STATE OF MINNESOTA
IN COURT OF APPEALS
A19-1886

State of Minnesota,
Respondent,

vs.

Tyler Ray Pauli,
Appellant.

Filed November 30, 2020
Affirmed
Schellhas, Judge[*]

St. Louis County District Court
File No. 69DU-CR-17-3210

Keith Ellison, Attorney General, Peter Magnuson, Assistant Attorney General, St. Paul, Minnesota; and

Mark S. Rubin, St. Louis County Attorney, Duluth, Minnesota (for respondent)

Cathryn Middlebrook, Chief Appellate Public Defender, Laura Heinrich, Assistant Public Defender, St. Paul, Minnesota (for appellant)

Considered and decided by Frisch, Presiding Judge; Johnson, Judge; and Schellhas, Judge.

[*] Retired judge of the Minnesota Court of Appeals, serving by appointment pursuant to Minn. Const. art. VI, § 10.

U N P U B L I S H E D O P I N I O N

SCHELLHAS, Judge

Appellant challenges his conviction of possession of pictorial representation of minors, arguing that the district court erred by concluding that (1) he did not have a reasonable expectation of privacy in the child-pornography content in his Dropbox account, and (2) law enforcement did not exceed the scope of Dropbox's private search of his account. We affirm.

FACTS

Appellant Tyler Ray Pauli established an account with Dropbox, a company that provides online file storage and sharing services to its users. As a precondition to creating an account, Dropbox required Pauli to agree to its terms of service. Those terms of service provided that users retain ownership of their own files, and that Dropbox believes that user information should receive the same legal protections on its servers as it receives on users' home hard drives. But the terms of service also provided that, in using Dropbox services, users "must not even try to . . . publish or share materials that are unlawfully pornographic or indecent," "violate the law in any way," or "violate the privacy or infringe the rights of others," and that Dropbox may access, store, and scan users' files. And, significantly, the terms of service provided that users granted Dropbox permission to access, store, and scan files; that Dropbox could review user conduct for compliance with the terms of service; and that Dropbox could disclose user information to third parties if necessary to comply with its own legal obligations and prevent abuse of its services.

In offering its services as an electronic service provider, Dropbox must comply with federal law. 18 U.S.C. § 2258A(a) (2018). Although the law mandates that electronic service providers report any "apparent violation" of federal child pornography law of which they have "actual knowledge," it does not require electronic service providers to actively monitor users or content, or to search, screen, or scan for violations. *Id.* (a), (f) (2018). The National Center for Missing and Exploited Children (NCMEC), a nonprofit organization, operates the CyberTipline to which electronic service providers must report suspected law violations. *Id.*; 34 U.S.C. § 11291(7) (2018). In turn, NCMEC investigates the reports and forwards them to applicable law enforcement agencies. 18 U.S.C. § 2258A(c) (2018). An electronic service provider that "knowingly and willfully fails to make a report" is subject to a fine. *Id.* (e) (2018).

In this case, Dropbox identified suspected child pornography in Pauli's account and reported 63 files from the account to NCMEC's CyberTipline. Consistent with its practices, NCMEC opened only two of the 63 files, confirmed that they contained child pornography, and forwarded the report to the Minnesota Bureau of Criminal Apprehension (BCA). BCA's Special Agent John Norberg opened all 63 files in the report and determined that they contained child pornography. Neither NCMEC nor BCA obtained warrants before their initial reviews of the files in Dropbox's report. After reviewing the 63 files received from NCMEC, Special Agent Norberg obtained warrants to search Pauli's residence and his entire Dropbox account. During execution of the warrant at Pauli's residence, Pauli admitted that he had a Dropbox account, that he obtained links to child pornography

through the Kik app,[1] and that he uploaded files to his Dropbox. In response to the warrant, Dropbox produced a USB device that contained Pauli's account files. Special Agent Norberg found child pornography in 156 of the files on the USB device and forwarded them to NCMEC. NCMEC confirmed that 20 files contained previously identified victims.

