

STATE OF WISCONSIN

COURT OF APPEALS

DISTRICT III

Appeal No. 2017AP000185 - CR

STATE OF WISCONSIN,

Plaintiff- Respondent,

RONALD LEE BARIC,

Defendant- Appellant.

RECEIVED

JUL 17 2017

CLERK OF COURT OF APPEALS
OF WISCONSIN

REPLY BRIEF OF DEFENDANT – APPELLANT

APPEAL FROM THE CIRCUIT COURT FOR OUTAGAMIE COUNTY
THE HONORABLE JOHN A. DES JARDINS PRESIDING

JOHN MILLER CARROLL LAW OFFICE
Attorney for Defendant – Appellant

John Miller Carroll
State Bar. No. 1010478

226 S. State St.
Appleton WI 54911
(920) 734-4878

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	<i>i</i>
SUPPLEMENTAL AUTHORITY.....	1
ARGUMENT.....	1-7
CONCLUSION.....	8
CERTIFICATION OF FORM AND LENGTH.....	9
CERTIFICATION OF ELECTRONIC FILING.....	9

TABLE OF AUTHORITIES

Cases

<u>See Riley v. California</u> , U.S., 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014)...	1,7
<u>State v. Purtell</u> , 2014 WI 101, ¶ 28, 359 Wis. 2d 212, 232, 851 N.W.2d 417, 427.....	1,7
<u>United States v. Finley</u> , 477 F.3d 250, 259–60 (5th Cir.2007).....	1,3,7
<u>State v. Carroll</u> , 2010 WI 8, ¶ 27, 322 Wis.2d 299, 778 N.W.2d 1.....	1,3,5
<u>United States v. Ortiz</u> , 84 F.3d 977, 984 (7th Cir.1996).....	1,3,6
<u>United States v. Wurie</u> , 612 F.Supp.2d 104, 109 (D.Mass.2009).....	1,3,6
<u>Kyllo v. United States</u> , 533 U.S. 27,40 (2001).....	5
<u>United States v. Maynard</u> , 615 F.3d 544 (2010).....	7
<u>United States v. Jones</u> , 565 U.S. 400, 404, 132 S. Ct. 945, 949, 181 L. Ed. 2d 911 (2012).....	7

SUPPLEMENTAL AUTHORITY
*WARRANTLESS SEARCHES DEPLOYING SENSE ENHANCING
DEVICES ARE UNCONSTITUTIONAL*

1. Ordinary citizens, even citizens who are subject to diminished **privacy interests** because they have been detained, have a legitimate expectation of **privacy** in the contents of their electronic devices. *See Riley v. California*, U.S., 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). *State v. Purtell*, 2014 WI 101, ¶ 28, 358 Wis. 2d 212, 232, 851 N.W.2d 417, 427

2. “As an initial matter, although the “containers” discussed in *Place* were pieces of luggage, it is reasonable to analogize the cell phone in this case to the luggage in *Place*. The underlying concern with the agents’ detention of the luggage in *Place* was that Place had a reasonable expectation of privacy in the contents of his bags. So, too, here, the concern is protecting a person’s reasonable expectation of privacy in the contents of his or her cell phone. Other courts, in assessing the validity of a search without a warrant, have likened a person’s privacy expectations in cell phones and electronic devices to that of closed containers in his or her possession. *See, e.g., United States v. Finley*, 477 F.3d 250, 259–60 (5th Cir.2007) (holding that the defendant had a sufficient privacy interest in his cell phone call records to challenge the search therein); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir.1996) (holding that the owner of a pager has the same reasonable expectation of privacy in its data as if it were a closed container); *United States v. Wurie*, 612 F.Supp.2d 104, 109 (D.Mass.2009) (“It seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone.”).” *State v. Carroll*, 2010 WI 8, ¶ 27, 322 Wis. 2d 299, 319, 778 N.W.2d 1, 10

ARGUMENT

The States position in Response is fundamentally flawed as these files were not held out to the public on a server like other file sharing networks of the past, rather these files are contained within individual personal computers that are searched on a massive scale without warrants, using sense enhancing devices to reach into a home for information that would not otherwise be available.

3. The States position is fundamentally flawed in its understanding of the eMule network, its function and how it works.

4. Specifically the State puts forth an argument that Baric in some way

held these files out to the public. *See Generally Response Brief of the State* What the state is failing to mention is the specific way that the eMule network works. Specifically eMule is different from its predecessors in that it uses "peer to peer" networking rather than using a server to host information. (R. 59 at page 5, lines 5-18)

5. Specifically eMule and other tor networks are typically used for receiving updates for software and online gaming. These updates are then stored on a local personal computer. When FBI agents deploy their specially engineered and not publically available software they are not reaching into a server held somewhere out to the public but are electronically entering the Defendants home and then personal computer. (R. 59 page 5 "allows two or more users to share files online") (R. 59 pages 8-9 "is that something that is publically available? No.")

