REQUEST FOR SEALING**

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the victim is a juvenile, the associated crimes are of a sexual nature, and items / information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

  
\_\_\_\_\_  
Officer Loren Larsen

SUBSCRIBED AND SWORN before me 14 day of June, 2019.

Time 1:24 pm

  
\_\_\_\_\_  
Circuit Court Judge

1 IN THE CIRCUIT COURT OF THE STATE OF OREGON

2 FOR THE COUNTY OF LANE

3 **STATE OF OREGON,** )  
4 )  
5 Plaintiff, ) Case No. 19CR43543  
6 )  
7 v. )  
8 )  
9 **RANDALL DE WITT SIMMONS,** )  
10 )  
11 Defendant. )  
12 )  
13 )  
14 )  
15 )  
16 )  
17 )  
18 )  
19 )  
20 )  
21 )  
22 )  
23 )  
24 )  
25 )

---

Grand Jury Testimony of Robert Weaver

July 24, 2019

16 APPEARANCES:

17 FOR THE PLAINTIFF: **PATRICIA W. PERLOW**  
18 **DISTRICT ATTORNEY**  
19 **BY: Jay D. Hall**  
20 125 East Eighth Avenue  
21 Eugene, Oregon 97401

22 TRANSCRIBED FROM AUDIO RECORDINGS

23 TRANSCRIBED BY: Peggy S. Jillson  
24 987 Tivoli Street  
25 Eugene, Oregon 97404  
(541) 689-7964

EUGENE, OREGON; WEDNESDAY, JULY 24, 2019

-o0o-

EXAMINATION

BY MR. HALL:

Q. Have a seat, and then introduce yourself to the grand jury and spell your name for the record.

A. My name is Robert Weaver, and it's W-E-A-V-E-R. And I'm a detective with the Springfield Police Department.

Q. And do you have your report here with you?

A. Yeah.

Q. Do you have your PC affidavit here with you?

A. Let's see if I have the PC affidavit. I know I have it in here somewhere.

Q. Okay. Well, if you need to take a moment and locate that, go ahead and do so. But I'm just going to ask you how you came to be involved in an investigation that led you to Randall De Witt Simmons and child pornography up in Oakridge.

A. So Oakridge Police Department, they're a small police department. They ended up getting in contact with me. I've helped them out on different cases. We have a digital forensics lab, and I do the -- I'm the digital forensic analyst for the police department, so I handle all the -- anything with technology. Processing of computers, cell phones, retrieving data off of things. So they've gotten

1 ahold of me to get -- to help out with some of their cases up  
2 there.

3           And last summer Officer Loren Larsen got ahold of  
4 me. And there had been a report from the A&W there that  
5 someone was logging onto their free WiFi and downloading  
6 child pornography. And so we kind of said -- I kind of said  
7 to them, "Okay, this is what you need to do. You need to  
8 look at getting a search warrant. You need to figure out who  
9 it is." And kind of put them on the right track to  
10 investigate it.

11           Well, then they got ahold of me this year and  
12 said they -- he thinks they've figured out who -- who was  
13 logging on there, and he thought he had enough for a search  
14 warrant. And so I helped him in writing a search warrant for  
15 a guy named Philip Thomas (phonetic). His -- his house and  
16 his person, because the computer that -- when -- when you  
17 hook up to WiFi, it act -- there's actually some information  
18 off the computer that's retrieved and stored on the server  
19 there. And we were able to identify the computer, the name  
20 of the computer, some information, some serial-number-type  
21 information on the computer. And based on some of the  
22 content of what this person was looking at, we had enough to  
23 get a search warrant for Philip Thomas.

24           Q.       And what did you think Philip Thomas, given the  
25 information that was known to you at that investigatory

1 level?

2 A. So Philip Thomas lives up there in Oakridge, and  
3 he likes to go by the name Ian Anderson (phonetic). He's  
4 like the only person up there that likes to -- that goes by  
5 Ian Anderson. There's no other Ian Anderson up there. And  
6 the computer's name was Ian Anderson PC. And some of the  
7 content that this person was looking at related to bike  
8 trails and the bicycle shop of there, and I think his  
9 Facebook account.

