2018 VT 92

No. 2017-127

State of Vermont — Supreme Court

v. — On Appeal from Superior Court, Rutland Unit, Criminal Division

Stuart Lizotte, Jr. — March Term, 2018

Cortland Corsones, J.

Thomas J. Donovan, Jr., Attorney General, and Ultan Doyle, Assistant Attorney General, Montpelier, for Plaintiff-Appellee.

Allison N. Fulcher of Martin & Associates, Barre, for Defendant-Appellant.

Christopher J. Schmidt, St. Louis, Missouri, Logan Rutherford, Kansas City, Missouri, and Lawrence G. Scarborough, New York, New York, of Bryan Cave LLP, for Amicus Curiae The National Center for Missing and Exploited Children.

PRESENT: Reiber, C.J., Skoglund, Robinson, Eaton and Carroll, JJ.

¶ 1. **SKOGLUND, J.** This case requires us to consider whether defendant's Fourth Amendment rights were violated when his online service provider, AOL, searched his transmissions, detected suspected child pornography, and sent information to the National Center for Missing and Exploited Children (NCMEC), which opened the email and attachment and provided it to law enforcement. We conclude that AOL was not acting as an agent of law enforcement when it searched defendant's transmissions, and that NCMEC and law enforcement did not expand AOL's private search by viewing the file already identified by AOL as containing child pornography. In addition, any expansion of the search by opening the related email did not

invalidate the warrant because the other information in the affidavit independently provided probable cause to search. We affirm.

¶ 2. The following facts are not disputed. Defendant registered an account with America Online, now known as AOL, an electronic service provider (ESP) and internet service provider (ISP), which was in effect in March 2013. He registered it under the screenname "lilstuisthebest." This is the account used to send the emails and attachments at the heart of this case. To use AOL's services, AOL requires its users to agree to its Terms of Service and Privacy Policy (TOS). The terms are designed to protect AOL's rights and to control members' behavior online and when using its services. At the time in question, the TOS specifically stated, among other things, that AOL could access the content of communications if it believed a crime had been committed, and that users could not post, transmit, or distribute illegal content. In addition, the TOS explained that if illegal material was posted or transmitted, then AOL would cancel the account and cooperate with law enforcement.

¶ 3. AOL monitors the content users send on its network through tools including Image Detection Filtering Process (IDFP).[1] IDFP uses the MD5 algorithm to compute the hash value of attachments and embedded images in messages sent by, replied to, or forwarded by an AOL user. The MD5 hash values are obtained by applying a mathematical algorithm to a digital file or data set. The resulting hash value is a unique numerical representation of that digital file or data set. Two images that are pixel-for-pixel identical will have the exact same hash value, and therefore, the hash value is referred to as a digital fingerprint. See United States v. Henderson, 595 F.3d 1198, 1199 n.2 (10th Cir. 2010) (explaining that hash value is unique

[1] AOL is not required by law to monitor transmissions by its users for child pornography, but it must report any suspected child pornography if it is discovered. See infra, ¶ 22. AOL began monitoring transmissions in response to complaints from its users, who were receiving child pornography in their email.

alphanumeric sequence developed from pixel-by-pixel analysis of particular image or video and called "digital fingerprint" because it is, "so far as science can ascertain presently, unique").

¶ 4. MD5 hash values are a well-established means of identifying and verifying electronic files. Using the hash algorithm, the scanning system can scan numerous files and identify those files with known hash values. The hash values used to identify images of apparent child pornography within AOL's system are created by AOL. All the hash values contained in AOL's data set were derived from images of apparent child pornography that have at one time been viewed by an AOL Graphics Review Team representative and determined to contain apparent child pornography. If the image is altered in any way, the hash value will not match.

¶ 5. When a file is identified by AOL using IDFP as having the same hash value as a file previously categorized as apparent child pornography, the file does not reach its intended destination, the sender's email account is terminated, the account is preserved, and AOL automatically files a report with NCMEC's CyberTipline. AOL sends a copy of the full email, the header information, and a copy of any image or files attached or embedded in the email. The header information is metadata about the email including routing information. AOL does not necessarily view the flagged file prior to submitting it to NCMEC, relying solely on the identification of the images by the hash value and its previous observation of the image with the same hash value. NCMEC cannot tell whether the file has been opened, but the report transmitted has a place for the ESP to indicate whether the file has previously been viewed.

