

LimeWire and similar programs connect network participants directly and allow them to download files from one another. To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer.

United States v. Flyer, 633 F.3d 911, 913 (9th Cir. 2011) (citation omitted). This ability to download a file directly from another user's personal computer is known as "peer-to-peer" file sharing.

By default, LimeWire stores downloaded files in a "shared" folder that is searchable by other LimeWire users. The user can change this default setting or manually move files out of the "shared" folder if he does not wish to share files. LimeWire users can also view the internet protocol ("IP") address of the computer from which they are downloading files. The IP address is a unique identifier assigned by an Internet service provider ("ISP") to a subscriber that can be used to determine the physical location of the subscriber if cross-referenced with the ISP's records. In addition, each installation of LimeWire is assigned a global unique identifier number ("GUID") that other LimeWire users can view. If one household has multiple computers that have installed LimeWire, the GUID can be used to determine which computer in the household is sharing a particular file.

B.

Marcus Penwell, a Franklin County Sheriff's Department deputy and a member of the county's multi-jurisdictional Crimes Against Children Task Force, used LimeWire on a daily basis to monitor child pornography possession and distribution. His work computer had a modified version of LimeWire that automatically searched for files bearing names associated with child pornography, but the modified software did not provide him with greater access to the files of

LimeWire users than a standard user would have. On September 12, 2010, Penwell identified a computer connected to LimeWire that was making “hundreds of files with titles indicative of child pornography” available for download. Penwell connected to the computer, downloaded some of the files, and found that they contained child pornography. He recorded the IP address and GUID of the computer in question and sent a subpoena to Insight Communications (“Insight”), the ISP that issued the IP address, to determine the location of the computer sharing the files. Insight provided Penwell with the address of Bobby Lawwell. Penwell successfully accessed files from this computer a second time on October 24, 2010, and obtained a warrant to search Lawwell’s home based on the files and the information provided by Insight on November 4.

When Penwell and a team of sheriff’s deputies arrived at the residence to execute the warrant on November 5, Lawwell met them at the front door of the house. She explained that she lived in the house with her children, and that Conner, her uncle, lived in an apartment in the garage at the rear of the residence. The deputies found Conner in the garage apartment, and he permitted them to walk through it to perform a protective sweep. They observed a desktop computer and monitor in the apartment. While other deputies stayed at the residence, Penwell obtained a second warrant to search the apartment due to concern that the separate residence would not be covered by the initial warrant. Penwell returned to the house later that day to execute the new search warrant.

Deputies retrieved Conner’s computer and numerous compact disks from the apartment. A forensic search of these items revealed numerous child pornography images. The forensic examination also indicated that the day before the deputies executed the search warrant, Conner reinstalled the operating system on his computer. This process confined the child pornography files

to “unallocated” space on the computer’s hard drive that is inaccessible to most users, although this space can be accessed with advanced computer forensic tools used by criminal investigators. The examination also confirmed that Conner had been using LimeWire to obtain and share child pornography. The file paths of many of the images found on the computer indicated that Conner downloaded them from LimeWire and that they were stored in folders searchable by other LimeWire users. In addition, the GUID of the version of LimeWire installed on the computer matched the GUID of the computer from which Penwell downloaded child pornography.

Lawwell also told the deputies that Conner’s daughter and ex-girlfriend had accused him of sexual molestation. Penwell arranged to meet with the two women on November 11, 2010. The daughter told Penwell that Conner had repeatedly raped her between the ages of five and nine years old and had made a pornographic video of her using a VHS video camera when she was six years old. Penwell again contacted Lawwell, and Lawwell confirmed that Conner had VHS recording equipment and tapes in his apartment. Penwell obtained another search warrant, and sheriff’s deputies seized a cache of VHS tapes in Conner’s apartment. Among the tapes seized was a pornographic video of Conner’s daughter that matched the description she gave to Penwell.

C.

