Filed 10/27/16

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION ONE

THE PEOPLE, Plaintiff and Respondent, v. RICHARD PATRICK EVENSEN, Defendant and Appellant.	A145162 (Napa County Super. Ct. Nos. CR165642, CR168007)

Defendant Richard Patrick Evensen pleaded guilty to various sex crimes after the trial court denied his motion to suppress evidence. The evidence leading to his arrest was obtained when police used software that targets peer-to-peer file-sharing networks to identify Internet Protocol (IP) addresses associated with known digital files of child pornography. A public website revealed one such identified IP address to be registered with Comcast, and the execution of a search warrant on Comcast showed the subscriber of the IP address to be Evensen's mother. A second search warrant was then executed on the mother's home, where Evensen lived, and further inculpatory evidence was found. After Evensen was arrested, more evidence of wrongdoing, some involving different victims, came to light.

Evensen argues that the trial court wrongly denied his motion to suppress because all of the evidence against him emanated from the police's use of the software that targets peer-to-peer networks. According to him, the use of this software violated his Fourth Amendment rights by infringing on his reasonable expectation of privacy in his computer. We reject the argument and affirm.

I.
BACKGROUND

By using a set of software tools known as RoundUp, police learned that an IP address,[1] later determined to be assigned to Evensen's mother, had downloaded child pornography. RoundUp enables law enforcement officials to detect child pornography on peer-to-peer file-sharing networks. Peer-to-peer networks allow users to share digital files over the Internet. To access these networks, users need only download onto their computers a free software program. The program allows a network user to upload a file onto his or her computer, and it then allows other users to access and download the file onto their own devices. A user who buys a music CD, for example, can convert it into a digital file and upload it onto the peer-to-peer network, thereby allowing other users to access and download the file.

When a network user uploads a file, it is placed in a "shared folder" on the user's computer. Other users can find files in shared folders by using a keyword search. When a user finds a desired file, the user can download it from one or multiple hosts. Using multiple hosts accelerates the download. A user could, for example, take the beginning of a video file from a computer in San Francisco, the middle from a computer in Berlin, and the end from a computer in Sydney. The peer-to-peer software reassembles the pieces into a single file.

In this case, Evensen used a peer-to-peer network called eDonkey, which he accessed through a program called eMule. The program creates a shared folder on each user's computer, and downloaded files are automatically placed in it. The shared folder is accessible to all other users unless the downloading user changes the default setting by selecting an option called "Nobody." Another way a downloading user can prevent

[1] "[A]n IP address . . . is a unique number identifying the location of an end[-] user's computer. When an end-user logs onto a[n] internet service provider, the user is assigned a unique IP number that will be used for that entire . . . session. Only one computer can use a particular IP address at any specific date and time." (*United States v. Henderson* (10th Cir. 2010) 595 F.3d 1198, 1199, fn. 1.)

others from accessing a file is to transfer it elsewhere on his or her computer and delete the copy in the shared folder.

Evensen used eMule between September 9, 2011, and December 16, 2012. At the hearing on his motion to suppress, Evensen testified that he took several measures to prevent other users from accessing his files. To begin with, he modified eMule's default settings by selecting the "Nobody" option. But, as Evensen acknowledged, the feature did not always work or he did not always activate it. One time, he saw another user downloading a pornographic file from his computer, and he canceled the download.

Evensen testified that he also transferred files from his shared folder to other places on his computer that were inaccessible to other network users. He admitted, however, that he did not always transfer them immediately. He testified: "At times when I was downloading I would usually move all of them, but sometimes I wouldn't move all of 'em due to the file progress. The files not actually being what they say they would be. They would be either viruses or zip folders . . . . So when I used that I didn't have time or I didn't want to take the time to unzip those folders that I downloaded of those files and so they'd sit in my shared folder."