¶ 6. NCMEC is a private, nonprofit corporation. Its mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC has five main project areas: (1) missing children; (2) child sexual exploitation; (3) training; (4) safety and prevention; and (5) child victim and family services. NCMEC has 350 employees over several different departments and divisions. None of NCMEC's employees are government employees or active law enforcement officers. NCMEC is funded through private donations, federal grants,

foundations, and corporate donations. Approximately seventy percent of its funding, around thirty-four million dollars, comes from federal grants from the Department of Justice and the Department of Homeland Security.

¶ 7. The Child Exploitation Division of NCMEC operates the CyberTipline and a child victim identification program. The child victim identification program uses hash values to identify images that contain child victims. The CyberTipline receives tips related to child exploitation. Reports can be submitted online. The CyberTipline was created through a grant and, at the time, law enforcement did not have any involvement in the program. The government was not involved in initiating the program and no statutes governed its operation. Since then, the federal government has enacted several laws related to the CyberTipline. Currently, federal law requires ESPs and ISPs to report apparent child pornography to NCMEC through the CyberTipline. See 18 U.S.C. § 2258A(a). NCMEC is then required to forward the report to law enforcement. Id. § 2258A(c)(1). Although ISPs and ESPs are not required to register with NCMEC, about twenty-five percent of them are registered, including AOL. Once registered with NCMEC, ESPs provide reports to the CyberTipline using a secure encrypted electronic connection that gives them the ability to upload files with their reports. Of the four million tips to the CyberTipline in 2015, ninety-eight percent were made by ESPs.

¶ 8. After NCMEC receives a report, the report is locked and cannot be altered. A staff member then uses publicly available tools to try to identify potential geographic information pertaining to the individual who is the subject of the report, as well as the geographic information of the ESP potentially used in the possession, receipt, or transmission of the apparent child pornography image files. After the staff member has determined a potential geographic location and the relevant ESP information, a CyberTipline report is made available to a law enforcement agency in the identified potential geographic location using a secured virtual private network. NCMEC is required by federal legislation to transmit or forward the report to the appropriate

law enforcement agency for investigation. See 18 U.S.C. § 2258A(c)(1)-(3) (requiring NCMEC to forward each report "to any appropriate law enforcement agency designated by the Attorney General" and allowing NCMEC to forward report to state law enforcement or foreign law enforcement); 34 U.S.C. § 11293(b)(1)(P) (describing that annual grant to NCMEC should be used to "operate a cyber tipline to provide online users and electronic service providers an effective means of reporting Internet-related child sexual exploitation"). NCMEC staff do not always open and view files before forwarding them to law enforcement. Staff sometimes open images for two reasons: to make sure the file was transmitted properly and to identify the location of the image, and therefore the involved minor, in furtherance of their goal of helping victims.

¶ 9. Law enforcement uses the private network to access and obtain the report. NCMEC neither has control over any subsequent investigation nor does it follow up with law enforcement on any tips that NCMEC sent.

¶ 10. In this case, AOL identified two emails that contained files with hash values matching AOL's database of suspected child pornography. AOL isolated the transmissions and did not allow the emails to be sent to their intended recipient. AOL then submitted two reports to NCMEC labelled as 1812852 and 1812853.[2] AOL reported an individual using an email address of lilstuisthebest@aol.com and provided the associated IP address. AOL identified the incident as child pornography based on its IDFP analysis. The attachment file name was referenced in the header information. The header also contained the MD5 hash value of the file that was sent. Staff at AOL did not view either the content of the two emails or the attachment at the time the report was made. Once received by NCMEC, a staff person at the CyberTipline viewed the video attachment and the opened the email. Using publicly available internet tools, that staff person determined that the IP address identified by AOL was associated with a Comcast

[2] There were two reports because there were two separate emails that attempted to send the same file.

account having a potential geographic location of Rutland, Vermont. Consequently, the CyberTipline sent a notification of reports 1812852 and 1812853 to the Office of the Vermont Attorney General for independent review and potential investigation.

¶ 11. The Attorney General's Office has a unit called Internet Crimes Against Children task force (ICAC). A detective from that unit received an email from NCMEC stating a tip was available. He logged onto the NCMEC virtual private network and downloaded the reports designated as 1812852 and 1812853. The reports indicated that AOL had not viewed the attachment. The detective opened and viewed both the emails and the video attachment. The detective applied for a warrant to search defendant's residence and any electronic devices found therein. The search warrant affidavit included information about NCMEC and the CyberTipline. The affidavit also provided the name of the attached video, a description of the video contents, information about the sender, and content from the emails. A subsequent search warrant was obtained to get information about the AOL account from AOL.

