

**STATE OF MINNESOTA
IN COURT OF APPEALS
A24-0555**

State of Minnesota,
Respondent,

vs.

Dylan Stephen Gaul,
Appellant.

**Filed February 3, 2025
Affirmed
Harris, Judge**

Steele County District Court
File No. 74-CR-22-1882

Keith Ellison, Attorney General, St. Paul, Minnesota; and

Robert J. Jarrett, Steele County Attorney, Connor B. Burton, Assistant County Attorney,
Owatonna, Minnesota (for respondent)

Cathryn Middlebrook, Chief Appellate Public Defender, Gina D. Schulz, Assistant Public
Defender, St. Paul, Minnesota (for appellant)

Considered and decided by Cochran, Presiding Judge; Ross, Judge; and Harris,
Judge.

SYLLABUS

A criminal defendant does not have a reasonable expectation of privacy in emails knowingly sent to a student's school-owned email account and received on a public school's server.

OPINION

HARRIS, Judge

Respondent State of Minnesota charged appellant Dylan Stephen Gaul with fourth-degree criminal sexual conduct based on emails Gaul exchanged with a 14-year-old public-school student. Gaul filed a motion to suppress the evidence against him. Gaul argued that the emails he sent to the student's school-owned email account were subject to an unconstitutional, warrantless search by the school when it used protective software to scan the emails. In support of this argument, he asserts that he had a reasonable expectation of privacy in email communications under the federal and state constitutions. After a contested omnibus hearing, the district court denied his motion. Gaul stipulated to the state's case to obtain review of the pretrial ruling, and the district court found him guilty of fourth-degree criminal sexual conduct. On appeal, Gaul argues that his conviction must be reversed because (1) the district court's finding that the search occurred after his emails arrived on the school server was clearly erroneous, and (2) he had a reasonable expectation of privacy in his email communications. Because we conclude that appellant did not have a reasonable expectation of privacy in email communications addressed to a student's school-owned email account and received on a public school's server, we affirm.

FACTS

The Owatonna School District is a public school district located in southern Minnesota. The school district provides its students with an email account and an associated email address to use while enrolled. Each email address issued by the school

district ends in “isd761.org.” Each student email account is hosted by Google servers.¹ The school district also uses a separate application called Bark that works in conjunction with the Google servers to screen emails going to-and-from the students’ school-owned email accounts. Its purpose is to monitor content indicating self-harm, violence, bullying, sexual contact or content, or drugs. When Bark detects this type of content, it sends an alert to the school’s information technology (IT) department along with a copy of the alarming material. The software can also label certain alerts as “severe.” While Bark can view everything, it alerts IT only when it detects concerning content in students’ email accounts. IT will then forward the material to the school resource officer (SRO) for further investigation.

In November 2022, the school’s IT department alerted the SRO that a 14-year-old female student was exchanging emails of a sexual nature with an external email address. After reviewing the correspondence, the SRO found that the communications were not only sexual in nature, but also referred to drug exchanges. And after further investigation, the SRO determined that the external email address was associated with Gaul, a former Owatonna High School Student.² The SRO applied for a search warrant for Gaul’s residence, phone, and person.³ At a contested omnibus hearing, the SRO agreed that he

¹ Google servers is an email-hosting service that provides server space to operate and manage email accounts.

² The SRO testified at a contested omnibus hearing that when he was initially contacted, he was given some information about the external email address, including the screen name associated with it. When the SRO conducted an internet search for the screen name, it brought him to a YouTube page that included photos of Gaul, whom he recognized.

³ The search warrant was never executed because Gaul was arrested outside his residence. But the SRO applied for and executed a second warrant for a search of Gaul’s phone.

would not have investigated Gaul but for the alert from IT. In a statement to the police, Gaul admitted that he had communicated with the student and discussed exchanging THC cartridges and vape pens for sex.⁴ Based on this evidence, the state charged Gaul with two counts of criminal sexual conduct under Minnesota Statutes section 609.344, subdivision 1a(b) and 609.345, subdivision 1a(b) (2022).