Finally, Evensen testified that he "max[ed] out" his download speed at 999 downloads, meaning he could download material from 999 sources at once, and reduced to "one" the speed by which another user could download his files. These settings apparently accelerated the speed by which Evensen could download a file, and they restricted other users to downloading only one file at a time from his shared folder. The full extent to which these settings impeded other users' ability to access his files is unclear from the record.

At the suppression hearing, Officer Daniel Ichige[2] also testified, and he explained how RoundUp works. He described how it retrieves information from peer-to-peer

[2] Officer Ichige is a police officer with the San Jose Police Department's Child Exploitation Detail—Internet Crimes Against Children Task Force. He is also a certified instructor in the use of the Gnutella network RoundUp tool. He has had about 90 hours of training with RoundUp tools, 20 hours of which was specific to eMule.

networks, uploads the information onto a server, and makes the information available to law enforcement officials. Officer Ichige explained that RoundUp is specifically used to search for known and verified digital files of child pornography. Each digital photograph has a "hash," a digital fingerprint or serial number, which, according to Officer Ichige, is more distinctive than DNA. Law enforcement officers feed RoundUp a set of hashes of known child pornography files, and RoundUp then searches peer-to-peer networks for them. Officer Ichige explained that RoundUp compiles information from files stored in network users' shared folders but not from files stored elsewhere on users' computers. Apparently, RoundUp runs unattended and constantly searches peer-to-peer networks for files with hashes matching known child pornography. By using the program, law enforcement officers avoid the need to search networks with keywords, identify suspicious files, download those files, and confirm whether they depict child pornography.

The RoundUp website reports IP addresses of computers that have downloaded files with hashes of known child pornography. Law enforcement officers can focus their RoundUp searches on IP addresses that are likely to be associated with computers physically located in the officers' jurisdiction. Officer Ichige explained that RoundUp can show the "history" of an IP address, starting "[f]rom the time that the first child pornography file was made apparent" to the program.

In this case, Officer Darlene Elia of the Napa Police Department used the RoundUp website in February 2013 to look for Napa County IP addresses used to download or share child pornography. She searched all available peer-to-peer networks. The search returned an IP address, eventually determined to be Evensen's mother's, that was first seen using eMule on September 9, 2011, and last seen on December 16, 2012. RoundUp flags files known to be child pornography by coding them in red. Looking at RoundUp's historical list for this particular IP address, Officer Elia saw over 200 red flags.

Using a public website, Officer Elia determined that the IP address was registered to Comcast. Officer Elia then obtained and executed a search warrant for Comcast

records and discovered that on December 16, 2012, the subscriber for the IP address was Evensen's mother. Officer Elia then obtained a second search warrant for the mother's home. Evensen was present when Officer Elia executed the warrant on the morning of April 11, 2013. After searching Evensen's room, Officer Elia arrested Evensen and read him his *Miranda*[3] rights.

Evensen told Officer Elia he had been viewing child pornography for some time and would generally watch it one to two hours per day. He confirmed that all of the computers and hard drives in his room were his, and he estimated that he had about 30 gigabytes of child pornography on his hard drives. He said he obtained child pornography primarily by using peer-to-peer file-sharing software. A forensic examination uncovered over 200 videos and images of child pornography on Evensen's laptop and external hard drives.

Evensen's arrest was made public, and evidence of more sex crimes came to light. After hearing of the arrest, Jane Doe 1 came forward and claimed that Evensen had raped her and performed other sex acts on her while she slept. Jane Doe 2, whom police identified from images on one of Evensen's external hard drives, revealed that she had, at Evensen's request, sent sexually explicit images of herself to him when she was 16 years old. And Jane Doe 3, who was identified by Jane Doe 1 from an image seized from Evensen's home, told police Evensen had performed various sex acts on her while she slept.

