

FOR PUBLICATION

In the  
United States Court of Appeals  
For the Eleventh Circuit

---

No. 25-10073

---

UNITED STATES OF AMERICA,

*Plaintiff-Appellee,*

*versus*

KENNETH MICHAEL MININGER,

*Defendant-Appellant.*

---

Appeal from the United States District Court  
for the Northern District of Alabama  
D.C. Docket No. 3:22-cr-00249-LCB-HNJ-1

---

Before BRASHER, KIDD, and WILSON, Circuit Judges.

BRASHER, Circuit Judge:

This appeal is about the reasonable expectation of privacy—or the lack thereof. Kenneth Mininger secretly placed video cameras in shared rooms in his ex-wife’s house. He used these cameras

to record his ex-wife's minor daughter undressing. The police examined the SD cards attached to these cameras without a warrant and, based on the cards' contents, obtained a warrant for Mininger's other devices. On those devices, law enforcement found large amounts of child sexual abuse material for which Mininger was convicted. He brings a Fourth Amendment challenge, arguing that the district court should have suppressed all of this evidence and that the resulting warrant was overbroad. But, in large part because he had no reasonable expectation of privacy in the SD cards he had placed, unsecured, in a shared room in his ex-wife's house, Mininger's Fourth Amendment arguments fail. Accordingly, we affirm his convictions.

### I.

Over Thanksgiving 2021, Mininger visited his ex-wife S.H. and two of her minor children from a prior relationship. During this visit, Mininger stayed (alone) in one of the children's bedrooms and had unfettered access to the house.

Over the course of Mininger's visit, S.H.'s seventeen-year-old daughter found a camera surreptitiously placed in her bedroom and directed at her bed. She further found a camera in the bathroom that was shared by the children and Mininger. The daughter determined that each of the devices contained an SD storage card and, because neither was password protected, she reviewed the stored footage. The footage included recordings of the daughter and a friend watching a movie in her room. She promptly informed her mother and showed her the cameras.

25-10073

Opinion of the Court

3

At this point, S.H. confronted Mininger, who denied placing the cameras. She repeatedly told Mininger to get out of her house. Mininger did so, taking one of the cameras with him; but S.H. and her daughter had removed the SD cards from both cameras.

S.H. called the police and, when a sheriff's deputy arrived, consented in writing to a police search of the SD cards. The police reviewed the contents of the cards, which included footage from May 2018, late 2019, and early 2020. Included in these videos was footage of S.H.'s seventeen-year-old daughter undressing when she was between fourteen and sixteen years old.

Based on this information, law enforcement obtained search warrants for Mininger's residence, any vehicles in which he was the occupant, his devices, and person. The warrant for the house authorized the seizure and examination of devices that may contain evidence of "Child Pornography and Sexual Exploitation." Dkt. 62 at 49.

Upon executing this warrant, the police located four devices containing child pornography. Mininger had used a program called VeraCrypt to encrypt and conceal his files. This program caused the child pornography contained on his drives to "present as random data." Dkt. 54 at 130. Nevertheless, a forensic examiner was able to identify suspicious encrypted files. He then ran a brute-force attack on the files, which were protected by two layers of passwords. After some effort, he was successful in accessing the files' contents, which included recordings documenting Mininger's sexual abuse of an eight-year-old.

The United States charged Mininger with 16 counts related to the production and possession of child pornography. Mininger moved to suppress the evidence obtained from the search of the SD cards, arguing that the search required a warrant. He further sought to suppress evidence obtained from the subsequent searches of his electronic devices because the search warrants were tainted by the unlawful search of the SD cards. Separately, he argued that the warrants were overbroad.

The district court denied Mininger's motion, and Mininger entered a guilty plea to two of the charged counts. The district court reasoned that, although Mininger had a reasonable expectation of privacy in the SD cards, S.H. had authority to consent to the search. Mininger's guilty plea was conditional, as he reserved his right to appeal the denial of his motion to suppress. The court then sentenced Mininger to 600 months' imprisonment, and Mininger timely appealed.

## II.

We apply a "mixed standard of review" to the denial of a motion to suppress evidence, "assessing the district court's factual findings for clear error and its application of the law to facts *de novo*." *United States v. Ewing*, 140 F.4th 1339, 1346 (11th Cir. 2025).