The government charged Conner with four counts of receipt of visual depictions of child pornography, 18 U.S.C. § 2252(a)(2), (b)(1), and one count of possession of child pornography, 18 U.S.C. § 2252(a)(4)(B). The visual-depictions counts related to images Conner downloaded from LimeWire, while the possession count addressed the video Conner made of his daughter. Conner made numerous pre-trial motions, but the only motion relevant to this appeal is his motion to

suppress evidence. He argued that Penwell’s use of LimeWire constituted an unlawful, warrantless “search” under the Fourth Amendment and that the court should suppress all evidence seized as a result of that search. After an evidentiary hearing in which Penwell and Dan Johnson, a computer forensic examiner working for the sheriff’s department, gave testimony, the district court denied Conner’s motion. Conner waived his right to counsel after the court denied the suppression motion and represented himself at trial. A jury found Conner guilty of all five counts in the superseding indictment.

Prior to his sentencing hearing, Conner reasserted his right to counsel. The pre-sentence report prepared for Conner calculated an offense level of 42, including a two-point enhancement for an offense that “involved . . . [d]istribution” under Sentencing Guideline § 2G2.2(b)(3)(F). Conner objected to this enhancement. He also argued that he should receive a two-level reduction in his base offense level under section 2G2.2(b)(1) of the Guidelines. The district court overruled the objections during Conner’s sentencing hearing and sentenced Conner to a within-Guidelines sentence of 360 months in prison—240 months for the visual-depictions counts and 120 months for the possession count, to be served consecutively.

II.

When a defendant appeals the denial of a suppression motion, this court reviews the district court’s factual findings for clear error and its legal determinations *de novo*. *United States v. Martin*, 526 F.3d 926, 936 (6th Cir. 2008). “A factual finding will only be clearly erroneous when, although there may be evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed.” *United States v. Navarro-*

United States v. Conner
No. 12-3210

Camacho, 186 F.3d 701, 705 (6th Cir. 1999). Because the government prevailed in the district court, this court must “consider the evidence in the light most favorable to the government.” *United States v. Campbell*, 549 F.3d 364, 370 (6th Cir. 2008).

Conner asks us to find that he had a “legitimate expectation of privacy” in the images he made available for sharing on LimeWire. In order to do so, we must answer two questions in the affirmative:

First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that “he [sought] to preserve [something] as private.” . . . Second, we inquire whether the individual’s expectation of privacy is “one that society is prepared to recognize as reasonable.”

Bond v. United States, 529 U.S. 334, 338 (2000) (alterations in original) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Conner’s argument fails because his expectation of privacy is not “one that society is prepared to recognize as reasonable.”

Generally speaking, computer users have a reasonable expectation of privacy in data stored on a home computer. *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). Conner argues that under *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (*en banc*), third-party access to information on one’s computer is consistent with a reasonable expectation of privacy in that information. In *Warshak*, we agreed that the government could not compel a commercial ISP to turn over the contents of a subscriber’s e-mails without a warrant because subscribers “enjoy[] a reasonable expectation of privacy in the contents of emails,” even though an ISP has the ability to view the contents of e-mail prior to delivery. 631 F.3d at 288. In the context of e-mail, ISPs are “the functional equivalent of a post office or a telephone company,” and like an ISP, both of these entities have the ability to intrude on the contents of messages in the course of delivering them to their

intended recipients. *Id.* at 286. Since the right or ability of third parties to intrude on phone calls and letters has not been deemed sufficient to defeat a reasonable expectation of privacy in those modes of communication, we agreed that “it would defy common sense to afford emails lesser Fourth Amendment protection” than telephone calls or letters. *Id.* at 285–86.

Warshak does not control this case because peer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls. Unlike these forms of communication, in which third parties have incidental access to the content of messages, computer programs like LimeWire are expressly designed to make files on a computer available for download by the public, including law enforcement. Peer-to-peer software users are not mere intermediaries, but the intended recipients of these files. Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”); *see also California v. Greenwood*, 486 U.S. 35, 40–41 (1988) (finding no reasonable expectation of privacy in “plastic garbage bags left on or at the side of a public street,” which are accessible by “members of the public” and left on the curb “for the express purpose of conveying [them] to a third party, the trash collector”).

