FILED
JAN 2 % 2010

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JOHN HENRY AHRNDT,

Defendant.

Criminal Case No. 08-468-KI

OPINION AND ORDER

Kent S. Robinson
United States Attorney
District of Oregon
Gregory R. Nyhus
United States Attorney's Office
1000 SW Third Avenue, Suite 600
Portland, Oregon 97204

Attorneys for Plaintiff

Francesca Freccero
Federal Public Defenders
101 SW Main, Suite 1700
Portland , Oregon 97204

Attorney for Defendant

KING, Judge:

Defendant John Henry Ahrndt, a convicted sex offender, is charged with transportation
and possession of child pornography in violation of 18 U.S.C. §§ 2252A, 2253. Before the court
is defendant's Motion to Suppress (#23), which seeks to suppress evidence defendant alleges was
obtained as a result of an illegal search in violation of his constitutional rights under the Fourth
Amendment. For the following reasons, I deny defendant's motion.

FACTS

The following facts were adduced at an evidentiary hearing. On February 21, 2007, a
woman referred to as JH was using her personal computer at her home in Aloha, Oregon. She
was connected to the internet via her own wireless network, but when her wireless network
malfunctioned, her computer automatically picked up another nearby wireless network called
"Belkin54G." Belkin54G refers to a wireless router, made by the company Belkin, that
broadcasts wireless internet in a roughly 400 foot radius.

JH connected to the internet via the Belkin54G wireless network. JH began using her
iTunes software. The iTunes software is designed to organize and play audio, video, and image
files. The iTunes software, when configured to "share," also allows users to browse music and
video that is stored in the iTunes libraries of other computers on the same wireless network.
When JH opened her iTunes, she noticed another user's library was available for sharing. JH

Page 2 - OPINION AND ORDER

opened the shared library and found a subfolder called "Dad's Limewire Tunes." JH opened

Dad's Limewire Tunes and observed files with names such as "11-yr old masturbating" and

words such as "tiny," "fuck," and "cunt," in conjunction with acronyms indicating age like

"5yoa" and "8yoa." Ex. A at 4.

JH noted twenty-five to thirty files with names that indicated child pornography, but did

not open any of the files. She did, however, contact the Washington County Sheriff's Office and

Officer McCullough responded at roughly 11:30 a.m. Officer McCullough duplicated the steps

that JH had used to access Dad's Limewire Tunes. Officer McCullough observed the same file

names and noted that some of the age acronyms in the files, e.g. "5yoa," were followed by the

words "getting raped" and "being raped." Ex. A at 5. Officer McCullough then asked JH to

open one of the files. JH opened the file briefly and the two saw a photo of a minor engaged in

sexually explicit conduct.

Two days later, on February 23, 2007, Washington County Sheriff's Office Detective Ray

Marcom and Department of Homeland Security Senior Special Agent James Cole interviewed JH

further about the incident. JH related to Marcom and Cole that she often had problems with

internet connectivity and would unwittingly become connected to the Belkin54G wireless

network. JH observed other wireless networks that broadcasted within reach of her house, but all

the other networks were password-protected and JH could not access them.

JH reported that she had accessed the same wireless network when she first moved in to

her house. At that time, only two nearby residences were occupied. JH, a former child protective

services worker, was uneasy about one of the two houses, 4390 SW 184th Ave., which was about

150 feet away. She said "the house has the windows blacked out and while there are children's

Page 3 - OPINION AND ORDER

toys in the yard she has seen little activity and no children since she moved in." Ex. A at 48-49.

Deputy McCullough subsequently ran the license plates of a car in the driveway of 4390 SW

184th Ave. and learned that defendant John Henry Ahrndt, a convicted sex offender, lives there.

Fredrick Harmon, a friend and tenant of defendant, also lives at the residence in a room above the

garage.

On April 2, 2007, Agent Cole applied to United States Magistrate Judge Dennis Hubel for

a search warrant to access the Belkin54g wireless network for the purpose of determining the

internet protocol ("IP") address of the router. An IP address would allow investigators to find out

from an internet service provider who owned the Belkin54G wireless network. Judge Hubel

granted the warrant the same day. On April 7, 2007, Agent Cole drove near the house, accessed

the Belkin54G network, and determined the network's IP address. Through the American

Registry for Internet Numbers, Agent Cole learned that the IP address belonged to Comcast. He

served a summons on Comcast and learned that defendant was the Comcast subscriber for the IP

address in question.