¶ 12. Based on information obtained from these searches, defendant was charged with four counts of possessing child pornography, three counts of promoting child pornography, three counts of aggravated sexual assault, and one count of lewd and lascivious conduct.[3] Defendant moved to suppress. He argued that he had a reasonable expectation of privacy in his emails and related attachments and that his rights under both the Fourth Amendment of the U.S. Constitution and Article 11 of the Vermont Constitution were violated because law enforcement opened the attachment and his email before obtaining a warrant.

¶ 13. The court denied the suppression motion. Based on defendant's agreement to the TOS with AOL, which notified defendant that his communications could be accessed or disclosed if there was a good faith belief a crime had been committed, the court held that

[3] The State amended the information several times, eventually including all of the charges listed.

defendant had no reasonable expectation of privacy in the transmissions involved in this case. With no expectation of privacy, the court concluded there was no violation of defendant's rights.

¶ 14. The court rejected the argument that AOL and NCMEC were acting as agents of law enforcement and therefore that their searches required a warrant. The trial court found the following: that law enforcement was not involved with AOL's process of identifying apparent child pornography and AOL was not working as an agent of same; no law enforcement or government entity was involved in setting up the CyberTipline and law enforcement did not direct NCMEC to establish it; the government neither directs nor provides guidance to NCMEC in its processing of CyberTipline reports; law enforcement is not involved with NCMEC's process of collecting reports; and NCMEC has no control over any subsequent criminal investigation and does not follow up with law enforcement on any tips that are sent. Based on these findings the court concluded that neither AOL nor NCMEC were functioning as agents of law enforcement and their private searches were not precluded by the Fourth Amendment. Finally, the court concluded that, even if NCMEC was a government agent, neither NCMEC nor law enforcement in the form of the detective, expanded the scope of the AOL search.

¶ 15. Defendant then entered a conditional guilty plea, pleading guilty to two counts of aggravated sexual assault, one count of possessing child pornography, and two counts of promoting child pornography. He reserved the right to appeal the denial of his motion to suppress. More information about the plea colloquy is set forth below. After a contested sentencing hearing, defendant was sentenced to twenty-two years to life. Defendant appealed.

¶ 16. On appeal, defendant argues that the motion to suppress should have been granted because the search warrant was based on evidence that was obtained in violation of his Fourth Amendment and Article 11 rights.[4] Defendant also argues that his guilty plea was invalid

[4] Although defendant cites both the Fourth Amendment and Article 11 of the Vermont Constitution, defendant does not provide any argument or rationale to distinguish the analysis under the Vermont Constitution. See State v. Brillon, 2010 VT 25, ¶ 6, 187 Vt. 444, 995 A.2d 557

because the court failed to establish a factual basis for one of the aggravated sexual assault charges.

¶ 17. As explained more fully below, we conclude that AOL was not functioning as an agent of law enforcement when it scanned defendant's transmissions, compared the attached file to its database of hash values, and reported defendant's email and attachment to NCMEC. However, we conclude that NCMEC was functioning as an agent of the government when it opened and processed the material sent by AOL and then transmitted it to law enforcement. We conclude that NCMEC and law enforcement did not expand the search conducted by AOL when they opened the video file because at some time prior AOL had already viewed that document and through the hashing technology law enforcement already knew what was contained therein. To the extent that NCMEC or law enforcement opened and viewed the contents of the email itself, we conclude that this was an expansion of the search conducted by AOL. We hold, however, that because the information from the content of the email was not necessary to provide probable cause, this expansion did not invalidate the warrant. Finally, we conclude that the plea colloquy was sufficient.

I. Reasonable Expectation of Privacy

¶ 18. On appeal, defendant first argues that he had a reasonable expectation of privacy in the content data associated with his emails that is protected by the Fourth Amendment and Article 11 of the Vermont Constitution.[5] Defendant also contends that any consent he gave to

(concluding state constitutional argument not adequately presented where there was no substantive analysis of how state provision differed from federal provision). Therefore, we analyze the issues under the existing federal standard. We do not address defendant's state constitutional arguments that are raised for the first time in his reply brief. See State v. Percy, 156 Vt. 468, 481 n.7, 595 A.2d 248, 255 n.7 (1990) (refusing to address constitutional argument raised for first time in reply brief).