6. Worse, this type of warrantless search "software" allows the FBI the ability to search hundreds if not thousands of personal computers across the country, sift the files contained therein and then systematically geolocate the homes where these computers are located, all without a warrant. (R. 59 at page 6)

7. It's interesting that at the time the FBI applied for a warrant in this case they already searched located and verified the information contained on the computer. This was again done by the CPS server electronically reaching into the Defendants computer and searching its files for particular files. (R. 59) (R. 32)

8. In this particular case there was not one warrantless search, not two but many searches that occurred prior to applying for a search warrant. (R. 59)

9. In essence the search had already produced the fruits of the crime that the warrant sought to gather. (R. 59) (R. 32)

10. Specifically, the engineered software contained on the CPS server down in Florida reached into many servers across the country to systematically search the contents of Barics personal computer. A computer that indisputably was within his home. The specialty software then searched the files contained on the server and computers for known files. Next the software compared specific files contained within baric's computer to controls contained in the coding of the software on the CPS server in florida. Then, the software searches for an IP address of the personal computer that had these files contained on it somewhere inside a home or business. This is typically done by establishing a direct connection between the searching computer and the

computer being searched. After the IP address is obtained the Officer geolocates the computer with the files using the IP address while deploying another software tool. In this particular case the Geolocation was done many times before applying for a warrant. (R. 59)

11. Simply put this is not holding files out the public. Rather, this is a police officer deputized to conduct FBI searches (only with an existing agent, which he didn't have) conducting a massive nationwide search of thousands of personal computers and servers, and even more files contained therein. The government action in this case specifically reached into an area storing files within a home with recognized 4th amendment protections, and then sifted through them at their leisure without a warrant. (R. 59)

12. "Other courts, in assessing the validity of a search without a warrant, have likened a person's privacy expectations in cell phones and electronic devices to that of closed containers in his or her possession." *See, e.g., United States v. Finley*, 477 F.3d 250, 259–60 (5th Cir.2007) (holding that the defendant had a sufficient privacy interest in his cell phone call records to challenge the search therein); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir.1996) (holding that the owner of a pager has the same reasonable expectation of privacy in its data as if it were a closed container); *United States v. Wurie*, 612 F.Supp.2d 104, 109 (D.Mass.2009) ("It seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone."). *State v. Carroll*, 2010 WI 8, ¶ 27, 322 Wis. 2d 299, 319, 778 N.W.2d 1, 10

13. The Search of Ronald Barics personal computer via means of invasive computer forensics constituted a search. Simply put officers of the law deployed a massive hacking operation to reach into and search private servers and personal computers, then search them for specific files, obtain an IP address, and then subsequently geolocate them.

14. The search deployed by the Shawano County Sheriff's office used sense enhancing devices in the form of a computer, two servers and police software to effectively search via the tor network and various servers for content located on a personal computer within a home protected by the 4th amendment. (R. 59) This is a multijurisdictional search without a warrant. The tools used to conduct the search were factually contained within the state of Florida. The locations of the many servers remain unknown. The full extent of personal files searched for hash values unknown but suspected to be national. (R. 59 at 14)

15. Without the use of these Sense Enhancing devices to monitor and

search for specific files on several servers which verify the files location on a personal computer, an area recognized as having 4th amendment protections similar to that of containers in a home, the FBI would know nothing about the Defendant. Without using engineered software to conduct a search of servers across the country, and thousands of computers (many of which are outside the jurisdiction of the officer conducting the warrantless search) for specific information these officers would not have been capable of detecting nor following the Defendants internet activity. They would not have been capable of ascertaining known files on the Defendants computer. (R. 59)

16. On October 14th, 2014 Detective Gordon Kowaleski of the **SHAWANO COUNTY SHERIFFS DEPARTMENT**, conducted a search, outside of his jurisdiction using sense enhancing devices to intrude into the home and personal effects of Ronald Baric, without a warrant. *Exhibit One to Defendants Motion To Suppress date June 17th, 2016, Affidavit of Gordon Kowaleski (R 32-6)*