On April 17, 2007, Agent Cole obtained a second search warrant from Judge Hubel

allowing a search of the home for wireless routers, computers, and any files or storage media that

could contain images of child pornography. The next morning officers searched defendant's

home and seized one computer, a Belkin wireless router, various hard drives, numerous disc

media and flash media.

Agents interviewed defendant when they executed the search warrant. They told him he

was not under arrest and that he was free to leave at any time. Defendant, however, stayed and

gave what seems to be a candid and lengthy account of his child pornography addiction. He

Page 4 - OPINION AND ORDER

admitted to downloading child pornography as recently as eight months previously using the

peer-to-peer file-sharing software Limewire, which integrates with iTunes. He also told agents

that he had deleted all the images, but that they would find child pornography images if they were

capable of recovering deleted images. Specifically, he told the agents they would find deleted

images on his external hard drives, which he had converted from hard drives of his old

computers. He denied, however, that there was any child pornography on his current computer,

which he had obtained from a member of his church in January 2007, and subsequently scrubbed

of the church member's residual personal information. Defendant also told agents that no one

else uses his computer, but that Mr. Harmon, his friend and tenant, uses the wireless network.

A subsequent computer forensic examination of the equipment found images of child

pornography on the current computer.

Defendant now brings a motion to suppress all evidence seized after Officer

McCullough's initial access of defendant's files through JH's computer, on the theory that without

McCullough's statement, the first and second warrants would not have issued.

STANDARD

"In order to benefit from Fourth Amendment protections, an individual must demonstrate

a subjective expectation that his activities would be private, and he must show that his

expectation was one that society is prepared to recognize as reasonable." U.S. v. Young, 573

F.3d 711, 715-16 (9th Cir. 2009) (internal citations omitted). Evidence seized in violation of the

Fourth Amendment constitutes an illegal search or seizure. See Pennsylvania Bd. of Prob. and

Parole v. Scott, 524 U.S. 357, 362 (1998). Evidence seized during an illegal search is tainted and

should not be included in the affidavit for a search warrant. Inclusion of tainted evidence in the

affidavit though, does not in itself taint the warrant or evidence seized pursuant to it. The court should excise the tainted evidence and decide if the remaining, untainted evidence provides probable cause to issue a warrant. United States v. Bishop, 264 F.3d 919, 924 (9th Cir. 2001). Furthermore, to be untainted by the prior illegal search, the officer's decision to seek the warrant must not have been prompted by what he saw during the prior illegal search. United States v. Hill, 55 F.3d 479, 481 (9th Cir. 1995).

DISCUSSION

"The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored." Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904 (9th Cir. 2008).

The issue in this case is whether the Fourth Amendment provides a reasonable, subjective expectation of privacy in the contents of a shared iTunes library on a personal computer connected to an unsecured home wireless network.

Defendant argues that when Officer McCullough duplicated the steps taken by JH and viewed defendant's child pornography, he conducted an illegal warrantless search in violation of defendant's Fourth Amendment right to privacy. According to Defendant, a warrantless search occurred because the facts indicate Officer McCullough's violated his reasonable expectation of privacy in his computer files. Alternatively, defendant argues that his expectation of privacy was per se reasonable because JH's conduct was illegal under the Electronic Communications Privacy Act. Defendant contends that all information gathered subsequently was fruit of the poisonous

tree and thus inadmissible. The government disagrees with defendant's contentions, maintaining

that defendant's conduct in operating his home computer system eliminated his right to privacy.

I.   Whether a Search Occurred

"[A] Fourth Amendment search does *not* occur–even when the explicitly protected

location of a house is concerned–unless 'the individual manifested a subjective expectation of

privacy in the object of the challenged search,' and 'society is willing to recognize that

expectation as reasonable.'" Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v.

Ciraolo, 476 U.S. 207, 211 (1986)).

In order to assess what society recognizes as reasonable in this case, I begin by evaluating

the relevant hardware and its settings, and then turn to the relevant software and its settings.

