Filed 9/8/22

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

THE PEOPLE, Plaintiff and Respondent, v. JEFFREY LEE ROWLAND, Defendant and Appellant.	H048799 (Santa Clara County Super. Ct. No. B1901606)

We consider in this appeal the presumptive reliability of information from a third-party electronic communication service provider in an affidavit supporting the application for a search warrant for child pornography.

Defendant Jeffrey Lee Rowland pleaded no contest to possession of child pornography (Pen. Code, § 311.11, subd. (a)[1]) in exchange for two years' formal probation with conditions, including serving nine months in the county jail. Before Rowland entered his no contest plea, the trial court had denied his motion to quash a search warrant that led to the seizure of his child pornography.

On appeal, Rowland claims that the search warrant was not supported by probable cause and the good faith exception to the exclusionary rule does not apply. Additionally, Rowland and the Attorney General agree that any unpaid balance of a criminal justice

[1] Unspecified statutory references are to the Penal Code.

administration fee and probation supervision fee imposed at sentencing should be vacated.

For the reasons explained below, we reject Rowland's challenge to the search warrant. We decide, inter alia, that although the search warrant affidavit did not name the employee who submitted two child pornography cybertips to the National Center for Missing and Exploited Children (NCMEC) or the person who forwarded the cybertips from NCMEC to the police, the totality of the circumstances supported a determination that the cybertips came from unbiased citizen informants who could be presumed reliable and thus did not need any independent corroboration. In addition, we modify the judgment to vacate the unpaid portion of the criminal justice administration fee and probation supervision fee and affirm the judgment in all other respects.

I. FACTS AND PROCEDURAL BACKGROUND

A. *Procedural History*

On April 16, 2019, the Santa Clara County District Attorney filed a complaint charging Rowland with a single count of possessing or controlling matter depicting a person under 18 years of age personally engaging in or simulating sexual conduct (§ 311.11, subd. (a); count 1).

In September 2019, Rowland filed a motion under section 1538.5 to quash the search warrant (motion) that led to a search of his residence and seizure of his electronic devices, including a "PNY Thumb Drive."

The district attorney opposed Rowland's motion. In his opposition, the district attorney noted that the PNY thumb drive "contained an estimated 1,000 images of child pornography and 25 videos of child pornography."

On November 15, 2019, the trial court heard argument from the parties and denied Rowland's motion.

In December 2020, after the trial court indicated a sentence, Rowland pleaded no contest to count 1 as charged.

On January 7, 2021, the trial court suspended imposition of sentence and placed Rowland on formal probation for two years with various conditions, including serving nine months in the county jail. Additionally, the court ordered Rowland to pay various fees including a $129.75 criminal justice administration fee to the City of Los Altos (former Gov. Code, § 29550 et seq.) and a probation supervision fee of $50 per month (former § 1203.1b).

Rowland timely appealed from the denial of his motion to quash the search warrant and his "sentence or other matters occurring after the plea that do not affect the validity of the plea."

B. *Background on the Search Warrant, Seizure of Evidence, and Motion to Quash*

1. Search Warrant Affidavit and Statement of Probable Cause

On February 22, 2019, Los Altos Police Department Detective Edgar Nava authored an affidavit and accompanying statement of probable cause (jointly, the search warrant affidavit or affidavit) in support of a search warrant for Rowland's residence and two vehicles. In the statement of probable cause, Detective Nava said he had been a peace officer for over nine years and that, as a detective, his duties included investigating child exploitation crimes. Regarding his prior training, Nava stated that in 2018 he had "attended a Child Exploitation Investigation Class that reviewed child pornography, child predators, legal aspects and investigative guidelines." He also had "attended classes and seminars, including the Digital Online Safety Class, taught by Verizon Media, [and] Continuous Professional Training (C.P.T.), regarding the investigation of the cases within the aforementioned realm" of child exploitation. Although Nava had previously "investigated crimes against children, this [case was his] first investigation dealing with the crime of possessing child pornography."

Detective Nava explained that, based on his training and experience, he knew "there are suspects who sexually objectify children." Nava described how these suspects "receive sexual gratification and satisfaction from . . . fantasy involving the use of

images, videos, electronic media, and/or writings on or about sexual activity with children." Nava explained further that "[t]hese suspects will often collect and possess sexually explicit objects such as . . . digital files (such as images or videos) which depict children or other young persons. Suspects who possess child pornography tend to collect it." Such suspects also commonly use "Internet searches" and "file sharing networks and programs" to obtain child pornography. "Because child pornography is illegal and not easily available," suspects/child predators tend "to save or retain the child pornography," "rarely, if ever, dispose of their sexually explicit materials," and "will treat their materials as prized possessions, causing collections to typically grow and leading to an obsession."

Additionally, Detective Nava explained that "[s]uspects will typically store child pornography and other sexually explicit material involving children in physical locations, such as a house or vehicle, or on their persons, or retain digital copies on electronic/digital storage devices." "Suspects who sexually objectify minors typically utilize electronic communication providers in an attempt to contact children via the internet or mobile applications for the purposes of sexual gratification." The suspects might "maintain contact information for their victims," "collect and maintain photographs or videos of children they are or have been involved with," "engage in activities or programs which will be of interest to the type of child victims they desire to attract," "collect, read, copy or maintain names, addresses, phone numbers or lists of persons who have similar sexual interests," "correspond via mail, e-mail, instant messages, or in person to share information about their exploits of children and/or the identities of their victims," and "exchange, trade, or sell photos and/or videos of child pornography with other persons with similar interests." "Such suspects go to great lengths to conceal and to protect their collections of illicit materials from discovery, theft, and damage." Furthermore, "deleted [digital] files can typically be recovered using forensic software."

Regarding his current investigation, Detective Nava stated that he was assigned to investigate a report about child pornography from Mountain View Police Department Sergeant Dahl—a member of the Silicon Valley Internet Crimes Against Children (SVICAC) Task Force. Dahl's "report indicated he investigated two 'Cybertips' of exploited children. The Cybertips were received from the [NCMEC], Cybertip 1 (#41968669) and Cybertip 2 (#42488363). NCMEC received the anonymous Cybertips from a Microsoft Online Operation employee who viewed both files" of apparent child pornography. "Both files were uploaded to the internet through the BingImage application from the IP address 108.90.42.164."[2] Nava stated the file name for each image attached to the cybertips, along with the date and time the two files were uploaded (i.e., October 11, 2018, at 10:08:56 UTC (Coordinated Universal Time) for Cybertip 1, and October 26, 2018, at 20:46:56 UTC for Cybertip 2).