17. This search intruded into the home and the personal effects of many residents throughout the state. (R. 59-14) "*Q: is it nationwide, do you know, A My understanding is yes*", (R. 59: 11,12) "*I think to better explain to, when somebody runs eMule and they download the program, when, files are created - - or folders are created by default. The incoming folder and attempt folder as that person does searches or downloads files of **any nature**, the files come in in chunks. **The chunks are stored initially in the temp folder** (NOTE: this is the same folder that was created on the user's computer by downloading and running the software) When the file is complete, it gets moved to the incoming folder. (another folder that is created by default on the user's computer) As you build files as a user of the eMule, the software reports the hash values and file names up the eMule servers. When I as a user go to do a search the server will say this person, this person, or however many people have the file you are looking for and will hand me off to the individual peer. And then I as a user download from there.*"

18. On October 14th, Detective Kowalseki used computer and computer software to conduct a search outside of his jurisdiction. (R 59-14)

19. On October 14th, Detective Kowalseki used a computer and computer software to locate, follow and electronically enter the home of Ronald Baric. (R. 59) (R. 32-6) *Exhibit One to Defendants Motion To Suppress date June 17th, 2016, Affidavit of Gordon Kowaleski*

20. From 4:24 GMT to 13:46, nearly twelve hours, investigators from **SHAWANO COUNTY** used sense enhancing tools and methods to intrude

into the home and personal effects of the Defendant Ronald Baric. Who is a resident of Outagamie County. (R. 32-6) *Affidavit of Gordon Kowaleski*

21. In deploying a search using the Gneuttela network investigator Kowaleski was able to search computers throughout the **STATE OF WISCONSIN** for specific information. (R. 32 -6) (R. 59 11-12)

22. Specifically, Detective Kowaleski used a computer and **software not available to the public** to enhance his ability to search through material online throughout entire state of Wisconsin for specific information. (R. 59 8-9)

23. Detective Kowaleski testified on June 22, 2016 that the software he used to search and find Baric through searching his files "is not publically available". *See June 22nd 2016 transcript page 8-9. (R. 59 8-9)*

24. This is inconsistent with the affidavit submitted to the Court in applying for the very warrant that was at issue that represents: "this Detective could then use **publicly available** software to request a list of internet network computers..." (R. 32 6-11) *Affidavit of Kowaleski*

25. "The Court held that the use of "sense-enhancing technology" **that is not in use by the public** and is able to gather information about activity within the home that, absent the technology, could not be gathered without entering the home, **Constitutes a search of the home within the scope of the 4th Amendment.**" *See Kylo v. United States, 533 U.S. 27,40 (2001); see April A. Otterberg, GPS tracking Technology; The case for revisiting knots and shifting the Supreme Courts Theory of the Public Space Under the Fourth Amendment, 46 B.C. L. REV. 661, 693 (2005) (discussing the Kylos Courts development of this new test.)*

26. Besides downplaying the fact that two searches occurred before obtaining an IP or applying for a warrant the **Affidavit of Detective Kowaleski is completely inconsistent with his testimony under oath that the software deployed was not publically available.** (R. 59) (R. 32 6-11)

"Q Earlier today you mentioned the term "my software" when you were referencing how you were plugging in hashtag values to find contraband images or certain key terms. What is the software that you've been using?

A CPS, Child Protective Services - - or Child Protective System. Im sorry

Q Is that something that is produced just for your agency?

A No.

Q Is that something that is publically available?
A No.” – (R. 59 8-9)

27. Compare this to the Affidavit in support for the warrant which indicates publically available software was being deployed. (R. 59) (R. 32 6-11)

28. These files would be contained on a personal computer and are only identified after the officer has searched online using specialty software and servers to find a file contained on a personal computer. “So is it possible that you would get a report *from your software* for a partial file either *being stored or downloaded on somebodys computer*? A. Correct” (R. 59-12)

29. After the sifting of thousands of personal computers for the presence of a specific file to obtain information pertaining to the crime a second search begins.

30. Now that the Officer has acquired the file from the personal computer they have what they need to begin the second search. After the suspect file is found its hashtags (digital signatures) are cross referenced against a list of known hashtags that the FBI has acquired.

31. The second warrantless search uses the IP address obtained by stiffing for files subsequently comparing the contents of those files.

“So I am going into the servers for CPS, which the servers for CPS are going in the servers for emule” - (R. 59-11)

“CPS has its own servers that check the networks, such as Gnutella or ED 2k, eDonkey 2000 Network, which emule typically runs or possibly the K.A.T. network” – (R. 59-11).

Detective Kowaleski goes on to describe the locations of files on personal computers and how they are accessed, sifted and compared using the CPS software.

“I think to better explain it, when somebody runs emule and they download the program, files are created- - or folders are created by default” (R 59-11)

This sentence is describing how when a personal computer user downloads the emule software (which is used to share legal files as well) the downloaded program automatically creates local files on the Personal Computer that are accessible by search to the emule network.