Respondent State of Minnesota charged Pauli with four counts of possession of pictorial representation of minors in violation of Minn. Stat. § 617.247, subd. 4(a) (2016). Pauli moved to suppress evidence located in the two files initially reviewed by NCMEC and the 63 files initially reviewed by BCA, arguing that NCMEC's and BCA's reviews violated his Fourth Amendment rights as warrantless searches. He also asserted that because the subsequent search warrants obtained by BCA were products of the "warrantless searches," evidence obtained during their execution must be suppressed. The district court denied Pauli's motion, conducted a stipulated evidence trial under Minn. R. Crim. P. 26.01, subd. 4, and found Pauli guilty of all four counts.

This appeal follows.

D E C I S I O N

Both the United States and Minnesota constitutions guarantee people the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV; Minn. Const. art. I, § 10. Evidence obtained in violation of these protections usually must be suppressed. *State v. Jackson*, 742 N.W.2d 163, 178 (Minn. 2007). A Fourth Amendment search occurs when the government (1) physically intrudes into a constitutionally protected area, or

[1] The Kik app is a chat and media-sharing sharing application.

(2) infringes on a person's objectively reasonable expectation of privacy. *United States v. Jones*, 565 U.S. 400, 407-08, 132 S. Ct. 945, 951 (2012); *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S. Ct. 1652, 1656 (1984).[2]

In reviewing the district court's pretrial suppression order, we will affirm the district court's factual findings unless they are clearly erroneous, but review the district court's legal conclusions de novo. *State v. Edstrom*, 916 N.W.2d 512, 517 (Minn. 2018). A defendant bears the burden of proving that his constitutionally protected right has been infringed. *Id.*

I.

The district court concluded that Pauli did not have a reasonable expectation of privacy in the child-pornography content in his Dropbox account. Pauli maintains that the district court erred. To demonstrate an expectation of privacy, a person must establish that (1) he or she had a subjective expectation of privacy in the place or thing searched, and (2) society recognizes that expectation as reasonable. *Smith v. Maryland*, 442 U.S. 735, 740, 99 S. Ct. 2577, 2580 (1979).

A. Subjective Expectation of Privacy.

The district court found that it was "understandable and likely" that Pauli had a subjective expectation of privacy in his Dropbox account. The state does not challenge

[2] The Fourth Amendment and Article I, Section 10 of the Minnesota Constitution are "textually identical," so Supreme Court precedents are persuasive but not compelling. *State v. Wiegand*, 645 N.W.2d 125, 132 (2002).

this finding on appeal. We therefore assume, without deciding, that Pauli had a subjective expectation of privacy in his Dropbox account.

B. Objectively Reasonable Expectation of Privacy.

The district court found that Pauli lacked an objectively reasonable expectation of privacy in the child-pornography content in his Dropbox account because Dropbox's terms of service undermined that expectation. We agree.

An expectation of privacy is objectively reasonable if it is one that society is prepared to recognize as reasonable. *State v. Perkins*, 588 N.W.2d 491, 492-93 (Minn. 1999). "The Fourth Amendment applies only to state action, so it does not constrain private parties unless they act as agents or instruments of the government." *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (citing *Jacobsen*, 466 U.S. at 113, 104 S. Ct. at 1656). Under the third-party doctrine, "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44, 99 S. Ct. at 2582; *see also State v. Carter*, 697 N.W.2d 199, 207 (Minn. 2005) (stating that a person has no Fourth Amendment protection in anything knowingly disclosed to the public). Similarly, a defendant may waive even a reasonable expectation of privacy if his or her behavior and the circumstances, taken as a whole, mandate the conclusion that the expectation was unreasonable. *Perkins*, 588 N.W.2d at 493.