Detective Nava stated that "[Sergeant] Dahl reviewed the images and confirmed both images appeared to be images of child pornography. He contacted Alexandra N[.] Gatlin, who is an Analyst 1 with the Child Victim Identification Program (CVIP). Gatlin confirmed via email to [Sergeant] Dahl that the person from Cybertip 1 had been identified and was confirmed to be underage at the time the photograph was taken. In a separate email, Gatlin informed [Sergeant] Dahl that the person in Cybertip 2 had not been identified." Dahl checked the IP address attached to the cybertips against "the American Registry of Internet Numbers (ARIN) and learned the IP address is assigned to a company named AT&T Mobility" (bolding omitted). On November 27, 2018, Dahl authored a search warrant for the subscriber information regarding the "IP address and

[2] " '[A]n IP address . . . is a unique number identifying the location of an end[-] user's computer. When an end-user logs onto a[n] internet service provider, the user is assigned a unique IP number that will be used for that entire . . . session. Only one computer can use a particular IP address at any specific date and time.' " (*People v. Evensen* (2016) 4 Cal.App.5th 1020, 1022, fn. 1; see also *People v. Nguyen* (2017) 12 Cal.App.5th 574, 577.)

learned the subscriber information was Richard Rowland," with an address in Los Altos, California (hereafter residence).

On January 15, 2019, Detective Nava met with Sergeant Dahl at the Mountain View Police Department and viewed "both images of child pornography associated with Cybertip 1 and Cybertip 2." Nava described the images in his statement of probable cause as follows. The image associated to Cybertip 1 "showed a fully nude female juvenile. The female sat in a bathtub that was partially filled with water. She sat with her legs spread open, exposing her vaginal area. The female was leaning back and was smiling for the camera. She had little to no breast development, was small in stature and appeared to be in the early stages of pubic hair growth." The image associated to Cybertip 2 "showed a fully nude female juvenile who seemed to be standing in a bathtub. The female juvenile had both hands above her vagina area and appeared to be spreading her vagina. The female juvenile had no breast development and was positioned with her head [] facing downward. The female was very small in stature and had no pubic hair." Nava stated his belief that the females depicted in each photo were, respectively, "between the ages of 10 to 13 years old" and "7 to 9 years old." Further, Nava said that, based on his training and experience, he believed each child "was positioned in [a] manner to expose the female juvenile's vagina for the sexual gratification of the viewer."

On January 17, 2019, Detective Nava conducted surveillance of the residence in Los Altos, approached it, and using a cell phone, "noticed the only unsecured Wi-Fi signal was a signal named 'xfinitywifi.' " On February 22, 2019, Los Altos Police Department detectives conducted additional surveillance and obtained photographs of the front of the residence. "An Accurint check of the residence revealed two possible residents, Richard Rowland (84 years old) and Jeffrey Rowland (37 years old). Both residents ha[d] valid drivers' licenses and vehicles registered to them," namely a 2011 Audi for Richard Rowland and a 2016 Jeep for Jeffrey Rowland.

Detective Nava asserted that, based on the facts provided, he had "reasonable cause to believe, and d[id] believe, that evidence of the commission[] of felonies, to wit: violation(s) of [section] 311.11[, subdivision] (a) – Possession of Child Pornography, and property documenting commission of said felonies, will be located on the premises described above." Detective Nava "request[ed] that a daytime search warrant be issued."

On February 22, 2019 (the same day that Detective Nava signed the affidavit), based on the information in Nava's affidavit, a judge of the Santa Clara County Superior Court found probable cause and issued a search warrant for the residence, the 2011 Audi, and the 2016 Jeep for "evidence and instrumentalities of possession of child pornography . . . occurring from January 1, 2000 to present."

2. Seizure of Evidence from Rowland's Residence

Five days after the search warrant issued, on February 27, 2019, police officers executed the warrant and seized the following items: Two Western Digital storage devices, a Dell tower computer, a PNY thumb drive, an Apple iPhone, an Apple laptop, and an Apple computer. The PNY thumb drive "contained an estimated 1,000 images of child pornography and 25 videos of child pornography."

3. Rowland's Motion to Quash

In his motion to quash the search warrant, Rowland claimed that the search warrant affidavit failed to state probable cause. He argued the showing was defective because: (1) "The only information in the affidavit linking the contraband to defendant is based entirely on an uncorroborated anonymous tip." (2) "The two images at issue that the affiant identifies as child pornography that form the basis of the search do not show minors engaged in sex acts. The affidavit merely describes two underage females sitting or standing in bathtubs with their legs spread displaying their vaginas. It is not possible to tell from affiant's description whether the two images are child pornography." (3) "The information linking the images to defendant's address was four months old, rendering it stale." Rowland further asserted that "the search warrant affidavit, on its

face, is so lacking in probable cause that it cannot even meet the minimum standards of the 'good faith' rule." Rowland urged the trial court to quash the search warrant and suppress the evidence seized, as well as any "statements and derivative evidence."

In opposition to the motion, the prosecutor contended that probable cause supported the warrant. The prosecutor urged the trial court to consider the tips from Microsoft as a report from a concerned citizen rather than an anonymous tipster. The prosecutor asserted further that Detective Nava's descriptions of the two images provided sufficient basis to conclude the images were child pornography and the magistrate was not obligated to personally view the images. The prosecutor also argued that the information supporting probable cause was not stale. Additionally, the prosecutor maintained that, even if probable cause did not support the issuance of the search warrant, the seized evidence should not be suppressed because it is "saved by the good faith rule."

On November 15, 2019, the trial court heard oral argument on Rowland's motion.[3] The court began the proceeding by providing its tentative ruling to the parties. The court explained, "Based on the affidavit by the officer, I found there was more than a fair probability that evidence of a crime would be found in executing that warrant. [¶] I found that the tips and tipster described . . . were best seen as information from a citizen observing a crime rather than a so-called common informant." The court acknowledged the existence of case law related to that issue and stated, "I thought that there was indicia of enough [] trustworthiness based on what I read . . . in the affidavit to reach that conclusion." Furthermore, the court stated that it did not find the information in the affidavit to be stale because there was no "common sense reason to believe that child porn[ography] at a search site would be gone in less than four months between the download date and the application for the search warrant." Based on Detective Nava's descriptions of the two images, the court "conclude[d] there was probable cause to

[3] The judge who ruled on the motion is the same bench officer who had previously signed the search warrant.

believe that those images were child pornography." The court "didn't think it was necessary for [it] to . . . actually view the images to reach that conclusion."