A.   Diminished Reasonable Expectation of Privacy in Data Broadcast via Unsecured
      Wireless Network Router

At the suppression hearing, defendant argued that a wireless network should be given no

less protection than a hardwired network under the Fourth Amendment. According to defendant,

if, hypothetically, defendant had possessed a hardwired home network, and officer McCullough

had obtained access to defendant's computer via the hardwired network, there would no question

that his access violated a reasonable expectation of privacy.

Courts, however, have long held that different communications hardware and

technologies carry different reasonable expectations of privacy. For example, while users of

traditional hardwired phones generally have a reasonable expectation of privacy in their

conversations, Katz v. United States, 389 U.S. 347, 352 (1967), users of cordless phones

generally do not because of the ease of intercepting wireless transmissions. See, e.g., United

States v. Hall, 488 F.2d 193, 198 (9th Cir. 1973) (particular speakers on radio telephones knew they could be overheard, and thus had no justifiable expectation of privacy); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989) (no justifiable expectation of privacy in conversations on cordless telephone); United States v. Hoffa, 436 F.2d 1243, 1247 (7th Cir. 1970) (no expectation of privacy for conversation over mobile telephones under Fourth Amendment analysis); Edwards v. Bardwell, 632 F. Supp. 584, 589 (M.D. La. 1986) (no privacy expectation for conversation "broadcast by radio in all directions to be overheard by countless people"); State v. DeLaurier, 488 A.2d 688, 694 (R.I. 1985) (phone came with manual alerting owner that conversation could be transmitted to others);

In the leading case on the subject, Tyler, the Berodt family discovered that their cordless telephone could intercept the cordless phone conversations of Scott Tyler, who lived four houses down the street. 877 F.2d at 705. After hearing conversations that indicated criminal activity, the Berodts contacted police, who, without a warrant, urged them to continue monitoring the conversations. Id. at 705-06. Police later filed criminal charges against Tyler. Id. at 706. After defeating prosecution in his criminal trial, Tyler brought suit against the Berodts, the county, and police. Id. The Eighth Circuit Court of Appeals, summing up precedent from a number of jurisdictions, wrote "[c]ourts have not accepted the assertions of privacy expectations by speakers who were aware that their conversation was being transmitted by cordless telephone." Id. The Tyler court granted summary judgment for the defendants, holding that Tyler had no justifiable expectation of privacy in his conversations on his cordless telephone. Id. at 707. In so holding, the Eighth Circuit acknowledged that the expectation of privacy in wireless phones is different

from that of wired phones because the practical realities of the different technologies give rise to varied subjective and objective expectations.

The expectation of privacy in cordless phones is analogous to the expectation of privacy in wireless networks, because wireless networks are so easily intercepted. Wireless networks are similar to cordless phones in that they transmit data over radio waves. James Ridge, What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive, 49 S. Tex. L. Rev. 725, 735 (2008). Unlike cordless phone signals, however, a wireless router signal can be received by an unauthorized user even though that user will not usually encounter personal or confidential information. Daniel Kamitaki, Beyond E-mail: Threats to Network Security and Privileged Information for the Modern Law Firm, 15 S. Cal. Interdisc. L.J. 307, 340 (2006). By using the wireless network signal for internet access, a joyrider[1] is not made privy to personal information of the broadcasting user. Ned Snow, The Law of Computer Trespass: Cyber Security or Virtual Entrapment?, 2007 Ark. L. Notes 109, 110 (2007). Information transmitted to and from the internet is invisible to the other user of a Wi-Fi signal. Id. In addition, most joyriders assume that using another person's unsecured wireless connection is entirely legal, Kamitaki, supra at 340-41, and experts have pronounced it ethical. Randy Cohen, The Ethicist: Wi-Fi Fairness, N.Y. Times, Feb. 8, 2004, at 6, available at 2004 WLNR 5575601. In any event, accidental unauthorized use of other people's wireless networks is a fairly common occurrence in densely populated urban environments. Kamitaki, supra at 341. Purposeful unauthorized use is perhaps equally ubiquitous, because, as one high-technology

---

[1] A "joyrider" is someone who "use[s] an open Wi-Fi connection to access the Internet." Benjamin Kern, Whacking, Joyriding, and War-Driving: Roaming Use of Wi-Fi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101, 138 (2004).

researcher put it, "Wi-Fi is in the air, and it is a very low curb, if you will, to step up and use it." Michel Marriott, Hey Neighbor, Stop Piggybacking on My Wireless, N.Y. Times, Mar. 5, 2006, at 11, available at 2006 WLNR 3698466.

