NOT FOR PUBLICATION

FILED

SEP 28 2022

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

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. RAYMOND J. LIDDY, Defendant-Appellant.	No. 20-50238 D.C. No. 3:19-cr-01685-CAB-1 MEMORANDUM[*]

Appeal from the United States District Court
for the Southern District of California
Cathy Ann Bencivengo, District Judge, Presiding

Argued and Submitted November 9, 2021
Pasadena, California

Before: COLLINS and LEE, Circuit Judges, and BAKER,[**] Judge.

Memorandum joined by Judge COLLINS and Judge LEE;
Partial Concurrence by Judge BAKER

Raymond J. Liddy appeals his conviction, following a bench trial, on a single count of knowingly possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

1. To secure Liddy's conviction under 18 U.S.C. § 2252(a)(4)(B), the

[*] This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

[**] The Honorable M. Miller Baker, Judge of the United States Court of International Trade, sitting by designation.

Government was required to prove that (a) Liddy possessed one or more "matters"—here, disks or drives—containing child pornography; and (b) Liddy knew those matters contained such "unlawful visual depiction[s]." *United States v. Lacy*, 119 F.3d 742, 747–48 (9th Cir. 1997) (citing 18 U.S.C. § 2252(a)(4)(B)). Liddy does not contest the first element; indeed, he signed a formal stipulation, for purposes of trial, that 10 specific files found on certain devices seized from his home by the FBI contained child pornography. Liddy contends, however, that the evidence was insufficient to prove the second element—*viz*., that he knew that those devices contained child pornography. Where, as here, we review "a district court's judgment in a bench trial," we review evidentiary sufficiency under the familiar standard established in *Jackson v. Virginia*, 443 U.S. 307 (1979), which requires us to determine whether, "'viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *United States v. Temkin*, 797 F.3d 682, 688 (9th Cir. 2015) (quoting *Jackson*, 443 U.S. at 319). Applying this standard, we conclude that the evidence of Liddy's knowledge was sufficient.

The 10 files at issue were found on three different devices: an external hard drive containing two images; a 16GB thumb drive containing three images; and a 1GB thumb drive containing five images. Nine of the 10 images, at the time of the

FBI's search, had been deleted and were located in "unallocated space" on the devices.[1] The tenth file was found on the external hard drive, saved in allocated space in a folder labeled, in relevant part, <USMC/Bios/Newfolder/JTFPanama>. (Liddy had served in the Marine Corps.) Although that file was a "JPEG" image, it was mislabeled with a "PDF" file extension. Due to the incorrect file extension, that file could not be opened simply by double-clicking on it, but the file could still be opened by other means.

In articulating the basis for its finding of guilt, the district court "particularly focus[ed]" on the five images on the 1GB thumb drive, because there was "undisputed evidence as to the dates they were created on the thumb drives." Specifically, those images had been saved to that thumb drive on separate occasions over a period of time—namely, on May 24, June 14, and June 17, 2017. The court concluded that this evidence supported an inference that Liddy had "moved" or "transferred over" files from his "desktop or some other source to these thumb drives" before later deleting them. Accordingly, considering Liddy's "statements" to law enforcement agents and the "circumstantial evidence" in the record, the court found "beyond a reasonable doubt that [Liddy] knew what he was

[1] "Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software." *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011).

saving, that he saved them to the drives, and he subsequently deleted them."

Liddy acknowledges that the posited sorting or moving of files could support an inference of knowledge, but he argues that (a) there was no evidence to support the district court's transfer theory, and (b) the trial evidence could not exclude the alternative theory that Liddy had downloaded what he thought was adult pornography *directly* onto the external devices, where he then "deleted them either without opening them or as soon as he recognized they were contraband." Considering several items of evidence together, we conclude that the district court could rationally find Liddy knowingly accessed, transferred, and stored the files on the drives.

First, the Government's expert noted that several of the files had date stamps showing that the files had been "modified" on dates that were earlier than their "created" dates, and he explained that this discrepancy supports an inference that "the image was modified on a different device before it was placed on th[e] particular device" on which it was found. Liddy's own expert similarly acknowledged that such a disparity in modified/created dates is a "common artifact when something is transferred from one local file system to another local file system" and is "an example of a transfer that can take place from a computer to a hard drive or a thumb drive." As noted, Liddy argues that the Government's evidence failed to exclude the reasonable alternative inference that the same

discrepancy could have occurred without Liddy having reviewed the files before they were saved onto his devices, *e.g.*, if Liddy had downloaded compiled ZIP files directly from the internet to the external drives. Liddy further contends that the Government's failure of proof in this regard is underscored by the lack of metadata showing that the files had ever been on Liddy's desktop computer or been viewed there. While these arguments have some force, we cannot say that, in light of the record as a whole, the district court could not reasonably draw the inference it did and find Liddy's knowledge to be established beyond a reasonable doubt.

Second, as the district court noted, Liddy made several statements to law enforcement that can reasonably be viewed as inculpatory. When agents asked Liddy whether he had ever sent images of "girls under the age of 18," Liddy initially replied, "[Y]eah, I've resent them," before changing his answer to, "I—I don't believe—I don't think I have." He subsequently volunteered that, "[y]ou know, um, if I looked at anything, it was strictly just curiosity and screwing around." When asked later whether he had saved any "child pornography-type stuff" to his computer, Liddy responded that "[u]m, if I had, it's gone." Liddy also stated, when asked whether a forensic search of his computer would uncover "a ton" of deleted child images, that "[y]ou probably would find some, but not a ton."