Conner responds that he did not know the files he downloaded from LimeWire would be publicly accessible. To prove this point, he emphasizes efforts he made to keep these files private by moving them to compact disks and reinstalling his operating system on the computer to “wipe[] the hard drive clean.” But these efforts only prove that he was ineffective at keeping the files he downloaded from LimeWire from being detected. They do not establish that he was unaware of a

risk of being discovered. As the Ninth Circuit observed when confronted with a similar argument, Conner’s “subjective intention not to share his files d[oes] not create an objectively reasonable expectation of privacy in the face of [the] widespread public access” to his files LimeWire created. *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (rejecting Fourth Amendment privacy claim of defendant who unsuccessfully attempted to use LimeWire’s privacy features “to prevent others from downloading or viewing the names of files on his computer”).

Furthermore, Conner’s assertions of ignorance are not supported by the record. Penwell downloaded images from Conner’s computer twice over a month-long period, meaning that the images were available on Conner’s computer for a significant period of time. Conner’s sister, Sandra Conner-Lewingdon, testified at trial that Lawwell had shown her and Conner how to use LimeWire to search for music files being shared by other users. The forensic examination of Conner’s computer confirmed that he was using LimeWire to download child pornography images from other users and storing those images in files used for sharing over LimeWire. The sheer number of files that were available for download—“hundreds,” according to Penwell—belies Conner’s purported ignorance in how the software worked. Finally, Conner concedes that while he made an effort to take some files off of his computer, he took no affirmative steps to limit the ability of other LimeWire users to access the files in his folder, despite a reasonably high level of competency with computers. “To argue that [Conner] 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,” and the district court did not err by rejecting Conner’s assertions of ignorance. *United States v. Ganoie*, 538 F.3d 1117, 1127 (9th Cir. 2008).

Sister circuits that have taken up this question uniformly hold that there is no reasonable expectation of privacy in files the government obtained using peer-to-peer sharing services like LimeWire. *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (“One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking.”); *Ganoe*, 538 F.3d at 1127; *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008). In line with these opinions, we agree that the district court properly declined to suppress the files Penwell downloaded from Conner’s computer and the fruits of the investigation that emanated from those files.

III.

A district court’s sentencing decision is reviewed for both procedural and substantive reasonableness. *United States v. Bolton*, 669 F.3d 780, 781 (6th Cir. 2012). Conner challenges the calculation of his offense level under the Sentencing Guidelines, which implicates procedural reasonableness. This court reviews the district court’s factual findings on sentencing issues for clear error and its legal interpretation of the Sentencing Guidelines *de novo*. *United States v. Brown*, 579 F.3d 672, 677 (6th Cir. 2009). When courts interpret the Guidelines, they may apply “the traditional canons of statutory interpretation.” *United States v. Jackson*, 635 F.3d 205, 209 (6th Cir. 2011).

The Sentencing Guidelines for child pornography offenses mandate a two-level increase in the offense level if the offense conduct “involved . . . [d]istribution.” U.S. Sentencing Guidelines Manual § 2G2.2(b)(3)(F). They also allow for a two-level reduction to the base offense level if section 262.2(a)(2) applies and if “the defendant’s conduct was limited to the receipt or solicitation of material involving the sexual exploitation of a minor” and “the defendant did not intend to traffic

in, or distribute, such material.” *Id.* § 2G2.2(b)(1). Conner raises two issues relating to these provisions on appeal. First, he argues that the “distribution” enhancement does not apply to him. Second, he asserts that because he “did not intend to traffic in, or distribute,” child pornography, the district court should have awarded him a two-level reduction. Both claims lack merit.

A.