[5] Defendant does not argue that he had a reasonable expectation of privacy in the noncontent data associated with the email such as the subscriber information and associated IP address. See State v. Simmons, 2011 VT 69, ¶¶ 13-14, 190 Vt. 141, 27 A.3d 1065 (recognizing

AOL by agreeing to the TOS did not diminish his expectation of privacy under the Fourth Amendment. For purposes of this decision, we assume that defendant had a reasonable expectation of privacy in the content of his email communication, including images attached or embedded in those emails.[6] Because we conclude that AOL was not functioning as an agent of law enforcement, we need not and do not reach the question of whether by accepting AOL's TOS defendant consented to the search of his transmissions by AOL.

II. Agents of Law Enforcement

¶ 19. The U.S. Supreme Court has long held that "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." Walter v. United States, 447 U.S. 649, 656 (1980). The Fourth Amendment and the exclusionary rule apply solely to government action because the constitutional provision safeguards "against arbitrary invasions by governmental officials." State v. Schofner, 174 Vt. 430, 431-32, 800 A.2d 1072, 1074 (2002) (mem.) (quotation omitted). In addition, the purpose of the exclusionary rule—to deter unconstitutional conduct—"would have little effect on a private person who is not acting to secure a criminal conviction." State v. Young, 2010 VT 97, ¶ 12, 189 Vt. 37, 12 A.3d 510.

¶ 20. Nonetheless, a private search will implicate the Fourth Amendment if the private party is acting as an agent of the government. United States v. Cameron, 699 F.3d 621, 637 (1st Cir. 2012). There is no specific test to measure whether such an agency relationship exists. The

---

that federal courts have held that Fourth Amendment does not protect noncontent data and holding that subscriber information is not private under Article 11).

[6] The State moved to strike a portion of defendant's appellant reply brief, arguing that defendant improperly raised new arguments to support his assertion that he had a reasonable expectation of privacy in the content data of his emails. Because we assume that defendant had a reasonable expectation of privacy in his emails, we need not reach the arguments advanced in defendant's reply brief and deny the motion as moot.

U.S. Supreme Court has explained that whether a private party acted as an instrument of the government "necessarily turns on the degree of the Government's participation in the private party's activities." Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989). This depends on the circumstances, including the government's "encouragement, endorsement, and participation" in the action. Id. at 615-16; see Young, 2010 VT 97, ¶ 14 (looking at "all the circumstances of the case" to determine if off-duty police officer was acting as private citizen during search). In general, "[a] search by a private person becomes a government search if the government coerces, dominates, or directs the actions of a private person conducting the search." United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) (quotation omitted).

¶ 21. Some federal courts have established factors to be considered in determining whether a private citizen acted as an agent of the government in conducting a search. The First Circuit looks at three factors: "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests." United States v. Momoh, 427 F.3d 137, 141 (1st Cir. 2005) (quotation omitted). The Tenth Circuit has a two-part inquiry: "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends." Souza, 223 F.3d at 1201 (quotation omitted). The Sixth and Ninth Circuits also look at two factors: " '(1) the government's knowledge or acquiescence, and (2) the intent of the party performing the search.' " United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008) (quoting United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981)). In all the tests, the critical facts are the government role in the private party's action and the private party's motivation for conducting the search. In addition, the defendant bears the burden of establishing that a private party acted as an agent of the government. United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) ("The defendant shoulders the burden of

establishing the existence of an agency relationship—a fact-intensive inquiry that is guided by common law agency principles." (quotation omitted)). We apply these considerations in turn to both AOL and NCMEC.

A. AOL

¶ 22. In considering the tests enunciated above, we conclude that AOL was not acting as a government agent when it searched defendant's transmissions over its network using its hashing technology. The facts presented as to AOL are as follows. Law enforcement is not involved in the daily operations of AOL. The law requires AOL to report suspected violations of federal law prohibiting sexual exploitation of children, but does not require AOL to monitor transmissions over its network to detect illegal action. See 18 U.S.C. § 2258A(a) (requiring ESP to report suspected child pornography); id. § 2258A(f)(1)-(2) (explaining that statute should not be construed to require ESP to "monitor any user, subscriber, or customer" or to "monitor the content of any communication"). IDFP, AOL's technology for identifying suspected child pornography, was developed independent of any government agency, and the government did not require its development. AOL developed the IDFP technology on its own to further private business concerns including the issue that its users were complaining about receiving images of child pornography.