In his motion to suppress, Evensen argued that the use of the RoundUp program amounted to an unconstitutional search and that all of the evidence against him should be suppressed because all of it emanated from this search. After a hearing, the trial court denied the motion, and Evensen then pleaded no contest to one count of advertising for sale obscene matter depicting a minor (Pen. Code, § 311.10), three counts of oral copulation of an unconscious person (*id.*, § 288a, subd. (f)), one count of rape of an unconscious person (*id.*, § 261, subd. (a)(4)), two counts of using a minor for sex acts

[3] *Miranda v. Arizona* (1966) 384 U.S. 436.

(*id.*, § 311.4, subd. (c)), and two counts of sodomy of an unconscious person (*id.*, § 286, subd. (f)). He was sentenced to fifteen years, eight months in prison.

II.
DISCUSSION

Evensen maintains that the use of the RoundUp program violated his Fourth Amendment rights "because he had a subjective expectation of privacy in his computer, which was objectively reasonable." (Capitalization omitted.) We are not persuaded.

We begin with the applicable standards of review. In ruling on a motion to suppress, the trial court "(1) finds the historical facts, (2) selects the applicable rule of law, and (3) applies the latter to the former to determine whether the rule of law as applied to the established facts is or is not violated." (*People v. Williams* (1988) 45 Cal.3d 1268, 1301.) "The court's resolution of the first inquiry, which involves questions of fact, is reviewed under the deferential substantial-evidence standard. [Citations.] Its decision on the second, which is a pure question of law, is scrutinized under the standard of independent review. [Citations.] Finally, its ruling on the third, which is a mixed fact-law question that is however predominantly one of law, viz., the reasonableness of the challenged police conduct, is also subject to independent review. [Citations.]" (*Ibid.*)

With these standards in mind, we turn to the governing law. " 'The Fourth Amendment protects an individual's reasonable expectation of privacy against unreasonable intrusion on the part of the government.' " (*People v. Hughston* (2008) 168 Cal.App.4th 1062, 1068.) It "protects people, not places. What a person knowingly exposes to the public, even in his [or her] own home or office, is not a subject of Fourth Amendment protection. [Citations.] But what he [or she] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (*Katz v. United States* (1967) 389 U.S. 347, 351.) "A person seeking to invoke the protection of the Fourth Amendment must demonstrate both that he [or she] harbored a subjective expectation of privacy and that the expectation was objectively reasonable. [Citation.] An objectively reasonable expectation of privacy is 'one society is willing to recognize as reasonable.' [Citation.]" (*People v. Hughston*, at p. 1068.)

Computer users generally have an objectively reasonable expectation of privacy in the contents of their personal computers. (*United States v. Ganoe* (9th Cir. 2008) 538 F.3d 1117, 1127 (*Ganoe*).) But there are exceptions to this general rule, and one of them is that computer users have no reasonable expectation of privacy in the contents of a file that has been downloaded to a publicly accessible folder through file-sharing software.[4] (*Ibid.*) The Ninth Circuit Court of Appeals's decisions in *Ganoe* and *United States v. Borowy* (9th Cir. 2010) 595 F.3d 1045 (*Borowy*) are instructive.

The defendant in *Ganoe* shared child pornography through LimeWire, a publicly available peer-to-peer file-sharing program. (*Ganoe*, *supra*, 538 F.3d at p. 1119.) A law enforcement officer used the same program to download a movie depicting child pornography from the defendant's computer. (*Ibid.*) After downloading additional child pornography files from this computer, the officer obtained a warrant and searched the defendant's home. (*Ibid.*) On appeal, the Ninth Circuit affirmed the district court's denial of the defendant's motion to suppress. (*Id.* at p. 1127.) The Ninth Circuit held that the defendant could not have had a reasonable expectation of privacy once he decided "to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." (*Ibid.*) The court also rejected the defendant's contention that his expectation of privacy was reasonable because he did not know that other users would be able to access files stored on his computer: "To argue