The trial court found unpersuasive Rowland's argument that the affidavit was deficient because it did not state that the police knew the identity of the informant as allegedly required by the "citizen informant exception." The court explained, "I thought there was enough there, a description. I'm not sure that it would really move the ball forward in this case to have a particular name, given the route that it had -- and I don't know that that would really give the court any better information to be able to assess reliability and credibility."

II. DISCUSSION

A. *Search Warrant*

Rowland contends the trial court erred by denying his motion to quash the search warrant because: (1) the only information in the affidavit linking the alleged child pornography to Rowland's residence came from an uncorroborated "anonymous tipster," which is insufficient to provide probable cause; (2) Detective Nava's description of the two images was too vague for the magistrate to conclude that they were child pornography; (3) the information supporting the warrant was too stale to establish probable cause; and (4) the good faith exception to the exclusionary rule does not apply.

1. Relevant Legal Principles

" 'The standard of appellate review of a trial court's ruling on a motion to suppress is well established. We defer to the trial court's factual findings, express or implied, where supported by substantial evidence. In determining whether, on the facts so found, the search or seizure was reasonable under the Fourth Amendment, we exercise our independent judgment.' " (*People v. Redd* (2010) 48 Cal.4th 691, 719.)

A defendant may move to suppress evidence on the ground that a search or seizure with a warrant was unreasonable for various reasons. (See § 1538.5, subd. (a)(1)(B)(i)–

(v).[4]) " 'In California, issues relating to the suppression of evidence derived from governmental searches and seizures are reviewed under federal constitutional standards.' " (*People v. Macabeo* (2016) 1 Cal.5th 1206, 1212.)

"The pertinent rules governing a Fourth Amendment challenge to the validity of a search warrant, and the search conducted pursuant to it, are well-settled. 'The question facing a reviewing court asked to determine whether probable cause supported the issuance of the warrant is whether the magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing.' [Citations.] 'The test for probable cause is not reducible to "precise definition or quantification." ' [Citation.] But . . . it is ' "less than a preponderance of the evidence or even a prima facie case." ' [Citation.] ' "The task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him [or her], . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." ' [Citations.] 'The magistrate's determination of probable cause is entitled to deferential review.' [Citations.] . . . [T]he warrant 'can be upset only if the affidavit fails as a matter of law to set forth sufficient competent evidence' supporting the finding of probable cause." (*People v. Westerfield* (2019) 6 Cal.5th 632, 659–660 (*Westerfield*).) "Although in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference

[4] Penal Code section 1538.5, subdivision (a)(1), provides in relevant part: "A defendant may move for the return of property or to suppress as evidence any tangible or intangible thing obtained as a result of a search or seizure on either of the following grounds: [¶] . . . (B) The search or seizure with a warrant was unreasonable because any of the following apply: [¶] (i) The warrant is insufficient on its face. [¶] (ii) The property or evidence obtained is not that described in the warrant. [¶] (iii) There was not probable cause for the issuance of the warrant. [¶] (iv) The method of execution of the warrant violated federal or state constitutional standards. [¶] (v) There was any other violation of federal or state constitutional standards."

to be accorded to warrants." (*United States v. Ventresca* (1965) 380 U.S. 102, 109; see also *People v. Weiss* (1999) 20 Cal.4th 1073, 1082–1083.)

Regarding persons who provide information to police about possible criminal activity, the California Supreme Court " 'ha[s] distinguished between those informants who "are often criminally disposed or implicated, and supply their 'tips' . . . in secret, and for pecuniary or other personal gain" and victims or chance witnesses of crime who "volunteer their information fortuitously, openly, and through motives of good citizenship." ' " (*People v. Scott* (2011) 52 Cal.4th 452, 475, quoting *People v. Ramey* (1976) 16 Cal.3d 263, 268–269 (*Ramey*).)

There is no requirement that information provided by a citizen informant be corroborated for it to constitute probable cause supporting the issuance of a warrant. (See *Ramey*, *supra*, 16 Cal.3d at p. 269; *People v. Smith* (1976) 17 Cal.3d 845, 852 ["An untested citizen-informant who has personally observed the commission of a crime is presumptively reliable."].) As *Ramey* explained, "It may therefore be stated as a general proposition that private citizens who are witnesses to or victims of a criminal act, absent some circumstance that would cast doubt upon their information, should be considered reliable. This does not, of course, dispense with the requirement that the informant—whether citizen or otherwise—furnish underlying facts sufficiently detailed to cause a reasonable person to believe that a crime had been committed and the named suspect was the perpetrator; and the rule also presupposes that the police be aware of the identity of the person providing the information and of his status as a true citizen informant. (*People v. Abbott* (1970) 3 Cal.App.3d 966, 970–971 [(*Abbott*)].) In short, probable cause will not be provided by conclusionary information or anonymous informants, but neither a previous demonstration of reliability nor subsequent corroboration is ordinarily necessary when witnesses to or victims of criminal activities report their observations in detail to the authorities." (*Ramey*, at p. 269; see also *People v. Hogan* (1969) 71 Cal.2d 888, 890–891 (*Hogan*).)

Furthermore, "[i]n order for the presumption of reliability to apply, [] the affidavit must affirmatively set forth the circumstances from which the existence of citizen-informer status can reasonably be inferred by a neutral and detached magistrate." (*People v. Kershaw* (1983) 147 Cal.App.3d 750, 755 (*Kershaw*); see also *People v. Lombera* (1989) 210 Cal.App.3d 29, 32 ["[I] is not necessary that the informant's name be disclosed in the affidavit for the status of citizen informant and its attendant presumption of reliability to attach."]; *People v. Superior Court* (*Haflich*) (1986) 180 Cal.App.3d 759, 768 (*Haflich*).)