¶ 23. Under these circumstances, we conclude that AOL was not acting as a government agent when it searched the transmissions defendant sent over its network using its hashing technology. AOL monitored defendant's transmissions based on its business interest, not because it was encouraged or directed to by government, and the government did not know about or participate in the action. This holding is consistent with the decisions of other courts that ISPs do not act as agents of law enforcement by monitoring the content of transmissions for suspected child pornography. See United States v. Stevenson, 727 F.3d 826, 831 (8th Cir. 2013) (holding that AOL searching email for child pornography was based on its own initiative not as

government agent); Cameron, 699 F.3d at 637-38 (concluding Yahoo! not acting as government agent when searching for child pornography because it did so for its own interests and government did not control or direct action); Richardson, 607 F.3d at 365-67 (holding AOL not acting as agent of government when it scanned email for suspected child pornography); United States v. Stratton, 229 F. Supp. 3d 1230, 1237-38 (D. Kan. 2017) (holding that electronic service provider was acting as private entity when it searched content of defendant's online gaming).

B. NCMEC

¶ 24. Defendant argues that NCMEC was acting as an agent of law enforcement when it opened his email and the related attachment. We agree.[7]

¶ 25. We first look at whether the government instigated, encouraged, or participated in the search. ESPs and ISPs are required by statute to report suspected child pornography and NCMEC's CypberTipline is the sole means to do so. NCMEC is required by statute to preserve the evidence and to forward the CyberTipline reports to law enforcement. Therefore, the government knew that NCMEC would be collecting reports of suspected child pornography and in fact through legislation directed NCMEC to do so. Although the statute does not require NCMEC to open the information in the reports, it does not preclude NCMEC from viewing the contents of the reports. The statute at least indicates that the government knew it was likely NCMEC would view and search the reports and at least acquiesced in this action. Further, NCMEC is treated like an arm of the government in that it is authorized to receive and possess child pornography, which is otherwise contraband. Moreover, the statute requires NCMEC to preserve the evidence and forward the information to law enforcement. These facts show

[7] The undisputed facts indicate that NCMEC is largely funded by government grants and that law enforcement officers serve on its board. Although these facts would be important to a determination of whether NCMEC is a government entity, they are not particularly relevant to the question of whether NCMEC was acting as a government agent when it opened and searched the email and attachment received from AOL. The latter issue instead depends on the government's role in instigating or participating in the search and its control over the search, and the private party's purpose for conducting the search.

government involvement in NCMEC's search: government knew NCMEC would be conducting searches like the one at issue here, provided direction on how the information would be treated, and mandated that the information obtained be shared with the government.

¶ 26. The other important consideration is NCMEC's motivation for opening the email and the attachment. The State argues that NCMEC was not acting as an agent of law enforcement because it was motivated by its private goals of helping to find missing children, reducing sexual exploitation of children, and preventing child victimization. The State relies on People v. Pierre, 29 N.Y.S.3d 110, 120 (Sup. Ct. 2016), which held that NCMEC was not acting as an agent of law enforcement because it had its own legitimate interests and motivation for creating the CyberTipline. Pierre in turn relied in large part on a similar holding in United States v. Ackerman, No. 13-10176-01-EFM, 2014 WL 2968164 (D. Kan. July 1, 2014), which was subsequently overruled. On appeal, the Tenth Circuit held that NCMEC was acting as agent of law enforcement because the government knew and acquiesced in its searches and NCMEC was motivated at least in part by a desire to assist law enforcement. United States v. Ackerman, 831 F.3d 1292, 1301-02 (10th Cir. 2016); see also United States v. Keith, 980 F. Supp. 2d 33, 41 (D. Mass. 2013) (concluding that NCMEC's operation of CyberTipline "is intended to, and does, serve the public interest in crime prevention and prosecution, rather than a private interest"). We acknowledge that NCMEC created the CyberTipline on its own initiative and not at government's direction and that NCMEC has important goals unrelated to law enforcement. Nonetheless, when NCMEC searched defendant's transmissions, it was doing so at least in part to assist law enforcement. The testimony indicated that NCMEC had independent reasons, including identifying victims, to view the images and the email, but it also sought to locate the sender of the transmission to aid law enforcement. We conclude that the combination of the government's knowledge and acquiescence in the search and the motive of NCMEC to assist law enforcement indicate that NCMEC was acting as an agent of the government when it opened

and viewed defendant's email and video attachment. See Ackerman, 831 F.3d at 1301-02 (concluding that NCMEC was acting as agent of law enforcement).