10 Q. Ian Anderson Facebook account?

11 A. Yeah, the Ian Anderson Facebook account, which is  
12 Philip Thomas. When you look at the picture, it's, oh,  
13 there's Philip Thomas. And Philip Thomas does bicycle  
14 shuttling service for people mountain biking. He shuttles  
15 them up to different trails and drops them off with their  
16 bikes and whatnot. And some of those maps and things like  
17 that were in the content. And so it -- the finger was  
18 totally pointing at Philip Thomas for this -- for accessing  
19 this.

20 Q. So did Oakridge Police Department go through that  
21 investigation and actually find Philip Thomas and talk to  
22 him?

23 A. Yeah, so we -- we -- Philip Thomas lives just  
24 outside of town. We served a search warrant on his house.  
25 And I gathered up all his devices and whatnot. I talked to



1 him, and he's like, "No, it wasn't me." I'm like, "Have you  
2 given away any computers? Have you -- why would somebody  
3 have your information?"

4 And he had mentioned a guy named Randy at that  
5 time, but he was so overwhelmed with the search warrant and  
6 all this stuff that he couldn't really explain everything.

7 I ended up -- he got lodged at the jail for  
8 another -- another, unrelated crime. And I listened to some  
9 of his jail phone calls. Well, he talks to his mom and he  
10 says to mom, "Hey, Mom, I gave that one computer of mine to  
11 Randy, and he now lives right across the street from A&W."

12 Q. Okay. So based on that statement, as part of  
13 your investigation, were you able to develop Randall De Witt  
14 Simmons as this Randy person --

15 A. Yeah.

16 Q. -- that is now the focus of the investigation?

17 A. Yeah. I actually sat down with Phil and he  
18 identified Randy. He told me exactly -- on the map, he  
19 showed me exactly where he lives, and that's where Randy  
20 Simmons lives. And --

21 Q. And so what procedure did you and the Oakridge  
22 Police Department do to hone in on Randall Simmons?

23 A. So at that time we just had kind of this old  
24 information that a computer was given from Phil to Randy  
25 Simmons. And Randy's actually said, "Hey, I -- I ordered

1 that computer online. You can go onto my account. You can  
2 look at the computers that I ordered and whatnot."

3 And I actually went in and found the order for a  
4 Toshiba Satellite laptop computer. And when you look at the  
5 specs of that computer, the information that's in there for  
6 the WiFi card on that computer matches what we were seeing  
7 connecting to the -- the server. You get -- from the server  
8 you can tell that the WiFi adaptor on the laptop is an Intel  
9 brand, which is -- most of them usually aren't Intel, but  
10 this one's Intel. And when you go into the specs for this  
11 Toshiba Satellite, it has an Intel brand WiFi adaptor.

12 And so some of that stuff matched up, but it was  
13 a couple of years old that he had -- we knew he had given  
14 this computer. So we were kind of like, wow, well, how are  
15 we going to figure out for sure it's Randy? And so I went  
16 through every web page that he had looked at because these --  
17 the server keeps logs of all the --

18 Q. You're talking about that you went through the  
19 server at A&W to see --

20 A. A&W server. They keep track -- they were keeping  
21 track for us of every website he was going to, and it was all  
22 child porn related. There was nothing -- I couldn't find a  
23 Facebook login or an email login or anything like that that  
24 would point the finger at Randy. So at that point I was kind  
25 of left with, okay, we're just going to have to try to track

1 him. So I knew that he had been logging on, based on the  
2 times he was logging on, between 11:00 p.m. and 2:00 almost  
3 every night. So I went up there and I sat with the Oakridge  
4 police officer, and I have a special computer. It's not a  
5 Windows computer. It actually runs a different operating  
6 system. And I have a WiFi antenna that's directional.

