January 7, 2025

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON DIVISION II

| STATE OF WASHINGTON, | | No. 58094-2-II |
|----------------------|-------------|---------------------|
| | Respondent, | |
| v. | | UNPUBLISHED OPINION |
| STEPHEN RIAN PRICE, | | |
| | Appellant. | |

CHE, J. — After Stephen Price posted videos and pictures of him raping and molesting his infant daughter and his neighbor's young son on the internet, private internet service providers (ISPs) submitted CyberTips reporting suspected child abuse and child sexual abuse materials¹ to the National Center for Missing and Exploited Children (NCMEC). NCMEC forwarded the tips to local law enforcement, and Price was ultimately convicted of five counts of first degree rape of a child, one count of first degree child molestation, three counts of first degree dealing in depictions of a minor engaged in sexually explicit conduct, four counts of sexual exploitation of a minor, and four counts of first degree possession of depictions of a minor engaged in sexually explicit conduct, with the jury finding aggravating circumstances on several counts.

Price appeals arguing that the trial court improperly denied his motion to suppress the evidence of his crimes obtained from the ISPs. He argues that the evidence was obtained through

¹ We employ the term "child sexual abuse materials" and not "child pornography" throughout this opinion to avoid using language that minimizes the harm experienced by children who are victims of these serious criminal offenses.

a warrantless search in violation of the Fourth Amendment and Washington Constitution article I, section 7. Price also argues that the trial court erred by ordering that his sentence be served consecutively to his prospective sentence in a related federal criminal case and by imposing various legal financial obligations. We hold that the trial court did not err by denying his motion to suppress but accept the State's concessions on the sentencing issues. Accordingly, we affirm Price's convictions but remand for correction of his judgment and sentence.

FACTS

Federal law mandates that internet service providers (ISPs) such as Google, Discord, AOL, and Skype report suspected child sex abuse that appears on the ISP's platform to the NCMEC. 18 U.S.C. § 2258A. ISPs often employ hashing technology to rapidly and automatically identify suspected child sexual abuse materials. Hash values are short, distinctive identifiers that enable the rapid comparison of one file to another. The NCMEC analyzes these "CyberTips" and forwards them to the regional Internet Crimes Against Children (ICAC) agency who then forwards them to local law enforcement.

Discord, an ISP that is primarily used by online gamers and gives gamers the ability to chat, identified suspected child sexual abuse materials through its hashing technology and sent a "priority one" CyberTip of child molestation to NCMEC. That same week, Skype also identified suspected child sexual abuse materials. Between Discord and Skype, six CyberTips of child sexual abuse, including a video, were submitted to NCMEC. NCMEC identified the video as child abuse and forwarded the video and a description of the abuse to the Vancouver Police Department. The video showed Price anally penetrating his infant daughter with his erect penis. Vancouver police issued exigency letters to various carriers and obtained an IP address.

Using the IP address and identifying information from chats and usernames in the six CyberTips, law enforcement determined the physical location and obtained a search warrant for a room at a motel in Washougal, Washington. Therein, police found Price, Price's pregnant girlfriend, Price's mother, and Price's infant daughter, KEP. A search of Price's laptop and cellphone revealed additional images of sexual abuse of minors. Police took Price into custody. He agreed to be interviewed.

During his interview, Price admitted sexually assaulting KEP multiple times and recorded the abuse on his cell phone. Price explained that he used Discord to distribute videos of the abuse. Price also admitted to filming himself sexually abusing the one-year-old son of a neighbor at the motel.

The State charged Price with five counts of first degree child rape, one count of first degree child molestation, three counts of first degree dealing in depictions of a minor engaged in sexual conduct, four counts of sexual exploitation of a minor, and four counts of first degree possession of depictions of a minor engaged in sexually explicit conduct.

Price filed a CrR 3.6 motion to suppress the evidence obtained from Discord and Skype. Price argued that Discord and NCMEC acted as governmental agents, Price had a reasonable expectation of privacy in his computer file storage and images on his computer, and therefore the viewing of files from the CyberTips constituted an unlawful search. The trial court denied the motion to suppress and explained, "State v. Harrier, 14 Wn. App. 2d 17 (2020) is directly on point. Mr. Price has no expectation of privacy in files obtained by a third party and delivered to the police. As a result, the opening and viewing of the files by the police was not unlawful." Clerk's Papers (CP) at 132.

The jury found Price guilty as charged. At the time of sentencing, Price had also been convicted of two counts of "production of child pornography" in federal court but had not yet been sentenced on his federal convictions. CP at 283. The trial court in this case imposed an exceptional sentence of 1306 months and ordered that it run consecutive to the anticipated sentence in Price's federal case. The trial court also imposed various legal financial obligations.

Price timely appeals.