III. Expansion of Search

¶ 27. Next, we turn to the question of whether the searches performed by NCMEC and law enforcement expanded on that performed by AOL because under the private search doctrine there is no violation of the Fourth Amendment if the police view evidence that is confined to the scope of the initial private search.

¶ 28. The private search doctrine was examined by the U.S. Supreme Court in United States v. Jacobsen, 466 U.S. 109 (1984). In that case a package arrived a Federal Express office damaged and torn. Employees opened the package to examine the contents. Inside, they found a box with a tube covered with silver tape. The employees cut the tube and found a series of plastic bags containing white powder. They notified the Drug Enforcement Administration. When federal agents arrived, an agent removed a plastic bag from the tube and opened four bags to remove the white substance. The federal agents tested the substance and identified it as cocaine.

¶ 29. The search was challenged by the defendant. The U.S. Supreme Court explained that the initial invasion was done by private action and the question was whether the additional invasions of privacy by the government "exceeded the scope of the private search." Id. at 115. The Court held that the Fourth Amendment does not prohibit the use of information obtained in a third-party search, but it is implicated if the government "use[s] information with respect to which the expectation of privacy has not already been frustrated." Id. at 117. The Court concluded that there was no expansion of the private search when DEA officers removed the plastic bags from the tube and powder from the bag because "the removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search." Id. at 120. The Court

also held that field testing the substance did not violate the Fourth Amendment because this action could only reveal whether the substance was cocaine, which did not compromise a legitimate interest in privacy and therefore was not a search. Id. at 122-23.

¶ 30. The question is then whether opening (1) the attachment and (2) the email to which it was attached provided an opportunity for the government to learn something that had not already been discovered during the private search. See United States v. Lichtenberger, 786 F.3d 478, 485-86 (6th Cir. 2015) (explaining that there is no expansion of search where government has "near-certainty regarding what they would find and little chance to see much other than contraband").

¶ 31. The facts relevant to the attached file are as follows. The file was identified by AOL as having a MD5 hash value matching an image that had previously been opened and identified by an AOL representative as child pornography. AOL did not need to open the attachment at the time that it was detected to know what it contained because each hash value is unique and AOL knew that the match indicated the image contained previously viewed child pornography. Therefore, when AOL sent the report to NCMEC with the hash value, NCMEC knew for certain that the image was (1) one that had been previously viewed by AOL; and (2) an image that contained apparent child pornography. Like in Jacobsen where law enforcement did not expand the search by looking in the plastic bag, when NCMEC and then law enforcement opened the attachment forwarded by AOL, they were not expanding AOL's search because they already knew what was contained in the attachment and they could not learn more than was already known by AOL about the attachment. Therefore, we hold that viewing the attachment did not expand the search. A federal district court reached the same result on similar facts, explaining that a hash value is not like a label written on a box; rather, it is a digital fingerprint that conveys that the information in the file is exactly the same as what was previously viewed. See United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *5-6 (E.D. Ky. June 23,

2017) (holding that law enforcement did not expand search by opening file that Google had previously identified as apparent child pornography and matched using hashing technology).

¶ 32. Defendant argues that NCMEC and law enforcement expanded on the search conducted by AOL when they opened the email and the attachment because AOL did not open either prior to transmitting to NCMEC. Defendant relies primarily on two cases. In Ackerman, using its hashing technology, AOL identified one of four images attached to the defendant's emails as child pornography. AOL forwarded the email and all of the images to NCMEC, which opened the email and viewed all of the images. NCMEC then alerted law enforcement. The court held that NCMEC was acting as a government agent. 831 F.3d at 1301-04. The court further held that NCMEC expanded the private search when it opened the three unidentified attachments and the email itself because these items could have disclosed information "previously unknown to the government." Id. at 1306.