Third, an undeleted image on the external hard drive was saved under a file path and name—"USMC/Bios/New folder/JTF Panama.pdf"—that could

reasonably be construed as referencing Liddy's time in the United States Marine Corps. The saving of a child pornography image with such a distinctive file name supports an inference that the possession of the image was not unintentional or unknowing. Indeed the "Panama" file—the only file that was found in "allocated space"—had been saved to the external drive less than nine hours before agents arrived at Liddy's home. Liddy argues that, because the Panama file had an incorrect file extension—".pdf" rather than ".jpg"—that file must be deemed "inaccessible" to Liddy and should be disregarded. But given the evidence of Liddy's computer use, including the presence of child pornography on multiple external devices, the district court was not required to conclude that Liddy was a digital naïf who could not access the Panama file or that he was unaware of its contents. Liddy also argues that we must disregard the Panama file because the district court did not reference it when announcing the court's verdict. But even assuming *arguendo* that the district court's findings did not include the Panama file in describing the *actus reus* and instead relied only on the other files (or a subset of those files), the Panama file remained circumstantial evidence that the district court could evaluate in determining what inferences to draw with respect to those other files, and such evidence is properly considered on appeal in assessing the sufficiency of the evidence in the trial record.

Considering the record evidence as a whole, we conclude that the district

court could rationally find, beyond a reasonable doubt, that Liddy knew the contents of the files in question. *See United States v. Richter*, 782 F.3d 498, 501 (9th Cir. 2015) (citing *United States v. Nevils*, 598 F.3d 1158, 1164 (9th Cir. 2010)). In contrast to *United States v. Flyer*, 633 F.3d 911 (9th Cir. 2011), there was sufficient evidence in the trial record in this case to show that the files in unallocated space were knowingly possessed by Liddy, before their deletion, during the time frame charged in the indictment.

2. Reviewing de novo, *see United States v. I.M.M.*, 747 F.3d 754, 766 (9th Cir. 2014) (citing *United States v. Bassignani*, 575 F.3d 879, 883 (9th Cir. 2009)), we hold that the district court correctly concluded Liddy was not in custody when he was interviewed at home by law enforcement and that the failure to give *Miranda* warnings therefore did not require suppression of his statements to the agents. Liddy relies on *United States v. Craighead*, 539 F.3d 1073 (9th Cir. 2008), but the circumstances of this case are very different. Unlike in *Craighead*, Liddy did not live on a military base; the questioning at issue occurred before Liddy knew that the officers had a warrant to search his home; he chose the room (the kitchen) in which the interview took place; there was no display of "unholstered" firearms; and his exit from the room was not physically blocked. *Id*. at 1078–79, 1085–89. Considering the totality of the circumstances, we conclude that a reasonable person would have felt free to terminate the interview and that Liddy

was therefore not in custody. *Howes v. Fields*, 565 U.S. 499, 508–09 (2012).

3. The district court did not err in denying Liddy's motion for a new trial, which challenged the validity of his waiver of jury trial. Liddy, himself a lawyer, executed a written waiver of his right to a jury trial and orally affirmed his waiver in open court. He nonetheless contends that his waiver was unintelligent because, had he known ahead of time that the testimony of a Government witness would ultimately be proved incorrect and retracted, he would have used the opportunity to impeach the unreliable witness before a jury. Reviewing the adequacy of his waiver de novo, *see United States v. Tamman*, 782 F.3d 543, 551 (9th Cir. 2015) (citing *United States v. Shorty*, 741 F.3d 961, 965 (9th Cir. 2013)), we reject this contention. "[W]ritten waivers are presumptively knowing and intelligent," *id*., and the record amply confirms that Liddy knew and understood the rights that he was giving up when he "request[ed] that the court alone decide if he is guilty or not guilty." The fact that Liddy could not have foreseen that a Government witness would later have his credibility damaged at trial does not vitiate the voluntary and intelligent nature of his jury waiver.

4. Liddy argues that, under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the district court should have suppressed the subscriber information that the Government obtained by subpoena, rather than with a warrant, from Liddy's internet service provider. This argument is foreclosed by *United States v.*

Rosenow, 33 F.4th 529 (9th Cir. 2022), in which we held that "a defendant 'ha[s] no expectation of privacy in . . . IP addresses' or basic subscriber information because internet users 'should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.'" *Id*. at 547 (alterations in original) (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)).

AFFIRMED.

BAKER, International Trade Judge, concurring:

I part company with my colleagues on two issues. I don't think we should rely on the "JTP Panama" file, not only because the district court didn't rely on it, but because the record is inconclusive as to whether Liddy would have known how to access it. In the absence of any evidence on this point—regarding the *relative* accessibility of this file to an ordinary computer user, if there is such a thing—I don't think we should speculate that it was accessible to Liddy. Given the government's burden of proof, ties go to Liddy.

I also can't rely on the district court's file transfer theory based on the "created date" and the "modified date." In my view, Liddy's counsel thoroughly debunked that theory at argument. There is no digital evidence on the PC to support the notion that Liddy transferred these images from his PC to the external drives. Counsel also pointed to expert testimony that files downloaded from an online zip file would contain the exact same sort of artifact—the "last modified date" would be the date the file was added to the zip file, and the "created date" would be when it was saved to the external drive.

Considering Liddy's incriminating statements outlined in the memorandum disposition, in my view the district court could rationally find Liddy knowingly stored and accessed the five files on the 1GB thumb drive before deleting them. In contrast to *United States v. Flyer*, his incriminating statements can be viewed as

"admission[s] that he had viewed [these] charged images on or near the time alleged in the indictment." 633 F.3d 911, 919 (9th Cir. 2011).

Except as to the issues discussed above, I join the memorandum disposition.