

FILED
JUL 14, 2014
Court of Appeals
Division III
State of Washington

32058-8-III

COURT OF APPEALS

DIVISION III

OF THE STATE OF WASHINGTON

STATE OF WASHINGTON, RESPONDENT

V.

CASEY D. PEPPIN, APPELLANT

APPEAL FROM THE SUPERIOR COURT

OF SPOKANE COUNTY

BRIEF OF RESPONDENT

STEVEN J. TUCKER
PROSECUTING ATTORNEY

ANDREW J. METTS
DEPUTY PROSECUTING

ATTORNEYS FOR RESPONDENT

ATTORNEY

COUNTY-CITY PUBLIC SAFETY BUILDING
WEST 1100 MALLON
SPOKANE, WASHINGTON 99260
(509) 477-3662

INDEX

I.	ASSIGNMENT OF ERROR.....	1
II.	ISSUES PERTAINING TO ASSIGNMENTS OF ERROR.....	1
III.	STATEMENT OF THE CASE.....	1
IV.	ARGUMENT.....	1
A.	THE DEFENDANT FAILED TO DEMONSTRATE THAT LAW ENFORCEMENT HAD PROGRAMS THAT ALLOWED DEEPER ACCESS TO THE DEFENDANT’S COMPUTER THAN THOSE AVAILABLE TO THE PUBLIC.....	1
B.	THE DEFENDANT HAS NOT SHOWN THAT HE MAINTAINED A RIGHT TO PRIVACY IN FILES READILY AVAILABLE TO THE GENERAL PUBLIC.....	4
C.	THE DEFENDANT’S REASONABLE EXPECTATION OF PRIVACY EVAPORATED WHEN HE INSTALLED A FILE SHARING P2P PROGRAM.....	5
D.	THE TRIAL COURT CORRECTLY DENIED THE DEFENDANT’S MOTION TO SUPPRESS BASED ON THE FACT THAT THE DEFENDANT COULD NOT HAVE A LEGITIMATE EXPECTATION OF PRIVACY IN FILES PLACED ON A FILE SHARING PROGRAM.....	6
V.	CONCLUSION.....	6

TABLE OF AUTHORITIES

WASHINGTON STATE CASES

State v. Young, 123 Wn.2d 173, 867 P.2d 593 (1994)..... 2

SUPREME COURT CASES

Katz v. United States, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) 5

Kyllo v. U.S., 533 U.S. 27, 121 S. Ct. 2038, U.S. Or., (2001) 2

FEDERAL COURT CASES

U.S. v. Borowy, 595 F.3d 1045 C.A.9 (Nev.), (2010)..... 5

U.S. v. Ganoë, 538 F.3d 1117, C.A.9 (Cal.),(2008)
(*cert. denied Ganoë v. U.S.*, 556 U.S. 1202, 129 S.Ct. 2037, 173 L.Ed.2d
1122, 77 USLW 3576 (2009) (No. 08-9446)..... 4, 5

I. ASSIGNMENT OF ERROR

The trial court erred in failing to grant Mr. Peppin's motion to suppress evidence that was the product of an illegal search.

II. ISSUES PERTAINING TO ASSIGNMENTS OF ERROR

- A. Has the defendant shown that law enforcement used a search program that was substantially different from that available to the public for free?
- B. Has the defendant shown that he had a right to privacy in the files readily available to the general public?
- C. Was the remote warrantless search of the defendant's computer a violation of the defendant's right to privacy?
- D. Did the trial court properly deny the motion to suppress the evidence of the files in the public sharing folder of the defendant's computer?

III. STATEMENT OF THE CASE

For the purposes of this appeal, the state accepts the defendant's version of the Statement of the Case.

IV. ARGUMENT

- A. THE DEFENDANT FAILED TO DEMONSTRATE THAT LAW ENFORCEMENT HAD PROGRAMS THAT ALLOWED DEEPER ACCESS TO THE DEFENDANT'S COMPUTER THAN THOSE AVAILABLE TO THE PUBLIC.

The first area needing to be corrected is the defendant's overall claims that the police used "enhanced" software that gave the police information that the

average user would not be able to obtain. This is not the case. For example, the defendant tries to infer that it is unfair for law enforcement to use Roundup and other programs specifically designed for law enforcement. Brf. of App., p. 5. The part not mentioned by the defendant is that the programs used by law enforcement are for *convenience* of the law enforcement personnel. The programs mentioned by the defendant cannot give law enforcement the power to penetrate into a person's computer greater than that available to the average user. The law enforcement programs simply allow organization of search limitations a collection of results of a search for computers that use any publically available P2P file sharing program such as that used by the defendant. The reason for the programs used by law enforcement is for convenience in confining searches to specific areas and structured returns of any "hits."

It would appear that the defendant is trying to convince this court that law enforcement was using their versions of the P2P software in a manner that made the law enforcement "snooping" somehow fall under the ambit of *Kyllo v. U.S.*, 533 U.S. 27, 121 S. Ct. 2038, U.S. Or., (2001) or *State v. Young*, 123 Wn.2d 173, 867 P.2d 593 (1994). The State maintains that such is not the case. The software may have made it easier for law enforcement to do their jobs, but there was no testimony that the native ability of law enforcement software was different from any public software. By using a file sharing program, the defendant conducted

the equivalent of throwing the child pornography files on his front lawn for all to see.