¶ 33. We are not persuaded that Ackerman supports a holding that there was an expansion of the search in this case as to the video file. The facts are distinguishable because in Ackerman there were attachments that had not been previously viewed by AOL and identified as suspected child pornography. Moreover, Ackerman did not answer the question of whether simply opening the one identified attachment, and not the email, would have expanded the search. The court specifically reserved that question. Id. (explaining that court did not have to reach question of whether only opening one image with matching hash value and not email would have been an expansion of search).

¶ 34. Defendant also relies on Keith, 980 F. Supp. 2d 33, in which AOL, using its hashing technology, identified an email containing an image that matched a hash value for an image containing child pornography. AOL forwarded it to NCMEC without opening or viewing it. In that case, there was no information about how the file originally was added to AOL's database; the evidence did not indicate whether the image had been viewed by an AOL employee

who placed it in the database or whether the image had been received by AOL from a different ESP and then placed in the database. Based on these facts, the court concluded that when NCMEC viewed the file it expanded the search because all that was shown was that the identified file's hash value matched that of an image in AOL's database and there was no evidence that "some AOL employee had opened the file and viewed the contents." Id. at 43. Here, in contrast, the undisputed evidence established that an AOL employee had previously viewed the image that was identified by the hashing technology. Therefore, we conclude that there was no expansion of AOL's private search when NCMEC and law enforcement viewed the video file that was identified by AOL.

¶ 35. Having analyzed the attachment, we consider whether NCMEC and law enforcement expanded AOL's search by opening the email. AOL did not open the email and had no knowledge of what was contained in that email. Although the trial court did not make specific findings on whether NCMEC and law enforcement opened the email file or just the video attachment, it is clear from the record that both NCMEC and law enforcement viewed the contents of the email to which the identified video file was attached.[8]

¶ 36. The logic underlying our conclusion that opening the video attachment did not expand the search is not applicable to the contents of the email to which the video was attached. AOL had previously viewed the video attachment and therefore when it was viewed by NCMEC and law enforcement, they already knew what it contained and could learn nothing more than had previously been learned through the private search. As to the email contents, however, AOL had no knowledge and this search could have disclosed information previously unknown to the government. See Ackerman, 831 F.3d at 1305-06 (holding that where government opened email

[8] The undisputed evidence demonstrates that law enforcement viewed the email insofar as the investigating detective admitted to opening the email and the affidavit of probable cause supporting the warrant contained text from the body of the email. On appeal, in its amicus brief, NCMEC also admits to opening the email.

itself this amounted to expansion of private search that had only opened attachment to email); see also Jacobsen, 466 U.S. at 120-21 (explaining that expansion of private search occurs where government may learn information not previously revealed during private search). Therefore, we conclude that this expanded the private search conducted by AOL.

¶ 37. There are, however, no grounds to invalidate the resulting warrant because, even without the information from the content of the email, the affidavit in support of the warrant established probable cause. "A search warrant is not invalid merely because it is supported in part by an affidavit containing unlawfully obtained information." State v. Moran, 141 Vt. 10, 16, 444 A.2d 879, 882 (1982). "Where the affidavit includes allegations based on illegally obtained evidence as well as independent and lawfully obtained information, a valid search warrant may issue if the lawfully obtained information, considered by itself, is sufficient to establish probable cause." Id. In prior cases, we have made this determination for the first time on appeal instead of remanding to the trial court. See State v. Morris, 165 Vt. 111, 129, 680 A.2d 90, 102 (1996) (recognizing that "it is not normally the function of appellate review to make a de novo determination of probable cause," but in accordance with prior law determining on appeal whether after excluding some information from affidavit "remaining information contained in the excised affidavit established probable cause for issuance of the warrant").

¶ 38. Therefore, we consider whether there was probable cause. A warrant must be supported by probable cause, which "exists when the facts and circumstances set forth in the affidavit are such that a judicial officer may reasonably conclude that the evidence sought is connected to the crime and located at the place indicated." Moran, 141 Vt. at 16, 444 A.2d at 882. The affidavit of probable cause in this case contained a detailed explanation of the investigation. It provided, among other things, the following: information about the CyberTipline and the reports made by AOL and NCMEC; the name of the video attachment; a detailed description of the video contents, including that it showed girls between six and eight

years old engaged in sexual acts; the sender email and associated IP address; information linking that IP address to Rutland; information from the internet provider that the IP address was assigned to someone with defendant's name; a visual description of the place to be searched including that the mailbox bore defendant's name; and an explanation that both the Department of Motor Vehicles and law enforcement records indicated that defendant lived at that address. This information was sufficient for a judicial officer to reasonably conclude that evidence of child pornography would be found at that location. In addition to the above, the affidavit reports content from that the email containing the suspected child pornography. It states that the identified attachment was part of series of emails in which the recipient writes "im waiting for you to send me back plz" and defendant's email replies "i did." We conclude that the supporting affidavit, absent this very limited information from the body of the email, established probable cause. Therefore, there are no grounds to invalidate the warrant, and we affirm the court's decision denying defendant's motion to suppress.