A defendant’s offense conduct “involve[s] . . . distribution” under section 2G2.2(b)(3)(F) when it involves

any act, including possession with intent to distribute, production, transmission, advertisement, and transportation, related to the transfer of material involving the sexual exploitation of a minor. Accordingly, distribution includes posting material involving the sexual exploitation of a minor on a website for public viewing but does not include the mere solicitation of such material by a defendant.

Id. § 2G2.2 cmt. 1. Conner argues that the government had to prove he either intended to distribute child pornography or knew he would be sharing images with others by using LimeWire. The government argues that it only needs to prove Conner knowingly used LimeWire because the capability of the software to share files with others is self-evident.

The definition of “distribution” provided by the Guidelines is silent as to the requisite state of mind with which the “act . . . related to the transfer of material” must be conducted. In the context of a criminal statute, this silence would permit the court to imply that the defendant must commit such an act knowingly. *See United States v. X-Citement Video, Inc.*, 513 U.S. 64, 71–72 (1994) (noting that courts may “presume a scienter requirement in the absence of express contrary intent” when interpreting statutes “akin to the common-law offenses against the ‘state, the person, property, or public morals’” (quoting *Morrisette v. United States*, 342 U.S. 246, 255 (1952))). While a

presumption of “knowing” conduct is not always warranted when interpreting the Guidelines, it is appropriate here. “Distribution” of contraband is “akin to common-law offenses,” and as such, a defendant should have to knowingly perform an “act . . . related to the transfer of material” to trigger this enhancement. The example at the end of the Guideline’s definition of “distribution” confirms this reasoning, since a defendant who “post[s] material . . . on a website for public viewing” performs a knowing act. We agree with the government’s position that a knowing “act . . . related to the transfer of material” is sufficient to satisfy section 2G2.2(b)(3)(F).

Conner argues that the Guidelines require proof of an “intent to distribute,” but the language of section 2G2.2(b)(3) does not support his position. The offense conduct only needs to “*involve[]* . . . distribution” for the enhancement to apply, and “distribution” is any act “*related* to the transfer of material.” This reading is confirmed by the subparagraphs immediately preceding section 2G2.2(b)(3)(F), which permit greater increases in a defendant’s offense level if the government can prove a specific motivation behind distribution, including distribution “for pecuniary gain,” distribution “for the receipt . . . of a thing of value,” and distribution “to a minor that was intended to persuade . . . the minor to engage in prohibited sexual conduct.” U.S. Sentencing Guidelines Manual § 2G2.2(b)(3)(A), (B), (E). The absence of a similar intent requirement for all crimes that merely “*involve[]* . . . distribution” leads to the conclusion that it is inappropriate to read an “intent to distribute” requirement into section 2G2.2(b)(3)(F). *See Nolfi v. Ohio Ky. Oil Corp.*, 675 F.3d 538, 553 (6th Cir. 2012) (observing that when a statute includes a requirement in one section, and excludes it in a neighboring section, the canon of *expressio unius est exclusio alterius* permits the inference that the neighboring section does not impose the requirement).

We agree with the government that knowing use of LimeWire, much like the posting of a file on a website, is sufficient to trigger section 2G2.2(b)(3)(F)’s two-level enhancement. *Bolton*, 669 F.3d at 781–83 (applying this standard without expressly adopting it); *United States v. Dodd*, 598 F.3d 449, 451–53 (8th Cir. 2010); *United States v. Layton*, 564 F.3d 330, 335 (4th Cir. 2009); *United States v. Carani*, 492 F.3d 867, 876 (7th Cir. 2007); *United States v. Todd*, 100 F. App’x 248, 250 (5th Cir. 2004), *vacated on other grounds*, 543 U.S. 1108 (2005). While defendants in some of these cases have argued that they had “no knowledge that [their] computer[s] [were] equipped to distribute” child pornography, courts have not required the government to prove such knowledge.