Gaul filed a motion to suppress all evidence and dismiss the criminal charges, arguing that the school district's use of the Bark software to screen his emails amounted to an unlawful search while in transit and prior to delivery in the student's inbox.⁵ At a contested omnibus hearing, Gaul called the school district's IT director as a witness. The IT director testified generally about the software applications, such as Google and Bark, that the school district uses. Regarding when the search of the email occurred, the following exchange was had:

GAUL'S ATTORNEY: And so it view -- it reviews the electronic content of every e-mail sent to student e-mail address, but then it only provides you an alert to look at something with certain things then?

M.H.: Correct.

GAUL'S ATTORNEY: And does Bark read the e-mails prior to the e-mail landing in the student's actual account, or does it do it once the e-mail's physically in the account?

M.H.: That's a good question. I don't know that I've got an answer that I could give you at this time.

⁴ The 14-year-old student also gave a statement that she and Gaul communicated to arrange sexual favors for THC cartridges and vape pens mostly through email.

⁵ Minn. Stat. § 609.352, subd. 2(a)(1); Minn. Stat. § 609.324, subd. 1(b)(2) (2022).

GAUL’S ATTORNEY: So it is – it’s possible then that Bark is screening each e-mail prior to it actually hitting the student’s e-mail drive or account I should say?

M.H.: It’s not – it’s not impossible. I don't know. My answer to that is I don’t know.

During cross-examination, the IT director agreed that outgoing emails from students contain a disclaimer indicating that the email account and its contents are managed by the Owatonna School District and subject to the district’s policies. Students are also made aware that school policy limitations—such as discussing the sale or purchase of drugs and acts of a sexual nature—apply to their student email accounts.

The district court denied Gaul’s motion to suppress, finding that “[t]he messages arrived at the server before the software initiated a search” and, therefore, Gaul had no reasonable expectation of privacy. Gaul waived his right to a jury trial and stipulated to the prosecution’s case under Minnesota Rule of Criminal Procedure 26.01, subdivision 4, preserving his suppression issue for appellate review. The state dismissed all charges but fourth-degree criminal sexual conduct and agreed that the pretrial issue was dispositive. The district court found Gaul guilty.

Gaul appeals.

ISSUES

- I. Did the district court clearly err by finding that the search of Gaul’s emails occurred after the emails were delivered?
- II. Did Gaul have a reasonable expectation of privacy or property interest in emails sent to a student’s school-owned email account and received on a public school’s server?

ANALYSIS

I. The district court did not clearly err by finding that the search of Gaul's emails occurred after they were received on the school district's server.

Gaul argues that the district court clearly erred in finding that the search of his emails occurred after they reached the school district's server. He contends that the timing of the search is critical because if the search occurred while the email was in transit it was an illegal search within the Minnesota and United States constitutions. Gaul asks us to reverse his conviction because the state did not carry its burden to prove the search of his emails occurred after it was received on the school district's server, and that he had a private property interest and a reasonable expectation of privacy in his email communications before they reached the school's server. We disagree.

“For pretrial motions to suppress, we review the district court's factual findings for clear error and its legal determinations de novo.” *State v. Leonard*, 943 N.W.2d 149, 155 (Minn. 2020). “Findings of fact are clearly erroneous if, on the entire evidence, we are left with the definite and firm conviction that a mistake occurred.” *State v. Andersen*, 784 N.W.2d 320, 334 (Minn. 2010). “If we find reasonable evidence to support the district court's findings of fact, we will not disturb those findings.” *State v. Evans*, 756 N.W.2d 854, 870 (Minn. 2008) (quotation omitted).

The district court found that the search took place after Gaul's emails to the student arrived on the school's server and therefore were no longer within his control. It stated that “Gaul's communications were received by a school district email server as he intended. It was only upon receipt of those communications that the *student's email* was subject to

the school's privacy policy and monitoring system." Gaul asserts this finding was clearly erroneous because the state presented no evidence that the emails were searched after delivery. We disagree.