Here, defendant used a Belkin54G wireless router to blanket his house and the surrounding area with wireless internet. He did not password-protect the wireless network, so any person within range could access it. JH had accessed the Belkin54G router multiple times. At the hearing, special agent Tony Onstadt testified that although the default setting of the Belkin54G router is not to have password protection, the router comes with a manual that includes detailed instructions on how to password-protect the router. According to his testimony, the manual stresses the importance of password protection. Agent Onstadt also testified that the range of the router was up to 400 feet in the shape of a donut around the house.

As a result of the ease and frequency with which people use others' wireless networks, I conclude that society recognizes a lower expectation of privacy in information broadcast via an unsecured wireless network router than in information transmitted through a hardwired network or password-protected network. Society's recognition of a lower expectation of privacy in unsecured wireless networks, however, does not alone eliminate defendant's right to privacy under the Fourth Amendment. In order to hold that defendant had no right to privacy, it is also necessary to find that society would not recognize as reasonable an expectation of privacy in the contents of a shared iTunes library available for streaming on an unsecured wireless network.

   B.   No Reasonable Expectation of Privacy in Shared iTunes Library on Unsecured
        Wireless Network

As a general matter an individual has an objectively reasonable expectation of privacy in his personal computer. United States v. Heckenkamp, 482 F.3d 1140, 1146 (9th Cir. 2007). The expectation of privacy in the information on one's computer, however, can be diminished by one's conduct with the computer. See United States v. Ganoe, 538 F.3d 1117, 1127 (2008). For example, when a person uses peer-to-peer file sharing software to download child pornography from others, but fails to configure his computer not to share his own files, he "open[s] up his download folder to the world, including [police]." If the individual "kn[ows] or should [know] that the software [installed on the computer] might allow others to access his computer," he "lack[s] a reasonable expectation of privacy in the files stored on his computer."

In Ganoe, the defendant used the LimeWire software to download images of child pornography. Id. at 1119. A government agent using LimeWire to locate people who download child pornography searched for certain keywords, and found the defendant's computer. The agent used the software's "Browse Host" feature to view the files on the defendant's computer, and he found images of child pornography. The agent downloaded the files and used the downloads to discover the IP address of the computer and the owner's address and identity. The agent used the information to obtain a search warrant, and a subsequent search yielded a computer with child pornography. The defendant moved to suppress the evidence, and argued that when the agent used LimeWire to access the child pornography files, he conducted an illegal warrantless search under the Fourth Amendment. Id. at 1127. He argued that he did not know that others would be able to access the files stored on his computer. The Ninth Circuit Court of Appeals, however, upheld the district court's denial of the motion to suppress. The court, analogizing to the plain view doctrine,

Page 11 - OPINION AND ORDER

"fail[ed] to see how th[e] expectation [of privacy] can survive [the defendant]'s decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program . . . . To argue that [defendant] lacked the technical savvy or good sense to configure [his software] to prevent access to his pornography files is like saying that he did not know enough to close his drapes."

Id.

The software used in Ganoe, LimeWire, is a file-sharing program that can be downloaded from the internet free of charge. Id. at 1119. It allows users to search for and share with one another various types of files, including music, movies, and pictures, on the computers of other persons with LimeWire. LimeWire users must choose when they install the program whether or not to share files on their computers with other LimeWire users. Id. at 1127. LimeWire users can click on an icon to connect their computer to other computers online that are also running LimeWire. Id. at 1119. Users can type search terms and receive a list of responsive files available on other computers connected to the internet and using LimeWire. LimeWire has a "Browse Host" feature that allows other users to view, without downloading, all of the files being shared by a particular "Host" computer. Id.