7 Q. So let me ask you this, then. When somebody goes  
8 to log on from a nearby place to that WiFi signal within --  
9 if it's within range, if you're also within range, can you  
10 essentially detect the -- that it's logging on and the sort  
11 of direction in which it's --

12 A. Yeah. So -- I can actually show you some  
13 examples. This is what you see on it. I can actually see,  
14 when I'm sitting up there, every single WiFi that's -- that  
15 it can pick up, even hidden ones. You can -- you can see all  
16 of them that are on there, and you can -- you can pick one.  
17 So I picked "A&W Subway guest." That's the A&W's. They  
18 share it with Subway.

19 And so I picked that one. And then at -- I think  
20 this was at 11:36, his computer popped up and connected to  
21 the A&W WiFi. And so --

22 Q. Did you find that it was going onto child  
23 pornography at that point?

24 A. Yes, it was. It was going onto child pornography  
25 sources.

1 Q. So based on everything up to that point, what did  
2 you do with that information?

3 A. So from this point -- at that point I focused in  
4 on that particular device and --

5 Q. No, not -- I guess what I'm saying is, once you  
6 had all of that information, did you put it into a search  
7 warrant?

8 A. Yeah, because basically I -- I used my  
9 directional antenna and it pulled up Ian Anderson's PC. And  
10 as I honed in on it, it's like, okay, it's over there. Let's  
11 walk over there. Okay, it's in the south part of this house  
12 right here. And you can actually see the signal. Actually,  
13 as I walked closer and passed it, it goes up and then it goes  
14 back down. And so you can say, okay, yep, the device, the PC  
15 that's connected to that WiFi is in that -- in that house  
16 right there. And that was enough to get a search warrant for  
17 his house.

18 Q. Okay. And then when did you do the search  
19 warrant?

20 A. We did it on June 27th.

21 Q. How close in time was that to the -- your  
22 operation there that you took the antenna up there?

23 A. That was on June 25th, I think.

24 Q. Okay. So within a couple days?

25 A. Yeah.

1 Q. All right. And once you served that search  
2 warrant, did you find this laptop that you were describing  
3 and anticipated finding?

4 A. Yeah. Initially, when I contacted Randall  
5 Simmons at the front door, he denied having a computer,  
6 having one from -- that he got from Phil. He said he knew  
7 Phil but he didn't have the computer. He started to say he  
8 didn't have any computers at all, but then said -- admitted  
9 he did. So I explained that I have a search warrant, I'm  
10 looking for this Toshiba Satellite. This is the model  
11 number, connected to the A&W, child pornography. And then,  
12 with that, he just said, "Okay, I'll tell you where I hid the  
13 laptop."

14 Q. Did he take you where he hid it?

15 A. Yeah. We had advising of his rights. He  
16 actually took and showed us. He had shoved it under some  
17 bedding on the bed. And then he acknowledged that he had  
18 been connecting to the A&W and looking at naked pictures of  
19 children.

20 Q. And that was right there before you even got into  
21 the laptop?

22 A. Yeah.

23 Q. And he acknowledged that?

24 A. Yeah.

25 Q. What specifically did he acknowledge?

1           A.       He was looking at young girls, including  
2 prepubescent girls. Pictures that were naked, pictures that  
3 were sexual. He told me that he's a photographer by trade.  
4 He's retired, but he said that -- he claimed that he was  
5 initially looking for modeling-type pictures of young girls;  
6 you know, like pageant-type stuff. Different photo shoots,  
7 posing and whatnot. And he said that, over time, he just --  
8 it just began getting more raunchy and more sexual and more  
9 naked, and stuff like. I asked him. I was like, "Why do you  
10 keep doing it? Why do you keep looking at that stuff?"

11                   And he just kind of paused and looked at me and  
12 said, "I can't tell you why I do."

13           Q.       So eventually you would get into this laptop;  
14 correct?

15           A.       Yes.

16           Q.       Did you find that he was just looking at these  
17 images or that he was actually duplicating them in some way?