Although M.H. could not definitively state when Bark screens the student's emails, other evidence in the record supports a reasonable inference that Gaul's emails were screened only after they arrived on the school's server. M.H. testified that Bark was a program used in conjunction with the Google hosting system and that Bark is a separate program connected to Google Gmail that screens student emails. There was testimony that Bark monitors only *student* accounts, not staff accounts, and those emails sent and received by students. Therefore, the record does not reasonably support Gaul's assertion that Bark could have screened Gaul's emails *before* they arrived on the school district's server. Under these circumstances, we are not left with a definite and firm conviction that the district court's finding was clearly erroneous.

II. Gaul did not have a reasonable expectation of privacy or property interest in emails sent to a student's school-owned email account and received on the school's server.

Gaul also challenges the district court's determination that he did not have a reasonable expectation of privacy in email communications that he sent to the student's school-owned email account and that were delivered to the school's server. This court reviews the district court's pretrial legal rulings de novo. *State v. Bourke*, 718 N.W.2d 922, 927 (Minn. 2006). Gaul bears the burden to establish that he has a protected right under the United States and Minnesota constitutions. *Leonard*, 943 N.W.2d at 156.

Both the United States and Minnesota constitutions require that government searches and seizures of people’s “persons, houses, papers, and effects” be reasonable. U.S. Const. amend. IV; Minn. Const. art. I, § 10. “A seizure of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Warrantless searches are per se unreasonable subject to only a few specifically delineated exceptions. *Arizona v. Gant*, 556 U.S. 332, 338 (2009); *State v. Diede*, 795 N.W.2d 836, 846 (Minn. 2011).

A search or seizure within the Fourth Amendment occurs when the [government] either “physically occupy[s] private property for the purpose of obtaining information,” *United States v. Jones*, 565 U.S. 400, 404 (2012), or invades a constitutionally protected privacy interest to gather information. *Katz v. United States*, 389 U.S. 347, 360-61 (1967). Gaul argues that both occurred here. We address each argument in turn and conclude that neither is persuasive.

A. Property Trespass

Relying on *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), Gaul argues that the government trespassed on his papers and effects when it searched his emails while in transit. In *Ackerman*, the defendant sent an email containing child pornography. 831 F.3d at 1294. However, before the email reached its intended recipient, the defendant’s Internet Service Provider (ISP), AOL, using an automated filter designed to stop its users from transmitting child pornography, stopped its delivery. *Id.* The Tenth Circuit applied a property-rights analysis articulated in *Jones* to hold that the government violates the Fourth Amendment when it trespasses upon emails sent to a third party. *Id.* at 1307-08.

Ackerman is distinguishable from this case. Unlike in *Ackerman* where the email never reached the intended recipient, the district court here found that Gaul's emails arrived in the student's inbox, at which point he relinquished his control and any property interest of his correspondence and, as discussed above, we concluded that this finding was not clearly erroneous. Because Gaul relinquished control of his emails when they successfully arrived at the school district's server, the school district did not "physically occup[y] private property for the purpose of obtaining information" and thus did not conduct a search within the meaning of the Fourth Amendment.

B. Reasonable Expectation of Privacy

The district court concluded that Gaul did not have a reasonable expectation of privacy because he relinquished control of his emails, which were searched after they were received by the school server. Gaul maintains that the district court erred, arguing that he had a reasonable expectation of privacy in his sent emails, an expectation that was not eliminated just because they were sent to a student's school-owned email account. To contest a government search, a person must demonstrate (1) that, by his conduct, he "exhibited a subjective expectation of privacy" (subjective prong); and (2) that society recognizes such an expectation as objectively reasonable (objective prong). *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quotation omitted); *In re Welfare of B.R.K.*, 658 N.W.2d 565, 571 (Minn. 2003). The subjective prong evaluates the circumstances and conduct of the individual and whether that person demonstrated that "he seeks to preserve something as private." *Smith*, 442 U.S. at 740 (quotation omitted). The objective prong

considers whether the person’s expectation was “justifiable under the circumstances.” *Id.* (quotation omitted).