At the motion hearing, the defendant called Jennifer McCamm and qualified her as an expert in this area of computers. The defendant downloaded and used “FrostWire,” a P2P sharing program. This is a free program with a default setting that shares files. RP 6, 7.

Ms. McCamm engaged in speculation when she testified that the law enforcement programs get information that the regular users do not get. On page 10 of the transcript, Ms. McCamm admits that she has never seen the law enforcement software. RP 10, 13.

Yet, in spite of never having seen the law enforcement software, Ms. McCamm states that law enforcement can get items that the public cannot. RP 10. Ms. McCamm opines that the police software can get “IP” addresses and can verify files using a “hash” number. RP 10. Ms. McCamm does not note whether the public can do the same thing. Ms. McCamm was not exactly certain what that law enforcement software could do. She does mention that she “thinks” the software had the ability to set search limits. RP 15. The ability to set search limits does not imply that the police version of P2P software has any greater ability to remotely look for files on a defendant’s computer than the more simple programs such as FrostWire and Limeware.

The defendant's expert had no solid knowledge about the law enforcement programs as she had never seen or used one. The issue is whether the defendant had an expectation of privacy that was violated by law enforcement. As the P2P software was described by the defendant's expert, the whole point of loading FrostWire (and its ilk) was to access shared files across the P2P network.

If an average user has the patience, he or she could engage in a search of the public Gnutella network to find all computers possessing and sharing the requested data, in this case, child pornography. In this case, the defendant's computer contained images of child pornography that were available to anyone accessing the P2P network.

B. THE DEFENDANT HAS NOT SHOWN THAT HE MAINTAINED A RIGHT TO PRIVACY IN FILES READILY AVAILABLE TO THE GENERAL PUBLIC.

The motion being contested by the defendant was decided on the basis that the defendant could not have had a reasonable expectation of privacy in his files that had to be placed in the "share" portion of his software program in order to make the files available to the public. The federal court in *U.S. v. Ganoe*, 538 F.3d 1117, C.A.9 (Cal.), (2008) (*cert. denied Ganoe v. U.S.*, 556 U.S. 1202, 129 S.Ct. 2037, 173 L.Ed.2d 1122, 77 USLW 3576 (2009) (No. 08-9446), has examined the issue of police remotely examining public computer files and stated, "Ganoe 'knew or should have known that the software might allow others to access his computer' and thus lacked a reasonable expectation of privacy in the

files stored on his computer. We agree and affirm the denial of the motion to suppress.” *Id.* at 1127.

Although as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, see *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir.2007), we fail to see how this expectation can survive Ganoë's decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program.

U.S. v. Ganoë, supra at 1127.

C. THE DEFENDANT’S REASONABLE EXPECTATION OF PRIVACY EVAPORATED WHEN HE INSTALLED A FILE SHARING P2P PROGRAM.

While the file sharing program used by Ganoë was Limewire and that used by the defendant was FrostWire, both are P2P file sharing software and the results are the same. The court in *U.S. v. Borowy*, 595 F.3d 1045 C.A.9 (Nev.), (2010), faced an argument under *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), government conduct qualifies as a search only if it violates a reasonable expectation of privacy.

The gist of the above cited case law is that a defendant’s expectation of privacy arguments cannot survive the defendant’s decision to install and use file sharing programs such as that installed on this defendant’s computer. The defendant in this case was aware of the file transferring nature of the software he was using; he had used that feature for years. There is little value in installing P2P file sharing software except for the purpose of making selected files on a personal computer available to anyone who is browsing the Gnutella network.

The defendant has not shown that law enforcement violated his right to privacy when the defendant loaded and used a P2P file sharing software program. This program allowed the public to access any file placed in the computer's "share" directory. As noted by the previously mentioned case law, there can be no legitimate expectation of privacy with such a voluntary arrangement.

D. THE TRIAL COURT CORRECTLY DENIED THE DEFENDANT'S MOTION TO SUPPRESS BASED ON THE FACT THAT THE DEFENDANT COULD NOT HAVE A LEGITIMATE EXPECTATION OF PRIVACY IN FILES PLACED ON A FILE SHARING PROGRAM.


The trial court was correct in denying the defendant's motion to suppress.

V. CONCLUSION

For the reasons stated previously, the State respectfully requests that the decision of the trial court denying the defendant's motion to suppress be affirmed.

Dated this 9th day of July, 2014.

STEVEN J. TUCKER
Prosecuting Attorney


Andrew J. Metts #19578
Deputy Prosecuting Attorney
Attorney for Respondent

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

DIVISION III

STATE OF WASHINGTON,)
)
 Respondent,) NO. 32058-8-III
 v.)
)
CASEY D. PEPPIN,)
)
 Appellant,)

I certify under penalty of perjury under the laws of the State of Washington, that on July 9, 2014, I e-mailed a copy of the Respondent's Brief in this matter, pursuant to the parties' agreement, to:

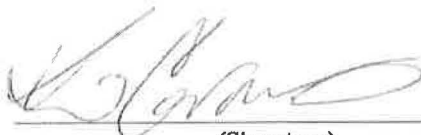
David N. Gasch, Esq.
gaschlaw@msn.com

and mailed a copy to:

Casey Dullea Peppin
DOC #367184
Airway Heights Corrections Center
P.O. Box 2049
Airway Heights, WA 99001

7/9/2014
(Date)

Spokane, WA
(Place)



(Signature)