ANALYSIS

I. MOTION TO SUPPRESS

Price argues that the trial court erred by denying his motion to suppress. Specifically, he argues that Discord and NCMEC were agents of the government, and the government's search constituted an unconstitutional trespass or trespass to chattels under the Fourth Amendment. We disagree.

The United States Constitution provides the minimum protection against warrantless searches and seizures by the government. Our state constitution provides greater protection under article I, section 7. *State v. Carter*, 151 Wn.2d 118, 125, 85 P.3d 887 (2004). "Article I, section 7 recognizes privacy interests that Washington citizens have held, and should be entitled to hold, free from governmental intrusion." *Id.* at 126. Generally, a person does not have a privacy interest in what is voluntarily exposed to the public. *Id.* Article 1, section 7 only applies when a person's private affairs are disturbed or their home invaded. *Id.* at 126.

The Fourth Amendment to the federal constitution protects against warrantless searches and seizures. *Id.* at 127. To be a search for purposes of the Fourth Amendment, the person seeking protection must have a justifiable, reasonable, or legitimate expectation of privacy in the

thing examined, and they must establish a subjective expectation of privacy. *Id.* "A subjective expectation of privacy is unlikely to be found where the person asserting the right does not solely control the area or thing being searched." *Id.* There is no Fourth Amendment protection for that which a person knowingly exposes to the public. *Katz v. United States*, 389 U.S. 347, 351, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

As the trial court noted below, this case is nearly identical to *State v. Harrier*, 14 Wn. App. 2d 17, 475 P.3d 212 (2020). There, an ISP discovered digital files and images of suspected child sex abuse using hash value comparison. *Id.* at 20. The ISP reported this information via CyberTip to NCMEC who then forwarded the information to local police for investigation. *Id.* On appeal, Harrier argued that the police conducted an unconstitutional search by opening and viewing the images. *Id.* at 22. We held that Harrier had no privacy interest in the images obtained by the ISP and delivered to the police, and therefore, there was no unlawful search. *Id.* at 19.

There is no factual distinction between this case and *Harrier*. Nonetheless, Price argues that the trial court erred by relying exclusively on *Harrier* without considering his argument that Discord and NCMEC were agents of the government and the government's search constituted an unconstitutional trespass or trespass to chattels under the Fourth Amendment.

"For much of the 20th century, the Supreme Court's 'Fourth Amendment jurisprudence was tied to common-law trespass' and applied only to constitutionally protected areas such as persons, houses, papers, and effects." *State v. Bowman*, 198 Wn.2d 609, 625, 498 P.3d 478 (2021) (quoting *Kyllo v. United States*, 533 U.S. 27, 31, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)). Fourth Amendment jurisprudence shifted with *Katz*, wherein the Supreme Court held that "the Fourth Amendment protects people, not places." *Katz*, 389 U.S. at 351. More recently,

the Court has explained that *Katz* was an expansion of the Fourth Amendment, not a limitation; government conduct can constitute a Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy *or* when it involves a physical trespass on a constitutionally protected space or thing for the purpose of obtaining information. *United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016); *United States v. Jones*, 565 U.S. 400, 409, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012).

To support his contention that Discord's search constituted an unlawful trespass under the Fourth Amendment, Price relies on *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). In *Ackerman*, the 10th Circuit Court extended *Jones*'s trespass test to electronic or digital trespasses for the first time. *Id.* There, AOL, an ISP, intercepted emails sent by Ackerman containing child sexual abuse materials and forwarded a report to NCMEC who opened the emails, viewed the images, and alerted law enforcement. *Id.* at 1294. On appeal, the 10th Circuit Court likened email to physical mail and held that NCMEC's opening of the intercepted email attachments constituted an unlawful search under the Fourth Amendment. *Id.* at 1302.

But Price's reliance on *Ackerman* fails for two reasons. First, whereas *Ackerman* involved the interception of private e-mail correspondence, which is easily analogized to the physical "papers" or "effects" historically protected by the Fourth Amendment, here, Discord's search was of files publicly shared in a chatroom. *Ackerman*, 831 F.3d at 1304. *Ackerman* likened private emails to personal letters traditionally protected under the trespass to chattels theory identified in *Jones*. *Id*. Posting pictures, videos, and messages in a chatroom maintained by a third party is qualitatively different from private correspondence such as emails. Users employ usernames that can be changed or altered by the user at will. At any time, a user could be

communicating with a law enforcement officer or the user's next-door neighbor and they would never know. Price's argument that the files he shared with chatrooms at large constituted his private papers and effects as contemplated by the traditional trespass test in *Jones* is unpersuasive. Price's descriptions of his past sexual abuse activities involving his infant daughter and his planned future child sex abuse in the third-party maintained chatroom was more akin to speaking in a public setting where one can readily be overheard than sending a private letter to a specific individual, the former of which is not protected under the Fourth Amendment. There is no Fourth Amendment protection for that which a person knowingly exposes to the public. *Katz*, 389 U.S. at 351.