Turning first to the subjective prong, Gaul did not exhibit a subjective expectation that his emails would remain private. *See Minnesota v. Carter*, 525 U.S. 83, 107, 119 (1998) (Ginsburg, J., dissenting) (recognizing a person’s reasonable expectation of privacy “turns in large part” on their “ability to exclude others from the place searched”). Here, Gaul engaged in private communications of a sensitive nature over a series of emails using a password-protected unique email with a screenname presumably designed to further conceal his connection to the email exchange. While Gaul insists that the highly sensitive nature of his emails, coupled with the fact that he communicated with just one student, demonstrates that he likely believed they would remain private, we are not convinced. Gaul emailed a student at their school-district-provided email address. The school’s head of IT, M.H., testified that when students send emails, there is a disclaimer in the footer of the email that states that the email account is owned and managed by the school district and is subject to the school district’s policies. M.H. additionally testified that there are policies that discuss the proper use of emails and affirmed that student emails are accessible by IT “just by virtue of them being school e-mail[s].” And according to the student, Gaul knew how old she was and that they “had talked about it.”⁶ For these reasons, we conclude that Gaul did not have a subjective expectation of privacy in the emails addressed to a student’s school-owned email account.

⁶ Gaul denies that he knew the student was a minor, but he did tell police that he met the student in a class that they had together in high school.

Even if we assume that Gaul had a subjective expectation of privacy in the emails, the next inquiry is whether that expectation is one that society is prepared to recognize as reasonable. *See New Jersey v. T.L.O.*, 469 U.S. 325, 338 (1985) (stating that “the Fourth Amendment does not protect subjective expectations of privacy that are unreasonable”). “Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable.” *Jacobsen*, 466 U.S. at 114. While letters and packages are in transit to the intended recipient, law enforcement generally cannot intercept and examine them without a warrant. *Id.* This is true for email messages and content. *City of Ontario v. Quon*, 560 U.S. 746, 762 (2010) (implying that “a search of [an individual’s] personal e-mail account” would be just as intrusive as “a wiretap on his home phone line”); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that “[t]he privacy interests in [mail and email] are identical”). The question remains, however, whether the *contents* of Gaul’s email messages receive Fourth Amendment protections once received by the student’s email account on the school server.

Here, the district court determined that Gaul relinquished any expectation of privacy once the emails were received by the intended recipient. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2nd Cir. 2004) (stating that individuals may not enjoy “an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient”) (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001)); *United States v. Barber*, 184 F. Supp. 3d 1013, 1017 (D. Kan. 2016) (“[A] legitimate expectation of privacy in an email is lost once the email reaches the recipient.”) (citing *Guest*, 255 F.3d at 333);

United States v. Lustyik, 57 F. Supp. 3d 213, 223 (S.D.N.Y. 2014) (“A person has no expectation of privacy in another person’s email account.”).⁷ We agree with the district court.

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; *see also Jacobsen*, 466 U.S. at 117 (“It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.”); *Katz*, 389 U.S. at 351 (“What a person knowingly exposes to the public is not a subject of Fourth Amendment protection.”); *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). The school district did not search Gaul’s computer containing the email, but rather searched a current student’s school-provided email account and found an email sent to that student by Gaul after it was delivered to the school’s email server. Under the third-party doctrine, Gaul relinquished any expectation of privacy in his email communications once they were sent and received by the student’s school-provided email account.

Gaul asserts that the third-party doctrine is an “open question” and does not immediately destroy the sender’s expectation of privacy in one-way transmissions of

⁷ 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), *rev. denied* (Minn. June 29, 2010).

information. He analogizes emails to one-sided phone conversations. It is true that disclosing information to a third-party does not automatically eliminate the person's expectation of privacy in that information. *See Katz*, 389 U.S. at 353 (holding that a person retains an expectation of privacy for conversations in a public telephone booth); *see also Carpenter v. United States*, 585 U.S. 296, 309 (2018) (holding that cell-site location information stored on a wireless carrier's server does not render an individual's expectation of privacy unreasonable). However, even if we accept the premise that emails are more like phone calls, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities." *United States v. Miller*, 425 U.S. 435, 443 (1976). A person assumes the risk that what they communicate to a third party, whether verbally or electronically, may be disclosed to another person, including the government. *Jacobsen*, 466 U.S. at 117. Whether the recipient verbally relays to police what the speaker told him, brings law enforcement the sender's letter, or forwards his email to police, the risk remains the same.