## III.

This appeal raises two questions. First, does a homeowner's overnight guest have a reasonable expectation of privacy in the contents of a recording device when the guest places that device in

25-10073

Opinion of the Court

5

a shared space without the homeowner's knowledge or consent, fails to secure the contents, and uses it to invade the homeowner's privacy? Second, must a warrant to search physical electronic devices be limited in time or category as to the electronic files that may be reviewed? We answer both questions "no." We discuss them in turn below.

A.

Mininger first argues that the police conducted a warrantless search of his SD cards in violation of his Fourth Amendment rights. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. A search occurs in two ways: when the government obtains information by "trespassory activity . . . intruding on a constitutionally protected area," *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012), and "when an expectation of privacy that society is prepared to consider reasonable is infringed," *United States v. Karo*, 468 U.S. 705, 712 (1984) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)).

Although Mininger does not argue that a physical trespass occurred, he asserts that the police invaded his reasonable expectation of privacy in the SD cards that he placed in S.H.'s home. The district court denied Mininger's motion to suppress, but it agreed that Mininger had a reasonable expectation of privacy in the contents of the SD cards. The government argues that the district court's expectation-of-privacy conclusion was in error. Because we

can “affirm the denial of a motion to suppress on any ground supported by the record,” *United States v. Cohen*, 38 F.4th 1364, 1386 (11th Cir. 2022), we consider this question anew.

Mininger bears the burden to demonstrate that a search, as defined under the Fourth Amendment, occurred. *United States v. King*, 509 F.3d 1338, 1341 (11th Cir. 2007). As relevant here, he must do so by establishing (1) that he had a subjective expectation of privacy and (2) “that the privacy expectation [is] one that society is prepared to recognize as reasonable.” *Id.* (citation modified). Whether a defendant has a reasonable expectation of privacy “is determined by an examination of the totality of the circumstances.” *United States v. Sarda-Villa*, 760 F.2d 1232, 1235 (11th Cir. 1985).

Considering the totality of the circumstances, we conclude that Mininger had no expectation of privacy in the SD cards that society would be prepared to recognize as reasonable. Put another way, whatever his subjective expectation of privacy, there was no objectively reasonable expectation that the contents of the SD cards would remain private. After all, he placed the video cameras and their attendant SD cards in a shared area of S.H.’s home where they could easily be discovered, he failed to protect the contents with a password, and he used those cards to invade the privacy of S.H.’s family members. In such circumstances, Mininger’s expectation of privacy in the contents of the SD cards is “not only unreasonable, but foolhardy.” *United States v. Miravalles*, 280 F.3d 1328, 1333 (11th Cir. 2002).

25-10073

Opinion of the Court

7

For starters, a person ordinarily lacks a reasonable expectation of privacy in computer files that he makes readily accessible to third parties. *King*, 509 F.3d at 1341–42. In such an event, the files are “akin to items stored in the unsecured common areas of a multi-unit apartment building or put in a dumpster accessible to the public.” *Id.* at 1342. Here, S.H., her children, or any guest could examine the contents of these SD cards without going into Mininger’s room. Because Mininger placed the SD cards—and thus the cards’ contents—in a shared area, liable to be discovered and examined by a third party, and beyond his area of control, he cannot claim to have a reasonable expectation of privacy in their content. *Id.*; see also *United States v. Hall*, 47 F.3d 1091, 1097 (11th Cir. 1995) (holding that there is no objectively reasonable expectation of privacy when a defendant does not “take sufficient steps to restrict the public’s access to [his] discarded garbage”).

Further, the cameras—located as they were in the bedroom and bathroom of S.H.’s minor daughter—were self-evidently placed to illegally invade the privacy of S.H.’s children. We have previously “found permissible warrantless searches where the container itself and the circumstances under which the police obtained it indicate that the contents are contraband.” *United States v. Epps*, 613 F.3d 1093, 1098 (11th Cir. 2010). So too, here. No one could reasonably expect a right to privacy in voyeuristic recordings made under these circumstances. Accordingly, the warrantless search of the illicitly placed cameras and their SD cards was permissible.