18           A.       He was actually duplicating them and -- and he  
19 was --

20           Q.       Okay. And when you talked to him, did he say he  
21 was just looking at them or did he acknowledge that --

22           A.       No, he acknowledged that he was -- he would look  
23 at them, pick out ones that he liked. He would sit -- grab  
24 them and save them onto his computer in the downloads  
25 directory. And then he said when he would -- he would go the

1 next day when he was more sober and pick through them and  
2 save the ones that he liked, and then delete the ones he  
3 didn't like.

4 Q. Okay. So there's this initial spot he's calling  
5 the downloads directory, but he's saving them over to  
6 another, what? File?

7 A. Saving them and putting them in another  
8 directory --

9 Q. Okay.

10 A. -- on the computer.

11 Q. Did you ever find out what that directory was  
12 called?

13 A. I -- well, when I looked at his computer.

14 Q. Right. What was it called?

15 A. Yeah, so it -- within his pictures directory,  
16 under the user, he had two different -- it was "new  
17 folder(2)" and "new folder(4)" were --

18 Q. Okay. So there wasn't any name that was  
19 associated with it. Is was just sort of --

20 A. "New folder."

21 Q. "New folder"?

22 A. Yeah.

23 Q. In your PC affidavit you went through and you  
24 selected some images. How many images, overall, would you  
25 say you looked at that were on this -- saved onto this

1 laptop?

2 A. The -- well, shoot, I've looked at thousands of  
3 images on there. But of the ones that were saved, there's  
4 probably hundreds of images.

5 Q. Of what?

6 A. Of young girls, young teenage girls, prepubescent  
7 girls. Various stages of undress. They'll be posing in  
8 sexual poses. Some of them are naked. Some of them have  
9 their legs spread and exposing their vagina, showing their  
10 breasts. Probably down to age -- of the saved ones, probably  
11 down to age five or so.

12 Q. Now, did you find during your investigation that  
13 there was a difference between what he might view online in  
14 terms of conduct and what he might save to his laptop?

15 A. Yes.

16 Q. Tell us about that.

17 A. So you can look at the Internet cache for the --  
18 the browsers. With the way that -- the way the browsers work  
19 is they actually -- when you look at a web page, they save a  
20 lot of that stuff to try to make the user experience better.  
21 So, if you go back to that page, it loads a lot faster. And  
22 so you can look at the cached images that are stored on  
23 the -- in the Windows system there, and there were images of  
24 adult males having sex with small children. A lot of images  
25 of naked prepubescent kids. I did end up today -- I went



1 through and looked at the deleted space, the unallocated  
2 space on his hard drive. And I found a lot more images of  
3 children and children that were having sexual -- sex or oral  
4 sex with an adult.

5 Q. Okay. And so if we just called those, you know,  
6 children being raped as opposed to children who are posing --

7 A. Yeah.

8 Q. -- anyway, did you find that the things that he  
9 was actually duplicating, the things he was saving included  
10 both or were just one or the other?

11 A. They were posing. They were a lot of posing  
12 stuff. I didn't see -- there were one or two images which I  
13 couldn't -- the girl looked young, but I couldn't tell if she  
14 was under 18.

15 Q. Okay.

16 A. That -- that did involve oral sex on a male.

17 Q. All right. Of the 15 that we're about ready to  
18 go over, can you tell within your experience and training  
19 whether or not any of these children could possibly be adults  
20 or be age over 18?