"[W]hen . . . the police do obtain a warrant, that warrant is presumed valid." (*People v. Amador* (2000) 24 Cal.4th 387, 393; see also *People v. Panah* (2005) 35 Cal.4th 395, 456 [" ' "[T]here is a presumption of validity with respect to the affidavit." ' "].) "Because a search conducted pursuant to a search warrant is presumed lawful, the burden of establishing the invalidity of the search warrant rests upon the defendant." (*People v. Lazalde* (2004) 120 Cal.App.4th 858, 865; *Amador*, at p. 393.)

"In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his [or her] judgment that the form of the warrant is technically sufficient." (*United States v. Leon* (1984) 468 U.S. 897, 921 (*Leon*).) "In *Leon*, the Supreme Court held that when 'an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope,' the 'marginal or nonexistent benefits' produced by suppressing the evidence obtained 'cannot justify the substantial costs of exclusion.' [Citation.] '[T]he exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates.' [Citation.] Therefore, suppression of evidence is an appropriate remedy only if 'the magistrate or judge in issuing [the] warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth,' the affidavit is ' "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," ' or the affidavit is so

deficient in particularizing the place to be searched or the things to be seized that the executing officer 'cannot reasonably presume it to be valid.' [Citation.] In considering the issue, we apply the objective test of ' "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." ' [Citations.] We review the trial court's application of the good faith exception de novo." (*People v. Lazarus* (2015) 238 Cal.App.4th 734, 766–767 (*Lazarus*).)

2. Analysis

a. Citizen Informant

We begin our analysis by addressing Rowland's contentions concerning the nature of the informants and information they provided to police about the two images uploaded from an IP address ultimately tied to his residence. Rowland argues the search warrant affidavit lacks necessary details about the identity and actions of the " 'Microsoft Online Operation' employee" (Microsoft employee) who provided the cybertips to NCMEC. Likewise, Rowland asserts that the affidavit fails to provide information about the interaction between the Microsoft employee and NCMEC or the identity of the person at NCMEC who passed the cybertips on to Sergeant Dahl. Based on these alleged deficiencies, Rowland contends "the essential information tying the images to [his] IP address / computer was provided by an anonymous tipster," such anonymously provided information "is legally insufficient to provide probable cause," and thus "the warrant affidavit could not show that there would be 'a fair probability that contraband or evidence of a crime will be found in a particular place,' " namely, his residence.

The Attorney General counters that the cybertips were sufficiently reliable to support the magistrate's probable cause finding. The Attorney General asserts that the cybertips are akin to reports by citizen informants, federal law obligated Microsoft to submit the information about apparent child pornography to NCMEC, and the cybertips were corroborated by the images, confirmation that one of the depicted girls was

underage, and the IP address. The Attorney General further contends that Rowland has failed to meet his burden to establish the invalidity of the search warrant.

We are not persuaded by Rowland that the magistrate acted improperly under the present circumstances in finding the unnamed Microsoft and NCMEC employees to be presumptively reliable citizen informants. Widely available information reveals that " '[t]echnology companies like Yahoo, Google and Microsoft scan for child pornography and are required to report any discoveries to the National Center for Missing and Exploited Children.' "[5] (*United States v. Brown* (2d Cir. 2016) 843 F.3d 74, 85, fn. 2 (conc. opn. of Sack, J.), quoting Savage & Perlroth, *Yahoo Said to Have Adapted Email Scanner to Aid U.S. Surveillance,* N.Y. Times (Oct. 6, 2016) at pp. B1, B6; see also *Wilson, supra,* 56 Cal.App.5th at pp. 137–138, 143–144 [describing Google's method, dating back to 2008, for "ensur[ing] its systems were free of illegal content, particularly child sexual abuse material"].)

Although Microsoft is not required by federal law to monitor its users or seek out child pornography, the company "has a duty under federal law [as a service provider] to report apparent child pornography to the NCMEC once it obtains actual knowledge of such content." (*Wilson, supra,* 56 Cal.App.5th at p. 138, fn. 6, citing 18 U.S.C. § 2258A(a); see also *United States v. Bohannon* (N.D. Cal. 2020) 506 F.Supp.3d 907, 914, fn. 3 ["Microsoft must report information to NCMEC when it has actual knowledge of child pornography [citation] but is not required to maintain a sophisticated system for obtaining such knowledge."]; 18 U.S.C. § 2258E(6).) The report to NCMEC must include, among other information, the service provider's "individual point of contact" (18 U.S.C. § 2258A(a)(1)(B)(i)), and may include information regarding the identity of the

[5] Rowland makes no argument that Microsoft, its employee, or NCMEC acted as government agents in this case. Generally, independent reports of child pornography by technology companies "constitute private action that was not performed at the direction of the government." (*People v. Wilson* (2020) 56 Cal.App.5th 128, 144 (*Wilson*).)

individual who appears to have violated child pornography laws (e.g., the related IP address) and other relevant information (18 U.S.C. § 2258A(b)). Knowing and willful failure to make a report is punishable by a fine of at least $150,000. (18 U.S.C. § 2258A(e).)

Relatedly, "NCMEC is statutorily obligated to serve as a national clearinghouse and maintain a tip line for internet service providers to report suspected child sexual exploitation violations. [Citations.] NCMEC is statutorily obligated to forward those reports, known as 'Cybertips,' to federal law enforcement and may, and often does, forward the reports to state and local law enforcement." (*Wilson*, *supra*, 56 Cal.App.5th at p. 137, fn. 5; see also 18 U.S.C. § 2258A(c).)

Although the search warrant affidavit here did not state the federal law obligations imposed on both Microsoft and NCMEC regarding child pornography, we presume the magistrate knew the law when reviewing the affidavit and deciding whether it stated probable cause. (See *People v. Martin* (2005) 127 Cal.App.4th 970, 977 ["A judge is presumed to know and follow the law."], disapproved on other grounds in *People v. Achrem* (2013) 213 Cal.App.4th 153, 157; *Di Sabatino v. State Bar* (1980) 27 Cal.3d 159, 162, fn. 2.) Moreover, because the child pornography reporting obligation is a known legal requirement, a magistrate's consideration of that legal requirement does not amount to improper consideration of facts that do not "appear within the ' "four corners of the warrant affidavit." ' " (*People v. Clark* (2014) 230 Cal.App.4th 490, 497; see also *People v. Thompson* (1979) 89 Cal.App.3d 425, 429 ["The affidavit must be read in a common sense fashion and in the light of matters which are of common knowledge."]; *State v. Woldridge* (Fla.Dist.Ct.App. 2007) 958 So.2d 455, 459 (*Woldridge*) ["while it is true that the search warrant affidavit does not reference this statutory mandate, the magistrate and the trial court, like all citizens, are charged with knowing the applicable law"].)