These files were discovered by officer Kowaleski, because CPS has a server and specialty software he used to sift the legal and illegal files stored in these automatically created files (stored locally on personal computers).

32. The software then identifies the file is present on the computer and cross checks it against a control. **This is a massive monitoring and search that is conducted automatically by the server.** “CPS has its own servers that check the networks, such as Gnutella or ED 2k, eDonkey 2000 Network, which emule typically runs on K.A.T. Then it will show up on the screen I open that there is a target within my area. So I am going into the servers for CPS, which the servers for CPS are going in the servers for eMule” (R. 59-11) It is important to note that through the servers for the tor client the items stored on a personal computer are accessed and checked.

33. The next search is also identified in the June 22nd testimony of Detective Kowaleski “When the server from the software I use finds those, it takes the IP address, because in order for peer-to-peer to work, the IP address has to be available, it geo locates that on a map. If it comes back to my area it will show up on my screen as a target.” (R. 59-9)

34. Ordinary citizens, even citizens who are subject to diminished privacy interests because they have been detained, have a legitimate expectation of privacy in the contents of their electronic devices. *See Riley v. California*, U.S., 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014); *State v. Carroll*, 2010 WI 8, ¶ 27, 322 Wis.2d 299, 778 N.W.2d 1. *State v. Purtell*, 2014 WI 101, ¶ 28, 359 Wis. 2d 212, 232, 851 N.W.2d 417, 427

35. The United States Court of Appeals for the District of Columbia Circuit reversed the conviction because of admission of the evidence obtained by warrantless use of the GPS device which, it said, violated the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544 (2010) *United States v. Jones*, 565 U.S. 400, 404, 132 S. Ct. 945, 949, 181 L. Ed. 2d 911 (2012)

36. The use of wide spread sense enhancing devices to conduct many warrantless searches of files on personal computers and servers, outside of the Jurisdiction of the officer and without meeting the restrictions on his deputization as well as conducting the search to geolocate the Defendant resulted in a warrantless search protected by the 4th amendment.

CONCLUSION

The Denial of the Baric's suppression motions should be reversed and his Judgment of conviction vacated. The conduct of Detective Kowaleski amounted to several warrantless searches by way of deploying not publically available, sense enhancing devices, to ascertain contents within the house that would otherwise not be available. Further, the Special Agents that responded to Baric's home failed to properly attain freely given consent.

THEREFORE, the decisions to deny the Appellants January and June 2016 Motions should be overturned and the matter should be remitted to the Circuit Court with the instruction that the Appellants Motions be granted.

Dated this 13th day of July, 2017.

Respectfully Submitted,

JOHN MILLER CARROLL
LAW OFFICE

By: 

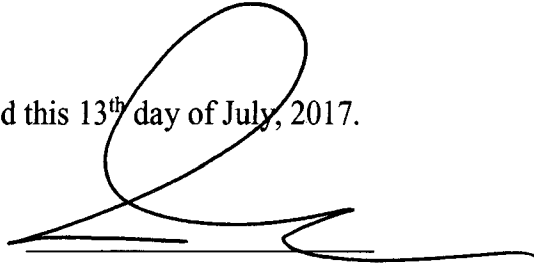
John Miller Carroll
State Bar # 1010478

226 S. State St.
Appleton, WI 54911
(920)734-4878

FORM AND LENGTH CERTIFICATION

I, John M. Carroll, hereby certify that this brief conforms to the rules contained in s. 809.19 (8)(b) and (c) for a brief and appendix produced with a proportional serif font. The length of this brief is 2,985 words.

Dated this 13th day of July, 2017.

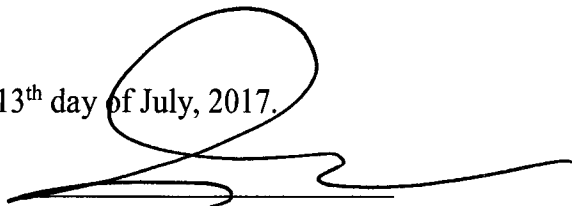
A handwritten signature in black ink, consisting of a large, stylized 'J' followed by 'M' and 'C'.

John Miller Carroll
State Bar #1010478

ELECTRONIC BRIEF CERTIFICATION

I, John M. Carroll, hereby certify in accordance with Sec. 809.19(12)(f), Stats, that I have filed an electronic copy of a brief, which is identical to this paper copy.

Dated this 13th day of July, 2017.

A handwritten signature in black ink, identical to the one above, consisting of a large, stylized 'J' followed by 'M' and 'C'.

John Miller Carroll
State Bar #01010478