21 A. No. These -- I purposely selected ones that were  
22 clearly either prepubescent or barely teenagers.

23 Q. Okay. Can you take us down through these 15,  
24 then.

25 A. Sure. So the first one was a jpeg image. It's

1 titled "8hyhh.jpeg." And it was in the pictures directory  
2 under that user, that Ian Anderson user, in a subdirector  
3 called "new folder(4)." And it's a prepubescent female  
4 laying on her back, exposing her vagina and a breast. And --

5 Q. What was the creation date of that image?

6 A. So the date -- the date time stamps in the file  
7 system showed August 11th of 2018.

8 Q. And is that consistent with being downloaded or  
9 duplicated on that date?

10 A. Yes.

11 Q. All right. Tell us about No. 2.

12 A. No. 2 is another jpeg image. "938" is the name  
13 of the -- the image. And that was also stored in the "new  
14 folder(4)" director. And that was a prepubescent female  
15 standing naked, exposing her breasts and vagina. And the  
16 date and time stamps on this showed February 19th, 2019.

17 Q. Is that consistent with being downloaded and  
18 duplicated on that date?

19 A. Yes, it is.

20 Q. Let's go with Count 3.

21 A. No. 3 is another jpeg image, and it's "825," is  
22 the title of the jpeg. And it was also stored in the "new  
23 folder(4)" subdirectory within the pictures. And it's an  
24 image of a prepubescent female standing on a beach naked,  
25 exposing her breast and vagina. And the date and time stamps

1 in the file system showed February 20th, 2019, and that's  
2 consistent with it being duplicated on that date.

3 Q. All right. What's image No. 4, Count 4?

4 A. No. 4 is a jpeg, "51.jpeg," and it was stored in  
5 the "new folder(2)," parentheses 2, subdirectory within the  
6 pictures. And it's a -- a girl approximately 10 to 12 years  
7 old, facing away from the camera, exposing her anus and her  
8 vagina. And the file -- the date and time stamps in the file  
9 system showed March 26, 2019, consistent with it being  
10 duplicated on that date.

11 Q. And how about image No. 5?

12 A. No. 5 is another jpeg image, and it's titled  
13 "150f." It was also stored in the "new folder(2)" directory.  
14 It's an image of a prepubescent female posing naked with some  
15 feathers, exposing her vagina and breasts. And the date time  
16 stamps in the file system were March 28th, 2019, and that's  
17 consistent with it being duplicated then.

18 Q. And image No. 6?

19 A. Is a jpeg titled "12" that was stored in the new  
20 folder(2) directory. And it's an image of a prepubescent  
21 female laying on her side, naked with her legs spread open,  
22 exposing her vagina. And the date time stamps were April 5th  
23 of 2019, and consistent with it being duplicated then.

24 Q. And 7?

25 A. Is a jpeg titled "33," and it was in the "new

1 folder(2)" directory. And it's a girl approximately 10 to 12  
2 years old sitting naked with her legs spread, exposing her  
3 vagina. And the date and time stamps were April 11th of  
4 2019, consistent with it being duplicated then.

5 Q. Image No. 8?

6 A. Is a jpeg titled "013," and it was also stored in  
7 the "new folder(2)" directory. It's an image of five  
8 females, four of which appear to be approximately 10 to 12  
9 years old, all standing together, naked, exposing their  
10 breasts and vaginas. The -- the date time stamps were for  
11 March -- or, excuse me, April 12th, 2019, and were consistent  
12 with it being duplicated on that day.

13 Q. No. 9?

14 A. No. 9 is jpeg image titled "301.jpeg," and it was  
15 stored in the new folder(2) directory. It's an image of a  
16 prepubescent female lying naked on her chest with her  
17 buttocks up, exposing her vagina. And the date time stamps  
18 were for May 8th of 2019 and were consistent with it being  
19 duplicated then.

20 Q. Image No. 10?

21 A. Is titled "26.jpeg," jpeg. It was in the  
22 downloads directory for this user, Ian Anderson. And the  
23 image is a prepubescent female laying on her chest, naked  
24 with her legs spread, exposing her vagina. And the date and  
25 time stamps for this file were for June 21st, 2019, and were

1 consistent with it being duplicated on that date.

2 Q. Okay. So that one, No. 10, apart from all the  
3 other ones, was in the downloads folder as opposed to one of  
4 the new folder numbers?