Although no California court has issued a published decision examining the reliability and credibility of service providers and NCMEC with regard to their reports of

child pornography, one federal court of appeals recently "h[e]ld that an NCMEC cyber-tip generated by information provided to NCMEC by an internet company such as Google carries with it significant indicia of reliability. The [relevant federal law] imbues such significant reliability by mandating 'electronic communication service provider[s] [and] remote computing service[s]' to report illicit, questionable activity that comes through their servers." (*United States v. Landreneau* (5th Cir. 2020) 967 F.3d 443, 453.) Several other courts have come to similar conclusions about reports of child pornography from service provides through NCMEC to law enforcement. (See *United States v. Cameron* (D.Me. 2009) 652 F.Supp.2d 74, 82 [rejecting a challenge to a warrant that contained information from unnamed sources at Yahoo! and NCMEC and noting "each carries significant indicia of reliability"]; *United States v. Kling* (N.D.Iowa, July 12, 2006, No. CR06-3007 MWB) WL 1980179, at *6, report and recommendation adopted (N.D.Iowa, July 21, 2006) WL 2054375 [finding no merit to the "argument that the warrant affidavit could not support a probable cause finding because it failed to identify the individual Yahoo employee who provided the original information about pornographic photographs being uploaded to or downloaded from the site."]; *People v. Rabes* (Colo.Ct.App. 2010) 258 P.3d 937, 941 [explaining that "the magistrate could have concluded that the tip [from AOL to NCMEC] alleging that the AOL images constituted 'child pornography' was reliable"].)

Likewise, other jurisdictions have held that service providers "are presumed to be reliable sources akin to identified citizen informants." (*State v. Henz* (N.M.Ct.App. 2022) 514 P.3d 1, 7, cert. granted June 27, 2022, No. S-1-SC-39350.) In *Henz*, the New Mexico Court of Appeals recently discussed several decisions from courts in other states and concluded: "We agree with the above jurisdictions that have determined providers like Tumblr and Google [(i.e., the service providers in that case)] to be credible sources who, by first-hand knowledge, gather their reported information regarding the transmission or receipt of child pornography in a reliable fashion, and adopt those

jurisdictions' reasoning here." (*Id*. at *6.) The decisions from other jurisdictions relied on by the New Mexico Court of Appeals include *State v. Sisson* (Del.Super.Ct. 2005) 883 A.2d 868, 880, affd. *Sisson v. State* (Del. 2006) 903 A.2d 288 ["AOL was essentially a citizen witness to a crime and, as such, is presumed to be reliable. Accordingly, the Court finds that, under the circumstances, AOL was a reliable informant and no independent corroboration of the information provided by AOL was required."]; *Woldridge*, *supra*, 958 So.2d at pp. 458–459 ["hold[ing] that AOL's compliance with a federal law mandating that it report [the defendant]'s activities to NCMEC provides a presumption of reliability akin to that afforded a citizen informant"]; *Manzione v. State* (Ga. Ct. App. 2011) 312 Ga.App. 638, 642 [719 S.E.2d 533, 538] [stating that law enforcement is "entitled to presume the reliability of the Yahoo! report as transmitted through NCMEC without independently verifying the credibility of the Yahoo! employee who initially viewed the offensive images"]; *State v. Silverstein* (Wis.Ct.App. 2017) 378 Wis.2d 42, 57 [902 N.W.2d 550, 557] [explaining that even if the identity of the person working for a service provider who reported to NCMEC is unknown, the service provider "is not an anonymous entity" because it is "a named, traceable entity that is reporting a crime in furtherance of public safety," "gains nothing from making the tip," and "is under federal mandate to report suspected child abuse to NCMEC," an obligation which courts have held "heightens the reliability of the tip"]; and *Adams v. State* (Ala.Crim.App. 2020) 316 So.3d 260, 266 ["hold[ing] that the tip from the Internet company was presumed reliable based on the mandatory federal reporting requirements" and noting that the police had "corroborated the tip by reviewing the images and verifying the IP address and the user's name and physical address," and "there was no 'basis for the warrant-issuing magistrate to conclude that the . . . source was not credible.' "].)

In the face of the decisions from other jurisdictions, Rowland contends that, under California Supreme Court and other California precedent, the police must know the identity of their informant at the time they submit the search warrant affidavit in order for

that informant to be considered a citizen informant and presumed reliable. Rowland also "knows of no published California case holding that all employees of an organization can be presumed reliable if the organization is found to be reliable" and asserts that "[t]he idea that an unknown employee of a reliable organization could be treated as a 'citizen informant' goes far beyond" our Supreme Court's decisions in *Hogan*, *supra*, 71 Cal.2d 888, and *Ramey*, *supra*, 16 Cal.3d 263.

In *Hogan*, the California Supreme Court explained that "information from a citizen who purports to be the victim of a robbery or an assault has been held sufficient even though his reliability has not been previously tested. [Citations.] Such a person, who may expect to be called to testify after an arrest, and may be exposing himself to an action for malicious prosecution if he makes unfounded charges, is more than a mere informer who gives a tip to law enforcement officers that a person is engaged in a course of criminal conduct." (*Hogan*, *supra*, 71 Cal.2d at pp. 890–891; see also *Abbott*, *supra*, 3 Cal.App.3d at p. 971 [discussing *Hogan* and stating that "the rationale for the citizen informer rule requires knowledge of the 'citizen's' identity"].)

As discussed *ante*, in *Ramey*, our Supreme Court similarly stated that the citizen-informant rule "presupposes that the police be aware of the identity of the person providing the information and of his status as a true citizen informant." (*Ramey*, *supra*, 16 Cal.3d at p. 269.)

We disagree with Rowland's assertion that, under our Supreme Court's decisions, it is improper in the present case to consider the unnamed Microsoft employee who viewed the two images and forwarded them to NCMEC as a citizen informant. Although the search warrant affidavit does not provide information regarding the identity of the Microsoft employee and further describes the cybertips as "anonymous," the critical question is whether the affidavit "affirmatively set[s] forth the circumstances from which the existence of citizen-informer status can reasonably be inferred by a neutral and detached magistrate." (*Kershaw*, *supra*, 147 Cal.App.3d at p. 755.)