For his part, Mininger points to *Minnesota v. Olson* and the “legitimate expectation of privacy” overnight guests have in their host’s home. 495 U.S. 91, 98 (1990). No doubt, an overnight guest retains a reasonable expectation of privacy notwithstanding that a host could, theoretically, look through his things while he is out. The Court in *Olson* stressed that this expectation of privacy is rooted in social norms and “the everyday expectations of privacy that we all share.” *Id.* “Staying overnight in another’s home is a longstanding social custom that serves functions recognized as valuable by society.” *Id.* Because “[w]e will all be hosts and we will all be guests many times in our lives . . . society recognizes that a houseguest has a legitimate expectation of privacy in his host’s home.” *Id.*

The social custom underpinning *Olson* does not help Mininger here. An overnight houseguest has the highest legitimate expectation of privacy in his own quarters. *See United States v. Rackley*, 742 F.2d 1266, 1270 (11th Cir. 1984). But, when guests leave unsecured belongings in shared areas, such as a bathroom, the expectation of privacy is much weaker. *Id.*; *see also Olson*, 495 U.S. at 98–99. And a guest’s reasonable expectation of privacy assumes a degree of reciprocity—the host and third parties will respect a guest’s right to privacy just as the guest and third parties will respect the host’s privacy. Consequently, no houseguest has a reasonable expectation of privacy in voyeuristic recordings made in his host’s home without his host’s knowledge or consent. When a guest so plainly exceeds the scope of societal custom and his host’s license, any expectation of privacy becomes unreasonable.

25-10073

Opinion of the Court

9

For the above reasons, we reject Mininger’s argument that the Fourth Amendment bars admission of the evidence gathered from the warrantless search of his SD cards.

*B.*

We turn now to Mininger’s argument that the warrants issued for his residence, vehicles, devices, and person were overbroad. Specifically, he complains that the warrants did not place “available, appropriate limits” on law enforcement’s search of Mininger’s devices. Appellant’s Br. at 37. He says that, because law enforcement had probable cause to search for pictures of specific people made during a specific time period, the Fourth Amendment requires them to have used forensics tools to limit their search to electronic files created of those specific people or during that particular time period. We disagree.

We have recognized that the Fourth Amendment prohibits the government from engaging in a “general, exploratory rummaging in a person’s belongings.” *United States v. Wuagneux*, 683 F.2d 1343, 1348 (11th Cir. 1982) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). And, when addressing searches of cloud accounts, we have suggested that time limits on “the scope of a search warrant for a cloud account” are a good way to ensure that warrants are not overbroad. *United States v. McCall*, 84 F.4th 1317, 1328 (11th Cir. 2023).

Nevertheless, our case law does not require that a warrant impose a time limit or a similar restriction on the search of an electronic storage device. We distinguished between electronic devices

and cloud accounts in *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017). There, we stressed that the “means of hiding evidence on a hard drive—obscure folders, misnamed files, encrypted data—are not currently possible in the context of a” cloud-based account. *Id.* at 974. “Hard drive searches require,” as the facts of this case highlight, “time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant’s home would be impractical, if not impossible.” *Id.* “By contrast,” with respect to cloud-based accounts, “the government need only send a request with the specific data sought and [the cloud service provider] will respond with precisely that data.” *Id.*

The facts of this case underscore the difference between the search of a cloud-based account and the search of an electronic storage device. The search warrants here were not directed at cloud accounts under the control of a third party; they were directed at electronic storage devices in Mininger’s physical possession. When these devices were in his possession, Mininger had gone to great lengths to obfuscate the nature of his data, employing the VeraCrypt program to conceal the files. The search required that a forensic examiner break the encryption of Mininger’s illicit files. This effort is a far cry from “send[ing] a request with the specific data sought” to a cloud-service provider and receiving exactly that data. *Id.* It is not feasible for a warrant to limit the scope of a “hard drive search[],” *id.*, in the same way a warrant might limit the search of a cloud account under the control of a third party.

25-10073

Opinion of the Court

11

A warrant must be as “specific as the circumstances and nature of activity under investigation permit[s].” *Wuagneux*, 683 F.2d at 1349; *see also United States v. Strauss*, 678 F.2d 886, 892 (11th Cir. 1982) (“A search warrant must indeed be sufficiently precise as not to permit a general search, but the test is . . . reasonableness . . .”). Here, the relevant warrant was limited to seizing “records relating to Child Pornography and Sexual Exploitation.” Accordingly, it was not overbroad.

#### IV.

For the reasons outlined in this opinion, Mininger’s convictions are **AFFIRMED**.