To persuade us otherwise, Gaul again relies on *Ackerman* to argue that he had a reasonable expectation of privacy for emails in transit. As discussed above in *Ackerman*, AOL detected the child pornography in the defendant's email, stopped the emails delivery, and reported the emails to the National Center for Missing and Exploited Children (NCMEC), as required by federal law. *Id.* at 1294. The defendant alleged that an unlawful search under the Fourth Amendment occurred because the NCMEC included the emails and each attachment, which an NCMEC agent could open and view. *Id.* at 1307-08. The court held that NCMEC's actions clearly amounted to a search when it opened and

examined private correspondence. However, the court did not decide whether Ackerman had a subjective or objective expectation of privacy because the district court had made no factual findings as to his subjective or objective expectations. *Id.* at 1305. The Tenth Circuit also expressly noted that the defendant's reasonable expectations of privacy could be constrained by "the parties' dealings," including Ackerman's acquiescence to the service provider's policies regarding child pornography. *Id.* at 1305. The court remanded the case for further analysis, as these were "[f]acts that could well impact the legal analysis." *Id.*

This is true for Gaul's argument as well. Similar to *Ackerman*, any reasonable expectation of privacy Gaul may have had in emails sent to the student was constrained by the parties' dealings because the school district did not guarantee or offer that the electronic "property" stored on its servers would be private. To the contrary, the school district expressly warns users that the email account, or contents of the email, are managed by the district and its policies. The school district's warning that the contents of the email are managed by the district and its policies is inconsistent with a reasonable expectation of privacy.

Gaul additionally relies on *Leonard*, 943 N.W.2d at 149, to assert that he has a reasonable expectation of privacy because the Minnesota Constitution provides greater protections than the United States Constitution. While it is true that state constitutions may provide more protections than the federal constitution, Gaul's reliance on *Leonard* is misguided. There, Leonard voluntarily shared certain private information with a hotel he checked into, as required by statute. *Id.* at 153. Police used this information to develop

individualized suspicion of criminal activity and conducted an arrest. Leonard argued that he had a reasonable expectation of privacy in information disclosed to a hotel's guest registry. *Id.* The supreme court agreed and held that "some third-party institutions are generally considered private (e.g., a doctor's examination room or a lawyer's office)" and, therefore, "sharing private information in these spaces does not destroy someone's reasonable expectation of privacy, but rather contributes to its private character." *Id.* at 159.

A student's school-owned email account, however, cannot be one of those third-party institutional spaces contemplated by the supreme court. Ordinary people reasonably expect that their lawyers and physicians will keep their information confidential, but it is unlikely that this expectation would extend to a student's school-owned email account. To this end, students have a reduced expectation of privacy because of the school's interest in "the preservation of order and a proper educational environment." *T.L.O.*, 469 U.S. at 339.

Gaul contends that, because he is not a student, he maintains the full scope of Fourth Amendment protections. Again, we are not persuaded. While he may not be a student, Gaul was emailing a current student at her school-owned email account, which should have alerted him that his communications were not private and likely to be monitored. As M.H. testified, emails from the student accounts included a disclaimer that expressly stated that the email is owned or managed by the school district thus communicating that the recipient of the email should have a diminished expectation of privacy in email communications with that email account. Gaul knew or should have known this because he exchanged multiple emails with the victim.

DECISION

Because the district court did not clearly err in finding that Gaul's emails were searched after they reached the school's server, and because Gaul did not have a reasonable expectation of privacy in email communications sent to a school-owned email server and delivered to a student's email account, we affirm the district court's pretrial ruling denying Gaul's motion to dismiss and suppress the evidence.

Affirmed.