As one Court of Appeal has explained, *Ramey*'s statement regarding the informant's identity and status as a citizen informant "does not mean the police necessarily must obtain the name of an informant before they act on his information. Unless the informant is a well known public figure whose reputation for probity is virtually synonymous with his name, determination of his name alone adds nothing to his reliability. Rather the police must have reason to believe, and in fact believe, the informant is truly a citizen informant as opposed to a police informant. This belief and its reasonableness must be gathered from the surrounding circumstances one of which, mere name alone, is rarely relevant."[6] (*Haflich, supra,* 180 Cal.App.3d at p. 768.)

Here, the affidavit informed the magistrate that a person who worked for Microsoft notified NCMEC about two suspect images that the employee had viewed. For the reasons discussed above, the magistrate could reasonably infer from this information that the Microsoft employee had acted in accord with Microsoft's legal obligation as a service provider when reporting the apparent child pornography to NCMEC. (See *Wilson,* supra, 56 Cal.App.5th at p. 137, fn. 5 & p. 138, fn. 6.) Furthermore, the magistrate could reasonably infer that the person was in fact a Microsoft employee acting in the course of his or her employment and complying with the company's federal reporting mandate for several reasons. First, the information provided indicated that the images were uploaded using a Microsoft product, "Bing Image." (See *Getty Images (U.S.), Inc. v. Microsoft Corp.* (S.D.N.Y. 2014) 61 F.Supp.3d 301, 302.) Second, the

---

[6] In *Haflich,* the Court of Appeal addressed a situation in which a police officer did not obtain the identity of an alleged crime victim (Porter) to whom the officer had spoken, in person, before conducting a warrantless entry and search of a residence. The court noted that "Porter's status as a citizen informant is unquestioned. Furthermore, unlike the anonymous informant in *Ramey,* Porter was physically present when he conveyed his information to the police and he personally directed [the officer] to the scene of the alleged crime. [Citation.] Failure to obtain Porter's name prior to entering defendant's house does not foreclose reasonable reliance on his information." (*Haflich, supra,* 180 Cal.App.3d at p. 768.)

information was detailed, such that it included the IP address from which the image files were uploaded to the Internet, the file names, and the exact times at which they were uploaded. Third, the fact that NCMEC—a longstanding clearinghouse and operator of the tipline—forwarded the cybertips to law enforcement suggests that the tips were submitted through the normal channel to NCMEC, and NCMEC had no reason to believe the tips (identified as coming from an employee at Microsoft, an established and major information technology company) were fraudulent. Lastly, the police subsequently reviewed the forwarded images and deemed them to be child pornography, confirming the reason why a Microsoft employee would have submitted a tip to NCMEC in the first place.

Although the affidavit fails to provide a name for the Microsoft employee who viewed and then sent the images and attendant information to NCMEC, federal law required that the cybertips include an "individual point of contact" at Microsoft. (18 U.S.C. § 2258A(a)(1)(B)(i).) Further, as a service provider, Microsoft was required to preserve the contents of its cybertips and related information for at least 90 days after submission to NCMEC. (See 18 U.S.C. § 2258A(h).) Given these requirements and the fact that the images here are electronic, it reasonable to believe that the police would have been able to trace the links in the chain between Microsoft, NCMEC, and themselves such that the specific people involved in the submission of the cybertips could have been found and held accountable if the tips were false.

Additionally, under the facts stated in the affidavit, it is not probable that the person who contacted NCMEC was an imposter unaffiliated with Microsoft who, for some personal or nefarious reason, fabricated the tips using his or her own child pornography to frame Rowland. To have done so, the person would have had to have known that the provided IP address had been assigned to Rowland's residence/computer equipment at the date and time stated in the tip. It also appears improbable that someone at NCMEC or a NCMEC imposter would have fabricated the cybertips and then sent

them to law enforcement. In fact, Rowland acknowledges that NCMEC simply acted as a conduit for passage of the information. In this context, the magistrate could reasonably presume that nefarious efforts by an imposter would have been recognized and exposed by law enforcement. The magistrate also could reasonably infer that the reporting persons here were in fact affiliated with Microsoft and NCMEC.

All in all, the police and magistrate (based on the search warrant affidavit) had reason to believe that the cybertips came from a reliable witness employed by Microsoft who acted in accord with Microsoft's federal obligation to report apparent child pornography. The police and magistrate also had reason to believe that a reliable person at NCMEC forwarded the two pornographic images to the police in accord with NCMEC's legal obligation. That the affidavit did not provide the name of the individual at Microsoft who originally submitted the tips or the person who forwarded the tips from NCMEC to the police does not, under the totality of the circumstances, undermine the determination that the tips came from unbiased citizen informants who could be presumed reliable and thus did not need any independent corroboration. Hence, we conclude the trial court did not err by rejecting Rowland's argument that the search warrant affidavit was deficient because an alleged anonymous tipster provided the information linking him to the two pornographic images.

b. Description of the Images

Rowland contends that the description of the two images set forth in the search warrant affidavit was too vague for the magistrate to conclude that they were in fact child pornography and thus other child pornography would be found when searching his property. He asserts that although a magistrate need not review images involving "explicit sex acts," if the images are described (as in this case) "very general[ly]" as involving "two nude female juveniles in bathtubs with their legs open exposing their vaginas," the magistrate has to view the images to determine if they are child pornography.

The affidavit here described both images as depicting "a fully nude female juvenile" in a bathtub. The juvenile in the image attendant to Cybertip 1 was sitting in the tub "with her legs spread open, exposing her vaginal area," "leaning back and [] smiling for the camera." The juvenile in the image attendant to Cybertip 2 "had both hands above her vagina area and appeared to be spreading her vagina" while apparently standing in a bathtub. The affidavit also described the juveniles' stature and stage of sexual development and included Detective Nava's belief about their ages and positioning "for the sexual gratification of the viewer." Additionally, Detective Nava relayed Sergeant Dahl's confirmation of the minor status of one of the juveniles and Sergeant Dahl's opinion that the images constituted child pornography.

Section 311.11, subdivision (a), prohibits knowing possession of "any matter, representation of information, data, or image . . . the production of which involves the use of a person under 18 years of age, knowing that the matter depicts a person under 18 years of age personally engaging in or simulating sexual conduct, as defined in subdivision (d) of Section 311.4." (§ 311.11, subd. (a).)