[4] Computer users also have no reasonable expectation of privacy in electronic data that is not itself content. (See, e.g., *In re Zynga Privacy Litig.* (9th Cir. 2014) 750 F.3d 1098, 1108-1109 ["courts have long distinguished between the contents of a communication (in which a person may have a reasonable expectation of privacy) and record information about those communications (in which a person does not have a reasonable expectation of privacy)"]; *United States v. Forrester* (9th Cir. 2008) 512 F.3d 500, 510 [computer users have no reasonable expectation of privacy in "to/from addresses of their messages or [] IP addresses of [] websites they visit"].) Here, without opening or viewing any pornographic file, the police used RoundUp to learn that a public folder on a computer associated with Evensen's mother's IP address had contained known digital images of child pornography. The parties have not addressed, and we therefore do not decide, whether Evensen had a reasonable expectation of privacy in the electronic data RoundUp analyzed in tying his IP address to child pornography.

that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes." (*Ibid.*)

The Ninth Circuit reached a similar decision in *Borowy*, *supra,* 595 F.3d 1045. In that case, an officer used LimeWire to search for a term known to be associated with child pornography. (*Id.* at p. 1046.) From the list of hits, the officer identified known child pornography images using a software program "that verifies the 'hash marks' of files and displays a red flag next to known images of child pornography." (*Ibid.*) At least one of the pornographic files was shared through what was later determined to be the defendant's IP address. (*Ibid.*) Based on the results of this investigation, the officer obtained a search warrant for the defendant's residence and found more than 600 images of child pornography. (*Id.* at p. 1047.)

Citing *Ganoe*, *supra*, 538 F.3d 1117, the Ninth Circuit held that the defendant did not have a reasonable expectation of privacy because he used a peer-to-peer file sharing program. (*Borowy*, *supra*, 595 F.3d at pp. 1047-1048.) The defendant argued that *Ganoe* was distinguishable because, unlike the defendant in *Ganoe*, he at least made efforts to prevent LimeWire from sharing his files. (*Borowy*, at p. 1048.) The Ninth Circuit disagreed. "Despite his efforts, Borowy's files were still entirely exposed to public view; anyone with access to LimeWire could download and view his files without hindrance. Borowy's subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access." (*Ibid.*) The Ninth Circuit also rejected the defendant's contention that the search was unlawful because the police used a " 'forensic software program' " that was unavailable to the public to confirm his files contained child pornography. The court explained that "Borowy had already exposed the entirety of the contents of his files to the public, negating any reasonable expectation of privacy in those files." (*Ibid.*)

Evensen argues that, unlike the defendants in *Ganoe* and *Borowy*, he took several measures to keep the contents of his computer private, including transferring files from his public folder to inaccessible locations, changing the default setting to prevent others

from accessing his shared public folder, and preventing more than one other user from downloading his files from his shared drive at any given time. But substantial evidence was presented from which the trial court could properly find that, notwithstanding these measures, Evensen had no reasonable expectation of privacy. As we have mentioned, Evensen testified that he did not always immediately move files out of his shared folder and that another network user once partially downloaded one of his pornographic files. He cannot claim that his shared folder was private at all times or that he believed it to be. Moreover, RoundUp would not have even detected Evensen's files if they had never been publicly accessible. According to Officer Ichige, RoundUp compiles information from files stored in network users' shared folders and cannot search files stored elsewhere on users' computers.

Evensen argues that it somehow matters that no evidence established that any of his files of child pornography could be downloaded from his shared drive by the time Officer Elia began her investigation in February 2013. He argues that the evidence showed only that child pornography files had at one time been in a shared folder on a computer with an IP address matching that of the computer he was using. But whether Officer Elia could view the child pornography in February is not determinative. RoundUp reported that known digital images of child pornography had been downloaded to Evensen's computer, and Evensen does not point to any evidence suggesting that the report was inaccurate. The information in this report constituted probable cause for the issuance of the ensuing search warrants. (*Illinois v. Gates* (1983) 462 U.S. 213, 238; *People v. Camarella* (1991) 54 Cal.3d 592, 601 [probable cause for a warrant present where "there is a fair probability that contraband or evidence of a crime will be found in [the] place [to be searched]"].)[5]