Defendant attempts to distinguish the present case from Ganoe. Defendant argues that use of a file-sharing program such as LimeWire is different from using an unsecured wireless network.[2] Defendant argues that he was not offering his files over the internet. Rather, in defendant's view, he was merely connected to his home wireless network, which exists

_____

[2]Ahrndt used LimeWire, the same software used in Ganoe, to download the child pornography in this case. The folder that JH and Officer McCullough viewed was called "Dad's LimeWire Tunes" because LimeWire has the capability to integrate with iTunes and automatically places all downloaded material in a LimeWire playlist in the iTunes library. Nevertheless, the child pornography in this case was discovered via the iTunes software, not the LimeWire software.

independently of the internet. Defendant analogizes sharing files over the internet with

LimeWire to announcing information in a public forum. Conversely, in defendant's view, using

an unsecured home wireless network is like having a conversation behind a closed, but unlocked

door.

Defendant's argument and analogy, however, ignore certain key facts and misunderstand

crucial technological details. Defendant was not merely using his unsecured wireless network.

He was also using his iTunes software, and its preferences were set to actively share his music,

movies, and pictures with anyone who had access to the same wireless network.

The iTunes software is a robust, multipurpose music and video management software

with many capabilities. Kent Schoen, Metro-Goldwyn-Mayer v. Grokster: Unpredictability in

Digital Copyright Law, 5 Nw. J. Tech. & Intell. Prop. 156, 166 (2006). Users can import music

from compact discs and store it in their iTunes library. Users can also purchase and download

music, videos, and images from any number of sources for storage and playback in their iTunes

library. Additionally, users are able to share iTunes content over networks, within which each

user can access another user's files. Within a network, a user can listen to another user's music or

view another's movies or images, but he cannot download files from another user. Id.

Special agent James Cole testified that the default setting of iTunes is *not* to share music

or images. Agent Cole's testimony is confirmed by the Apple support website, which lists six

affirmative steps a user must take in the software's preferences in order to enable sharing.

iTunes: How to share your music, http://support.apple.com/kb/HT2688 (last visited Jan. 21,

2010). The iTunes website explains in a section called "Sharing over a Network" how the

functionality works: "[e]nable sharing in iTunes preferences, and users on your network can play

Page 13 - OPINION AND ORDER

media from your library through your local network. Choose whether they have access to everything in your library or just specific playlists. Add a password to your shared library for limited access." iTunes A to Z, http://www.apple.com/itunes/features/#bonjoursharing (last visited Jan. 14, 2010).

LimeWire, the software used in Ganoe, shares important similarities with iTunes. Both can be downloaded legally for free. Both require users to set preferences that either allow or block other users from browsing and sharing their files. After enabling sharing, both programs allow users to view the contents of the shared libraries of other users.

There are differences as well—iTunes does not, like LimeWire, allow other users to download a copy of the content. iTunes is also distinguishable in that it only shares over a network, but not, like LimeWire, over the internet with users in far flung locations. Rather, sharing is limited to users connected to the network—in this case, anyone with a laptop within 400 feet of defendant's house.

Despite the differences, the use of iTunes to share on an unsecured wireless network is not like a private conversation behind an unlocked door. Nor are files shared by LimeWire like an announcement in a public forum, because users do not actively send files to anyone. Rather, LimeWire users search each other's computers for files that interest them and, if one user finds a file of interest on another user's computer, they can view or download the file.

I draw a different analogy. When a person shares files on LimeWire, it is like leaving one's documents in a box marked "free" on a busy city street. When a person shares files on iTunes over an unsecured wireless network, it is like leaving one's documents in a box marked "take a look" at the end of a cul-de-sac. I conclude that iTunes' lesser reach and limit on file

Page 14 - OPINION AND ORDER

distribution does not render it unlike LimeWire in terms of its user's reasonable expectation of privacy.

C. The Electronic Communications Privacy Act

Alternatively, defendant argues that the Electronic Communication Privacy Act ("ECPA") provides another basis for concluding that JH and Officer McCullough violated his reasonable expectation of privacy. According to defendant, when the two accessed his wireless network and viewed his iTunes, they illegally accessed an electronic communication under the ECPA. Since the access was illegal, says defendant, he could not have reasonable expected it.

The access, however, was not illegal under the ECPA. On the contrary, because the wireless network and iTunes software were configured so that the general public could access them, access was expressly lawful under the ECPA.