In turn, section 311.4, subdivision (d)(1), defines " 'sexual conduct' " as "any of the following, whether actual or simulated: sexual intercourse, oral copulation, anal intercourse, anal oral copulation, masturbation, bestiality, sexual sadism, sexual masochism, penetration of the vagina or rectum by any object in a lewd or lascivious manner, *exhibition of the genitals or pubic or rectal area for the purpose of sexual stimulation of the viewer*, any lewd or lascivious sexual act as defined in Section 288, or excretory functions performed in a lewd or lascivious manner, whether or not any of the above conduct is performed alone or between members of the same or opposite sex or between humans and animals. An act is simulated when it gives the appearance of being sexual conduct." (§ 311.4, subd. (d)(1), italics added.) (See also *People v. Kongs* (1994) 30 Cal.App.4th 1741, 1754–1757 (*Kongs*) [describing the requirements of section 311.4, subdivision (d)(1)].)

The descriptions provided by Detective Nava satisfied the definition of child pornography as set forth in the relevant statutes. The depicted females were underage, nude, in a bathtub, and exhibiting their genitals. One female had her legs spread while leaning back and smiling. The other appeared to be spreading her vagina with her head facing downward. As described, the images showed the females in unnatural poses that were sexually evocative. (See *Kongs*, *supra*, 30 Cal.App.4th at pp. 1755, 1757.) We conclude the descriptions in the affidavit established that the images were child pornography, such that they depicted an "exhibition of the genitals or pubic . . . area for the purpose of sexual stimulation of the viewer." (§ 311.4, subd. (d)(1).) Moreover, when reviewing the affidavit, the magistrate could properly rely on Detective Nava's and Sergeant Dahl's expertise and assessment of the images as child pornography. (See *People v. Sandlin* (1991) 230 Cal.App.3d 1310, 1315; *People v. Nicholls* (2008) 159 Cal.App.4th 703, 711 (*Nicholls*); see also *United States v. Krupa* (9th Cir. 2011) 658 F.3d 1174, 1178.)

Additionally, we are not persuaded that the magistrate was required to view the images in this case in order to ascertain probable cause. Because the description of the images in the affidavit was sufficient to reasonably believe that the images amounted to child pornography under California law, the magistrate could rely on that description and did not have to view the images to decide whether a warrant should issue to search and seize Rowland's property. (See *New York v. P.J. Video, Inc.* (1986) 475 U.S. 868, 874, fn. 5 [noting that the high court had "never held that a magistrate must personally view allegedly obscene films prior to issuing a warrant authorizing their seizure," and stating "that a reasonably specific affidavit describing the content of a film generally provides an adequate basis for the magistrate to determine whether there is probable cause to believe that the film is obscene, and whether a warrant authorizing the seizure of the film should issue"].)

c. Staleness

Rowland contends the information about the uploading of images from an IP address tied to him was stale because the search warrant was not executed until February 27, 2019, over four months after the uploading occurred.[7] He further asserts that the affidavit fails to provide information "that suggests that someone in possession of two images showing only nudity would keep a collection of child pornography information indefinitely."

"Information that is remote in time may be deemed stale and thus unworthy of consideration in determining whether an affidavit for a search warrant is supported by probable cause." (*People v. Hulland* (2003) 110 Cal.App.4th 1646, 1652.) "No bright-line rule defines the point at which information is considered stale. [Citation.] Rather, 'the question of staleness depends on the facts of each case.' [Citation.] 'If circumstances would justify a person of ordinary prudence to conclude that an activity had continued to the present time, then the passage of time will not render the information stale.' " (*People v. Carrington* (2009) 47 Cal.4th 145, 163–164.)

"The question turns on whether 'facts supporting the warrant application establish it is substantially probable the evidence sought will still be at the location at the time of the search.' [Citation.] 'Substantial delays do not render warrants stale where the defendant is not likely to dispose of the items police seek to seize.' " (*Lazarus*, *supra*, 238 Cal.App.4th at pp. 764–765; see also *United States v. Morales-Aldahondo* (1st Cir. 2008) 524 F.3d 115, 119 (*Morales-Aldahondo*) [Courts "must assess the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information."]; *United States v. Seiver* (7th Cir. 2012) 692 F.3d

[7] The image attached to Cybertip 1 was uploaded on October 11, 2018 (139 days before the search). The image attached to Cybertip 2 was uploaded on October 26, 2018 (124 days before the search). Detective Nava submitted the search warrant affidavit on February 22, 2019, and the magistrate signed the warrant that day. The police executed the warrant five days later.

774, 777 [“ ‘Staleness’ is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. Computers and computer equipment are ‘not the type of evidence that rapidly dissipates or degrades.’ ”].)

Courts have recognized that persons who possess child pornography are likely to retain it for lengthy periods. (See, e.g., *United States v. Wagner* (10th Cir. 2020) 951 F.3d 1232, 1246 [“Courts are less receptive to staleness challenges when the warrant concerns child pornography because ‘persons interested in those materials [are likely to hoard them] in the privacy of their homes . . . for significant periods of time.’ ”]; *United States v. Irving* (2d Cir. 2006) 452 F.3d 110, 125 [“When a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that ‘images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.’ ”]; *United States v. Richardson* (4th Cir. 2010) 607 F.3d 357, 370; *Morales-Aldahondo, supra,* 524 F.3d at p. 119; *United States v. Lacy* (9th Cir.1997) 119 F.3d 742, 746 (*Lacy*).)

Here, the affidavit stated that the two pornographic images were uploaded from Rowland’s IP address 15 days apart in October 2018. Additionally, Detective Nava described, based on his training and experience, the common tendencies of persons who “sexually objectify children,” including that they derive sexual gratification and satisfaction “from fantasy involving the use of images . . . about sexual activity with children,” “will often collect and possess sexually explicit objects such as . . . digital files . . . which depict children,” and “tend to collect” child pornography. Nava explained that “[b]ecause child pornography is illegal and not easily available, suspects must typically use significant efforts to locate and obtain it.” This effort “will typically lead a suspect/child predator to save or retain the child pornography” and “rarely, if ever, dispose of their sexually explicit materials.” Nava also explained that even if such person

were to "delete their digital files containing child pornography," those "deleted files can typically be recovered using forensic software."