Dodd, 598 F.3d at 452. “[T]he purpose of a file sharing program is to share, in other words, to distribute,” and knowing use of such a program qualifies as conduct that “involve[s] . . . distribution.” *Id.*

Unique among courts that have addressed this issue, the Eighth Circuit has held that the presumption that users of peer-to-peer software understand they are sharing files with others can be rebutted by the defendant. The *Dodd* court recognized that “[a]bsent concrete *evidence* of ignorance—evidence that is needed because ignorance is entirely counterintuitive—a fact-finder may reasonably infer that the defendant knowingly employed a file sharing program for its intended purpose.” *Id.* In *United States v. Durham*, 618 F.3d 921 (8th Cir. 2010), the Eighth Circuit relied on this language to reverse a district court’s imposition of the “distribution” enhancement on a defendant that used peer-to-peer software. The defendant in *Durham* showed that another person had installed file-sharing software on the defendant’s computer. 618 F.3d at 932. Moreover, he demonstrated that he did not know how to use the program and “was not knowledgeable regarding

the program’s capabilities.” *Id.* The court found that these extenuating circumstances comprised “concrete evidence of ignorance” under *Dodd*. *Id.* at 928–32; *but see id.* at 937–43 (Gruender, J., concurring in part, dissenting in part, and announcing the judgment of the court in part) (criticizing the majority’s application of *Dodd*). No other circuit has taken up the issue of whether the section 2G2.2(b)(3)(F) enhancement is automatically imposed when a defendant knowingly uses peer-to-peer software, or if the defendant can rebut the presumption that he understood how the software worked by presenting “concrete evidence of ignorance.” In *Bolton*, this court distinguished *Durham* from cases out of the Fourth and Seventh Circuits, but did not recognize the defense outlined in *Durham* because the defendant did not present evidence of ignorance that would allow him to invoke it. *Bolton*, 669 F.3d at 782–83.

Conner argues that we should follow *Durham* and reverse the district court’s imposition of the section 2G2.2(b)(3)(F) enhancement. But like the defendant in *Bolton*, Conner cannot point to “concrete evidence of ignorance” in the record that would raise the issue the *Durham* court confronted. He argues that “the government did not develop the record in any way sufficient to demonstrate any knowledge on Conner’s part that files he downloaded to his hard drive would be accessible to others,” even though *Durham* places the burden of introducing evidence on the defendant. *Durham*, 628 F.3d at 931 (“[U]nless a defendant presents ‘concrete evidence of ignorance,’ the fact-finder may reasonably infer the defendant utilized a file-sharing program to distribute files.” (emphasis added)). It is not relevant that the government may have had better evidence in *Bolton* of the defendant’s understanding of the operation of peer-to-peer software than it does in this case. *See Bolton*, 669 F.3d at 781 (noting that defendant had removed file-sharing

software from his girlfriend's computer and read "multiple . . . advisories" about the operation of such software prior to installing it on his computer) (internal quotation marks omitted). Finally, the only evidence on this topic that is in the record points in the government's favor. Conner's sister testified that Lawell had shown her and Conner how to use LimeWire. Conner made "hundreds" of files available for download, and the forensic computer examiner found numerous child pornography files on Conner's computer with file paths indicating the images were downloaded from and being shared on LimeWire.

Since the record only bolsters the sound presumption that users of file-sharing software understand others can access their files, the district court properly imposed the section 2G2.2(b)(3)(F) enhancement in this case. As in *Bolton*, we do not reach the issue of whether the Eighth Circuit's *Dodd / Durham* rule applies in this circuit.

B.

Conner also argues that the court should have reduced his offense level by two levels under section 2G2.2(b)(1) of the Guidelines. See *Durham*, 618 F.3d at 932 (ordering the district court to consider this reduction after concluding the section 2G2.2(b)(3)(F) enhancement was inappropriate). This reduction is inappropriate because Conner's offense conduct also involved sexual exploitation of minors and was therefore not "limited to the receipt or solicitation" of child pornography. Accordingly, the district court properly denied Conner's request for a reduction in the offense level.

IV.

For these reasons, we affirm the judgment of the district court.