FILED

APR 06 2012

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff - Appellee, v. JOHN HENRY AHRNDT, Defendant - Appellant.	No. 10-30281 D.C. No. 3:08-cr-00468-KI-1 MEMORANDUM*

Appeal from the United States District Court
for the District of Oregon
Garr M. King, District Judge, Presiding

Argued and Submitted March 7, 2012
Portland, Oregon

Before: W. FLETCHER, FISHER and BYBEE, Circuit Judges.

John Henry Ahrndt appeals the district court's denial of his motion to suppress evidence he claims resulted from a police officer's unconstitutional warrantless search made by connecting to Ahrndt's personal wireless network and opening one of his shared files. We reverse and remand for additional factfinding, as we explain.

*This disposition is not appropriate for publication and is not precedent except as provided by 9th Cir. R. 36-3.

JH, a resident of Aloha, Oregon, was using her computer at home and connected to a nearby unsecured wireless network to access the Internet. When she opened her iTunes software, she noticed a shared library called "Dad's Limewire Tunes." She opened the library and observed several files with names indicating that the files contained child pornography. After JH called the police, Deputy John McCullough arrived at her residence and directed her to repeat the process of connecting to the network and accessing the shared library. McCullough also asked JH to open one of the images; the image she opened depicted a minor engaged in sexually explicit conduct. Based on this information, law enforcement officers obtained a search warrant to connect to the wireless network and determined that the network belonged to Ahrndt. Officers then obtained and executed a warrant to search Ahrndt's home, from which they seized storage media that contained images of child pornography.

The central issue is whether connecting to Ahrndt's network, accessing his shared library and opening one of his files amounted to a "search" within the meaning of the Fourth Amendment. A search occurs when the government violates an individual's reasonable expectation of privacy. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984). "An individual has a reasonable expectation of privacy if he can demonstrate a subjective expectation that his activities would

be private, and he [can] show that his expectation was one that society is prepared to recognize as reasonable." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (internal quotation marks omitted) (alteration in original). A search also occurs whenever "the Government obtains information by physically intruding on a constitutionally protected area." *United States v. Jones*, 132 S. Ct. 945, 950 n.3 (2012).

1. The district court held that no search occurred because Ahrndt had no objectively reasonable or subjective expectation of privacy in the computer file that Deputy McCullough accessed. The court's conclusion was based on its finding or assumption that Ahrndt used iTunes to share his files, a process that would have required Ahrndt to take several affirmative steps. This finding, however, is unsupported by the record. Special Agents James Cole and Anthony Onstad, the two law enforcement officers who testified about iTunes, each testified that they had no knowledge whether JH's iTunes software was capable of detecting files on Ahrndt's computer that Ahrndt did not affirmatively share by using iTunes. Robert Young, the only computer expert who appeared, testified that JH's iTunes software was capable of detecting files that were shared by other programs on Ahrndt's computer, such as Limewire. There is insufficient evidence that Ahrndt took affirmative actions to enable open sharing in this manner. Furthermore, there is no

evidence that Ahrndt ever installed iTunes on his computer. Thus it was clearly erroneous to find that Ahrndt used iTunes to affirmatively share his files over the network, and from that finding to conclude that Ahrndt lacked a reasonable expectation of privacy. *See Red Lion Hotels Franchising, Inc. v. MAK, LLC*, 663 F.3d 1080, 1087 (9th Cir. 2011).

2. Further factfinding regarding the following questions also may be beneficial in determining whether Ahrndt had a reasonable expectation of privacy in his computer files:

- As a technical matter, is sharing files over a wireless network accurately characterized as a "broadcast" of the contents of those files, such that JH's computer simply intercepted Ahrndt's images outside Ahrndt's home? Or, alternatively, did the act of connecting to Ahrndt's network, accessing his library and opening the image involve sending wireless signals into Ahrndt's home to communicate with his router and computer?

- Did Ahrndt intentionally enable sharing of his files over his wireless network? If not, did he know or should he have known that others could access his files by connecting to his wireless network?

- Was the image in "Dad's LimeWire Tunes" library that JH and McCullough opened accessible over the Internet by Limewire users at the time JH and McCullough accessed the files, or at any time prior?

Given the flawed premise regarding Ahrnt's affirmative use of iTunes, and the technical questions we have noted, we reverse the district court's denial of Ahrndt's motion to suppress, and remand for further proceedings and factfinding

regarding the questions identified above, and any other questions the court deems relevant. *See United States v. Wright*, 625 F.3d 583, 604, 620 (9th Cir. 2010) (remanding for factfinding in the context of a suppression motion). The court should also evaluate whether a search occurred in light of *Jones*, 132 S. Ct. 945, decided after the district court's original ruling. The panel shall retain jurisdiction over any further appeals.[1]

REVERSED and REMANDED.

[1] The government argues that, even if an unconstitutional search occurred, suppression would be inappropriate because McCullough acted in good faith. We do not reach that issue.