The ECPA, part of the Federal Wiretap Act, is intended to protect against the unauthorized interception of electronic communications, and to protect stored electronic communications and transactional records from unauthorized access. 132 CONG. REC. H4039-01 (daily ed. June 23, 1986); S. REP. NO. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557. It is also intended to define the circumstances under which a law enforcement agent must obtain a search warrant before intercepting or accessing a communication. See United States v. Petti, 973 F.2d 1441, 1443-44 (9th Cir. 1992) (analyzing ECPA's warrant requirements); see also S. Rep. No. 99-541, at 38 (detailing warrant requirements for some types of governmental access to electronic communications). In enacting the legislation, Congress sought to "represent[] a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." S. Rep. No. 99-541, at 5. The effect of the ECPA, therefore, is to

provide "statutory protection in accordance with the Fourth Amendment's prohibition on unreasonable searches and seizures." Kern, supra, at 138.

The statute provides, "[i]t shall *not* be unlawful under this chapter or chapter 121 of this title for any person . . . to intercept or access an electronic communication made through an electronic communication system *that is configured so that such electronic communication is readily accessible to the general public.*" 18 U.S.C. § 2511(g)(i) (emphasis added). "The term 'configure' is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection." S. Rep. No. 99-541, at 18.

Here, defendant's wireless network system was configured so that any electronic communications emanating from his computer via his iTunes program were readily accessible to any member of the general public with a Wi-Fi enabled laptop.

I hold that defendant's conduct in operating his iTunes software with the preferences set to share, in conjunction with maintaining an unsecured wireless network router, diminished his reasonable expectation of privacy to the point that society would not recognize it as reasonable.

D. No Subjective Expectation of Privacy

In order to invoke the protection of the Fourth Amendment, defendant would also need to demonstrate a subjective expectation that his activities were private. Young, 573 F.3d at 715-16 (holding that to invoke Fourth Amendment protection defendant must have objective and subjective expectation of privacy).

Although defendant's lack of an objective expectation of privacy is fatal to his motion to suppress, it is worth noting that defendant has also failed to demonstrate he had a subjective expectation of privacy. Defendant does not argue he was without the technological know-how to

Page 16 - OPINION AND ORDER

avoid iTunes sharing. Nor does he argue that he did not know about the unsecured nature of his

wireless network.[3] On the contrary, defendant told police that he works as a representative for a

technology company, Hewlett-Packard, and that "he has an intermediate level of computer

knowledge and that he uses the computer for banking, downloading music and uploading his

timesheets for work." Ex. A at 26. He also told agents that "he has two external hard drives that

were from previous computers that he owned and that he converted them to external hard drives

when he changed computers." Id. at 27. Defendant, therefore, is at least a somewhat

sophisticated computer user. Even if, hypothetically, he did not know about either his iTunes

sharing preferences or the unsecured nature of his wireless network, his level of sophistication

dictates that he should have known. In addition, defendant acknowledged when his home was

searched that his tenant Mr. Harmon also uses the wireless network. For the foregoing reasons,

defendant has not demonstrated that he had a subjective expectation that the contents of his

iTunes library would be private.

D. Conclusion

Having failed to demonstrate either a reasonable objective or subjective expectation of

privacy, defendant cannot invoke the protections of the Fourth Amendment. When JH and

Officer McCullough accessed the child pornography in defendant's iTunes library, no search

occurred. The affidavits for the search warrants, therefore, were not tainted. I need not reach

---

[3]At the suppression hearing, defendant did not testify. He also submitted no declaration
regarding his personal expectations about the functionality of his wireless network and iTunes
software. In the absence of testimony or a sworn statement, I am hard pressed to find evidence
that defendant had a subjective expectation of privacy in the contents of his iTunes library.
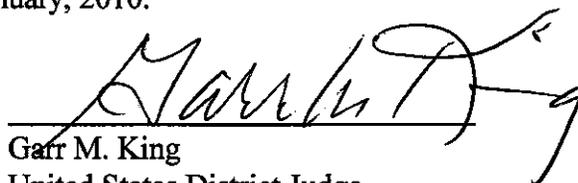
whether probable cause existed to issue the warrants without Officer McCullough's statement about initially viewing the files.

CONCLUSION

Defendant's Motion to Suppress (#23) is denied.

IT IS SO ORDERED.

Dated this _____28ᵗʰ_____ day of January, 2010.

_____

Garr M. King
United States District Judge

Page 18 - OPINION AND ORDER