Several courts have encountered iterations of this issue and have concluded that users do not have a reasonable expectation of privacy in messages they share publicly in chat rooms. *See*, *e.g.*, *United States v. Morel*, 922 F.3d 1, 9-10 (1st Cir. 2019) (concluding that images uploaded to a website lacked a reasonable expectation of privacy); *United States v. Maxwell*, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (noting that "[m]essages sent to the public at large in [a] 'chat room' lose any semblance of privacy."). As one district court observed in rejecting a claim of Fourth Amendment protection for messages posted in publicly accessible online chat rooms, the defendant "could not have a reasonable expectation of privacy in the chat rooms," because "when Defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent." *United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997). These courts all examined the public nature of chat rooms, including the lack of control over and knowledge of who received the communications. All those same criteria are present in this case.

Second, *Ackerman* concluded that NCMEC was acting as a government entity when it opened Ackerman's emails. In contrast, Discord is not a government entity, and Fourth Amendment protections do not apply to searches by private entities unless that private entity is acting as a government agent. *United States v. Jacobsen*, 466 U.S. 109, 113-15, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984). Price relies on *Ackerman* to support his contention that Discord acted as a government entity, but *Ackerman* did not determine whether the third-party ISP was a governmental agency or actor. *Ackerman*, 831 F.3d at 1308. There, the 10th Circuit raised, but did not decide, the question of whether other doctrines, such as the third party doctrine, might result in denial of the suppression motion based upon the third-party ISPs actions prior to NCMEC. *Ackerman*, 831 F.3d at 1304-05, 1308-09.

Price offers no case holding that a private ISP acts as a government agent under these circumstances—likely because each court that has considered the issue has determined that ISPs are private actors that conduct private searches when they look for or find child abuse or child sexual abuse materials on their servers. *See, e.g., United States v. Coyne*, 387 F. Supp. 3d 387, 396 (D. Vt. 2018) (concluding that neither Microsoft nor Chatstep was a government agent); *United States v. Miller*, 982 F.3d 412, 425-26 (6th Cir. 2020) (holding that Google's use of hash-value matching software to find child sexual abuse materials did not turn its private search into government action); *United States v. Sykes*, 65 F.4th 867, 877 (6th Cir. 2023) (holding that Facebook's search did not constitute governmental action); *United States v. Ringland*, 966 F.3d 731, 736-37 (8th Cir. 2020); *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Bebris*, 4 F.4th 551 (7th Cir. 2021).

And if Discord is not a government entity or agent, even assuming Price had some privacy interest in his chatroom posts of child sexual abuse, then the subsequent viewing by NCMEC and law enforcement was not an unlawful search under the private search doctrine. "Under the private search doctrine a warrantless search by a state actor does not offend the Fourth Amendment if the search does not expand the scope of the private search." *State v. Eisfeldt*, 163 Wn.2d 628, 636, 185 P.3d 580 (2008). The underlying rationale of the private search doctrine is that an individual's reasonable expectation of privacy is destroyed when the private actor conducts his search. *Id.* Thus, where the expectation of privacy has been extinguished by a private actor, a subsequent search by a government entity does not offend the Fourth Amendment so long as the scope of the search is not expanded. *Id.* Price does not argue, and the record does not show, that a government entity expanded the scope of the third-party, private search in this case.

In sum, Price had no reasonable expectation of privacy in his files publicly posted in a third-party chatroom, his files did not amount to personal effects protected by the trespass to chattels theory, and Discord and Skype are not government entities. Accordingly, we hold that the trial court did not err by denying Price's motion to suppress.

II. SENTENCING ERRORS

Price also argues, and the State concedes, that the trial court erred by ordering that Price's sentence run consecutively to his federal sentence that had not yet been imposed and by imposing various legal financial obligations. A trial court "has no authority to determine whether a current sentence shall run consecutively to or concurrently with a sentence yet to be imposed."

In re Pers. Restraint of Long, 117 Wn.2d 292, 305, 815 P.2d 257 (1991). Yet that is what the trial court here attempted to do.

Additionally, because Price was indigent as defined in RCW 10.01.160(3), and his case was pending on appeal when statutory amendments prohibiting the imposition of the \$500 victim penalty assessment on indigent defendants and eliminating the \$100 DNA collection fee went into effect, these legal financial obligations must be stricken from his judgment and sentence. *See State v. Ellis*, 27 Wn. App. 2d 1, 16-17, 530 P.3d 1048 (2023).

CONCLUSION

We affirm Price's convictions but accept the State's concessions and remand to the trial court for correction of the judgment and sentence.

A majority of the panel having determined that this opinion will not be printed in the Washington Appellate Reports, but will be filed for public record in accordance with RCW 2.06.040, it is so ordered.

Che, J.

We concur:

Maxa, P.J.

Price, J.

^{*} Stephen Price bears no relation to Judge Erik Price.