5 A. Yes.

6 Q. Is that downloads folder something that you  
7 actively have to click on the image and download it, or is  
8 that something where -- that stores like cookies, like you  
9 were talking about earlier --

10 A. Typically --

11 Q. -- that are easier to come back to that website?

12 A. He was using the Firefox browser. And typically  
13 the Firefox browser, when you -- when you right click on an  
14 image and you put "save as" or save the image, it defaults to  
15 throw those images into the downloads directory.

16 I'd have to -- that's one of the things I have to  
17 do, is I have to go in there and confirm in the settings that  
18 that's still the case, but that's what appeared to be the  
19 case.

20 Q. So I guess another way of asking that is, is that  
21 a place where you would expect to see cookies that are  
22 automatically downloaded when you're just viewing an image or  
23 something --

24 A. No, those are actually --

25 Q. -- where you see an active, "I choose to save

1 this," and it automatically goes to that --

2 A. Yeah, those are actually stored in a really  
3 obscure place in Windows, totally separate from the downloads  
4 directory.

5 Q. Okay.

6 A. It's actually in that -- a hidden directory  
7 called the app data directory. And you have to go into where  
8 Firefox is, and there's a whole little subdirectory that has  
9 all that.

10 Q. Image No. 11, start with that.

11 A. That was titled "24g," and it was in the "new  
12 folder(2)" directory. It's an image of a prepubescent female  
13 lying naked on her side with her leg up, exposing her vagina.  
14 And the date and time stamps were June 23rd, 2019, and  
15 consistent with it being duplicated then.

16 Q. Image No. 12?

17 A. Is titled "ua-58-070.jpeg." And that was in the  
18 downloads directory. It was a picture of a juvenile female  
19 about 13 to 14 years old, posing naked with a beach ball,  
20 exposing her vagina and breasts. And it said -- a lot of the  
21 websites that he was going to and looking at were Ukrainian  
22 or Russian. That's where we typically find that a lot of the  
23 child pornography is coming from. And it was actually tagged  
24 up in the corner like a little -- little name up the corner  
25 that said "Ukrainian angels." It was kind of like a little

1 advertisement up there on that one. The date and time stamp  
2 for that was June 24th, 2019, and was consistent with it  
3 being duplicated on that date.

4 Q. Image No. 13?

5 A. Is titled "422.jpeg," and it was also stored in  
6 the downloads folder. It's an image of a prepubescent female  
7 standing naked, exposing her breasts and vagina. And the  
8 date time stamps were for June or -- yeah, June 25th, 2019,  
9 and were consistent with it being duplicated then.

10 Q. And image No. 14?

11 A. Is titled "217.jpeg." It was in the downloads  
12 folder. It's a -- a naked prepubescent female posing with  
13 her leg up on a rock and exposing her vagina. And the date  
14 and time stamps were for June 26, 2019, and the time stamps  
15 were consistent with it being duplicated then.

16 Q. And the final image that you've selected for  
17 this?

18 A. Was titled "1567.jpeg." It was stored in the  
19 downloads folder, and it was tagged up in the corner "Lovely  
20 Nymphets." And it showed a prepubescent female posing naked  
21 with a portion of her vagina as -- is visible. And the date  
22 and time stamp for it was on June 27th, which was the day  
23 that we served the search warrant, and consistent with it  
24 being duplicated then.

25 Q. And so each one of these 15 images had different

1 titles, according to your testimony. Are each one of these  
2 15 images different when you actually view them, from one to  
3 another?

4 A. Yes. Yeah, there's no --

5 Q. So there are no duplicates within these 15?

6 A. Not within those, yeah.

7 MR. HALL: Those are my questions for you. Does  
8 anybody else have any questions for this?

9 *(Recording ends.)*

10  
11 --oOo--

12  
13 *I certify, by signing below, that the foregoing*  
14 *pages 1 through 20 constitute a correct transcript of FTR*  
15 *recordings provided of the above-entitled matter, this 29th*  
16 *day of August, 2019.*

17  
18 

19 PEGGY S. JILLSON, TRANSCRIBER