[5] At oral argument, Evensen's counsel argued that the search was also illegal because the search warrant was not executed until April 2013, four months after Evensen was last seen on the peer-to-peer network. Counsel argued that by the time the warrant was executed the police had no reason to believe any contraband still remained on the premises. We are not persuaded. First, as a matter of procedure, Evensen forfeited this argument by failing to make it below or in his briefing. Second, on the merits, we

Evensen contends that this case is analogous to *Kyllo v. United States* (2001) 533 U.S. 27 because the RoundUp program is enhanced technology. In *Kyllo*, the police used a thermal imager to scan the defendant's home and detect high-intensity lamps typically used for indoor marijuana growth. (*Id.* at pp. 29-30.) Based in part on information gathered from the thermal scan, the police obtained a warrant to search the defendant's home and found an indoor growing operation. (*Id.* at p. 30.) The Supreme Court held that the use of the thermal imager constituted an unlawful search. (*Id.* at p. 40.) The court reasoned that where the government uses sense-enhancing technology that is not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." (*Id.* at pp. 35, 40)

Kyllo v. United States, *supra*, 533 U.S. 27 does not control here. While it is true, as Evensen points out, that RoundUp may be sophisticated and only available to law enforcement officials, the software does not search for otherwise unknowable evidence of illegality. Instead, it monitors only activities on a public peer-to-peer network, a space where, as we have discussed, Evensen had no reasonable expectation of privacy.

Evensen's reliance on *United States v. Ahrndt* (D. Or. Jan. 17, 2013, No. 3:08-CR-00468-KI) 2013 WL 179326 is also misplaced. In that case, the defendant unknowingly, and through a program default, shared content in his LimeWire folder over his home wireless network. (*Id.* at p. *7.) The defendant's neighbor inadvertently accessed the defendant's wireless network and alerted the police after seeing a list of file names on the defendant's computer suggesting the presence of child pornography. (*Id.* at pp. *1-2.) The district court held that there was no Fourth Amendment violation when the police looked at data on the network that the neighbor, a private citizen, had previously searched. (*Id.* at p. *6.) At the same time, the court held that there was a Fourth Amendment violation when the police opened images the neighbor had not viewed. (*Id.*

---

disagree that the passage of four months rendered the information too stale to support the search warrant's execution. (See, e.g., *United States v. Hay* (9th Cir. 2000) 231 F.3d 630, 636.)

at p. *8.) It reached this holding because there was no evidence the defendant "intentionally enabled sharing of his files over his wireless network, and there [was] no evidence he knew or should have known that others could access his files by connecting to his wireless network." (*Id.* at pp. *6-7.) In contrast, here the police did not violate any reasonable expectation of privacy because, unlike the defendant in *Ahrndt*, Evensen intentionally used a publicly accessible peer-to-peer network.

In short, we reject Evensen's Fourth Amendment claim because Evensen had no reasonable expectation of privacy in his shared folder associated with the peer-to-peer network. In light of this conclusion, we need and do not decide whether Evensen would have had a reasonable expectation of privacy if he had been able to successfully prevent other users from accessing his shared folders or if he had downloaded the digital pornographic material by means other than using a peer-to-peer network.

III.
DISPOSITION

The judgment is affirmed.

_____

Humes, P.J.

We concur:

_____

Margulies, J.

_____

Dondero, J.

Trial Court:
Napa County Superior Court – Main

Trial Judge:
Honorable Mark Boessenecker

Counsel for Appellant:
Paul Richard Kleven, First District Appellate Project

Counsel for Respondent:
Kamala D. Harris, Attorney General
Gerald A. Engler, Chief Assistant Attorney General
Jeffrey M. Laurence, Senior Assistant Attorney General
René A. Chacón, Supervising Deputy Attorney General
Bruce Ortega, Deputy Attorney General

People v. Evensen (A145162)