IV. Plea Colloquy

¶ 39. On appeal, defendant argues that as to Count 6 the plea colloquy was insufficient. Count 6 alleged that defendant committed aggravated sexual assault based on the victim being under the age of thirteen, 13 V.S.A. § 3253(a)(8). Defendant contends that under Vermont Rule of Criminal Procedure 11(f), defendant must personally admit the facts underlying the charge and in this case he simply agreed that the facts recited were alleged by the State, not that he admitted those facts.

¶ 40. Before turning to defendant's substantive argument, we address the State's argument that we should not review defendant's claim because it was unpreserved and therefore subject to plain-error review, but defendant has not argued plain error on appeal. We agree that defendant did not raise this objection below and therefore it is technically subject to plain-error review. We recently held that although Rule 11(f) challenges on direct appeal are reviewed for

plain error, our standard for reviewing these claims on direct appeal is the same as that for collateral challenges. See State v. Bowen, 2018 VT 87, ¶ 10, __ Vt. __, __ A.3d __. In other words, in Rule 11(f) direct-appeal challenges, the defendant need not demonstrate the typical plain-error elements. Therefore, in this case, even though on appeal defendant did not mention plain error or demonstrate its elements, those elements are not relevant to his particular claim. He has argued the standard that applies to his argument and therefore we address it.

¶ 41. Rule 11(f) requires the court to make "inquiry as shall satisfy it that there is a factual basis for the plea." V.R.Cr.P. 11(f). To satisfy this requirement, there must be "some recitation on the record of the facts underlying the charge and some admission by the defendant to those facts." In re Bridger, 2017 VT 79, ¶ 21, __ Vt. __, 176 A.3d 489. The inquiry need not be made in a particular fashion; it must demonstrate "the defendant's admission to the facts as they relate to the law for all elements of the charges." Id. (quotation and alteration omitted). We conclude that the colloquy in this case sufficed.

¶ 42. At the change-of-plea hearing, the court had the following exchange with defendant.

> THE COURT: And the nature of the allegations in Count VI are that between 2010 and August of 2013, Stuart Lizotte, Jr., of Rutland, at Rutland, was a person who was at least eighteen years of age and engaged in a nonconsensual sexual act with a child under the age of thirteen, specifically, on several occasions he made contact with his mouth and the penis of J.W., a child under thirteen years of age, in violation of 13 V.S.A. § 3253(a)(8). Do you understand that's the nature of the allegations against you?
>
> THE DEFENDANT: I do, Your Honor.
>
> THE COURT: Okay. I'm going to ask the State to state the factual basis, and I'm going to ask you listen carefully to the factual basis, Mr. Lizotte, because I'm going to ask if you agree with those facts after the State is done.

The prosecution provided a detailed account of the facts underlying the charge of aggravated sexual assault. The court then asked defendant "do you agree with those facts?" and defendant answered "I do, Your Honor."

¶ 43. We conclude that this colloquy was sufficient to satisfy Rule 11(f). The court explained to defendant that the State was going to recite the facts underlying the charge and then defendant would have an opportunity to indicate if he agreed with the facts. After the State's recitation of the facts supporting all elements of the charge, defendant indicated that he agreed with those facts. This is unlike other cases where we have found noncompliance with Rule 11(f) because the colloquy simply asked the defendant whether he agreed that the charging affidavits provided a factual basis for the charges. See, e.g., Bridger, 2017 VT 79, ¶ 4 (reciting colloquy that asked defendant if he agreed that affidavit provided factual basis). Here, rather than just asking vaguely whether defendant agreed that the affidavit demonstrated a factual basis or that the State had alleged facts to support the charge, the State recited the factual basis and defendant specifically stated he agreed with those underying facts. We therefore affirm.

Affirmed.

FOR THE COURT:

Associate Justice