In the context of electronic service providers like Dropbox, courts are split with regard to whether terms of service eliminate or diminish a user's objectively reasonable expectation of privacy. *Compare United States v. Ackerman*, 296 F. Supp. 3d 1267, 1272 (D. Kan. 2017) (holding that, given appellant's agreement to AOL terms of service,

appellant did not have reasonable expectation of privacy in a particular email and its attachments), *aff'd*, 804 Fed. Appx. 900 (10th Cir. Feb. 26, 2020) *with United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (holding that defendant had reasonable expectation of privacy in email, despite subscriber agreement notifying him that email provider may access his information, but acknowledging that subscriber agreement could be "broad enough to snuff out a reasonable expectation of privacy").[3]

Here, Pauli agreed to Dropbox's terms of service before he established his Dropbox account. The terms are clear and unambiguous that although users retain ownership of the files stored in their Dropbox accounts, Dropbox's terms of service prohibit publishing or sharing illegal content of any kind, specifically including unlawful pornographic content, and allow Dropbox to review user "conduct and content for compliance" with the terms of service, and to disclose any violations to third parties. Dropbox's terms of service were much like the electronic service providers' terms of service in cases in which courts found that a user had no objectively reasonable expectation of privacy. In those cases, as here, the terms of service prohibited illegal activity, permitted the provider to review user activity and content, and permitted the provider to report violations of their terms and other law to third parties. *See Ackerman*, 296 F. Supp. 3d at 1272; *United States v. Stratton*, 229 F. Supp. 3d 1230, 1242 (D. Kan. 2017) (noting that terms of service prohibited illegal uses of services, allowed provider to monitor online activity, and allowed provider to disclose

[3] Though not binding on Minnesota courts, authorities from other states or federal courts can be persuasive. *State v. McClenton*, 781 N.W.2d 181, 191 (Minn. App. 2010), *review denied* (Minn. June 29, 2010).

information to law enforcement). *But see Warshak*, 631 F.3d at 287; *United States v. DiTomasso*, 56 F. Supp. 3d 584, 592 (S.D.N.Y. 2014) (holding that, despite terms of service that allowed providers to disclose violative content to law enforcement, defendant retained expectation of privacy in email and online chats).

In this case, the undisputed evidence reflects that Pauli voluntarily stored his child-pornography content with Dropbox despite clear and unambiguous warnings that such content violated Dropbox's policies; that Dropbox could review Pauli's conduct and content for compliance; and that Dropbox could report his content to law enforcement. Pauli voluntarily turned his information over to a third party subject to clear and unambiguous terms of service that undermined any objectively reasonable expectation of privacy in his Dropbox account content. When a person lacks an objectively reasonable expectation of privacy, no unreasonable search occurs, and the constitutional protections of the Fourth Amendment and Article I, Section 10 of the Minnesota constitution are not implicated. *See Smith*, 442 U.S. at 745-46, 99 S. Ct. at 2583 (holding that installation of pen register was not a search and no warrant was required because defendant had no reasonable expectation of privacy in the phone numbers he dialed); *Perkins*, 588 N.W.2d at 493 (holding that defendant's expectation of privacy was unreasonable and his Fourth Amendment rights were not infringed by search of his hotel room). Such is the case here. We therefore affirm the district court's determination that Pauli did not have an objectively

reasonable expectation of privacy in his Dropbox account, and we affirm the district court's denial of Pauli's suppression motion.[4]

II.

Because we conclude that Pauli did not have an objectively reasonable expectation of privacy in the child-pornography content in his Dropbox account, federal and state constitutional protections do not apply to NCMEC's review of two of the 63 files reported by Dropbox or to BCA's initial review of all 63 files provided by NCMEC. We therefore conclude that neither NCMEC's nor BCA's review of the files in Dropbox's report violated Pauli's constitutional rights and need not address whether the private-search doctrine applies here.

Affirmed.

[4] Pauli also argues that NCMEC and BCA trespassed on his digital property, therefore meeting the *Jones* test for an unreasonable search. 565 U.S. at 407, 132 S. Ct. at 951. We are not persuaded. NCMEC and BCA did not access Pauli's Dropbox account; rather, they reviewed files included with Dropbox's report. We conclude that neither NCMEC nor BCA trespassed on Pauli's digital property.