Considering the instant facts, Detective Nava's opinions, and the relevant legal principles, we discern no error in the magistrate's determination that the affidavit's information was not stale. Four months is not an inordinate amount of time when digital child pornography is at issue. (See *United States v. Newsom* (7th Cir. 2005) 402 F.3d 780, 783 ["Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned."]; *Lacy, supra,* 119 F.3d 742 at p. 746 [finding information not stale where there was " 'good reason[]' " to believe computerized images of child pornography would still be present 10 months later].) Further, the uploading of two images over a couple of weeks suggests that the person who uploaded the images had an ongoing interest in child pornography, did not act purely by mistake or ignorance when posting the two images to the Internet, and could reasonably be considered a person who sexually objectifies children. These circumstances, combined with the information contained in the affidavit regarding the proclivities and predilections of persons who sexually objectify children and view child pornography, provided the magistrate a substantial basis for finding that child pornography would be found on Rowland's property in February 2019.

We are not persuaded by Rowland's reliance on *United States v. Weber* (9th Cir. 1990) 923 F.2d 1338, which is distinguishable on its facts. In *Weber*, the court described the information possessed by the agent who signed the affidavit as follows: "He knew (1) that two years previously, [the defendant] had been sent advertising material that was described by the customs agent who intercepted it as 'apparently' child pornography; (2) that although [the defendant] was advised that Customs had the material, he never claimed it; (3) that there was no proof that [the defendant] requested the advertising material; and (4) that [the defendant] answered a government-generated advertisement for child pornography and ordered materials that were to be delivered by the government just

before the execution of the warrant." (*Id*. at p. 1344.) The court observed that "to find probable cause for the materials listed in . . . the warrant [(i.e., various forms of child pornography)] would be to justify virtually any search of the home of a person who has once placed an order for child pornography—even if he never receives the materials ordered." (*Ibid*.) The court also rejected the government's reliance on opinions regarding the habits of " 'child molesters,' 'pedophiles,' and 'child pornography collectors' " because the affidavit failed to provide "reason to believe that [the defendant] was one of the 'types' described or possessed any of the habits ascribed to such types." (*Id*. at p. 1345.)

By contrast to *Weber*, in the present case Detective Nava's opinions were combined with concrete information establishing that someone at Rowland's residence had twice uploaded child pornography in the recent past. The magistrate thus could reasonably conclude that the person who did so was "a member of the class of persons who tended to keep child pornography." (*Nicholls*, *supra*, 159 Cal.App.4th at p. 713; see also *Lacy*, *supra*, 119 F.3d at p. 746, fn. 6 [distinguishing *Weber* on the ground that the affidavit "contained sufficient evidence that [the defendant] had downloaded computerized visual depictions of child pornography to provide a foundation for evidence regarding the practices of possessors of such pornography"].)

In sum, we agree with the magistrate that the search warrant affidavit sufficiently provided probable cause to believe that evidence of the possession of child pornography could be found in Rowland's residence and the vehicles identified in the search warrant. Rowland has not established that the affidavit failed to provide " 'sufficient competent evidence' " to support the magistrate's finding of probable cause. (*Westerfield*, *supra*, 6 Cal.5th at p. 660.)

d. Good-Faith Exception

Because we conclude the search warrant affidavit demonstrated a fair probability that a search would uncover wrongdoing, there is no need to examine whether the good

faith exception to the exclusionary rule applies. (See *People v. Hansborough* (1988) 199 Cal.App.3d 579, 584–585.) Nevertheless, because the People contended at trial (and now on appeal) that even if there were deficiencies in the affidavit, the seized evidence should not be suppressed because the police executing the warrant acted in good faith, we will address the People's contention.

"The good faith exception to the exclusionary rule applies when police act in objectively reasonable reliance on a search warrant issued by a detached and neutral magistrate. [Citation.] The prosecution bears the burden to prove officers' reliance on a warrant was objectively reasonable. [Citation.] 'This objective standard "requires officers to have a reasonable knowledge of what the law prohibits." ' " (*People v. Nguyen* (2017) 12 Cal.App.5th 574, 586–587; see also *Lazarus*, *supra*, 238 Cal.App.4th at pp. 766–767.)

Here, Rowland does not contend that the affidavit contained false information, the warrant was issued by a magistrate who "wholly abandoned his judicial role," or the warrant was "so facially deficient —i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers [could not] reasonably presume it to be valid." (*Leon*, *supra*, 468 U.S. at p. 923.) Rather, the present dispute turns on whether the affidavit " 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.' " (*Ibid*.) Rowland grounds his argument against application of the good faith exception on the same contentions we have addressed *ante* regarding the alleged deficiencies in the affidavit.

For substantially the same reasons that we hold the warrant was supported by probable cause, we conclude that the good faith exception applies. Given that there was no published California precedent on the question whether a cybertip from a service provider (like Microsoft through NCMEC) could be presumed reliable under the citizen-informant rule, but several other jurisdictions had previously concluded that such tip is presumptively reliable and akin to a tip provided by an identified citizen informant, we

decide the police could have reasonably relied in this instance on the magistrate's finding of probable cause. (See *People v. Pressey* (2002) 102 Cal.App.4th 1178, 1191.) Similarly, with regard to the alleged vagueness of the image descriptions and staleness, under the facts, precedent, and statutes discussed *ante*, there was a basis for the police officers involved in the search to have concluded that there were reasonable grounds to support probable cause. Therefore, we discern no error in the trial court's ruling denying Rowland's motion to quash the search warrant.

B. *Court-Imposed Fees*

"On September 18, 2020, the Governor signed Assembly Bill [No.] 1869 . . . [¶] . . . [which] abrogated the authority to impose and collect 23 different administrative fees, including, as relevant here, the probation supervision fee and the criminal justice administration fee." (*People v. Greeley* (2021) 70 Cal.App.5th 609, 625 (*Greeley*).) Assembly Bill No. 1869 added section 1465.9 to the Penal Code and section 6111 to the Government Code. (Stats. 2020, ch. 92, §§ 11, 62.) Relevant to the probation supervision fee, current section 1465.9, subdivision (a), provides that "[t]he balance of any court-imposed costs pursuant to" former section 1203.1b, as that section "read on June 30, 2021, shall be unenforceable and uncollectible and any portion of a judgment imposing those costs shall be vacated."[8] (§ 1465.9; Stats. 2021, ch. 257, § 35.) "Relevant to the criminal justice administration fee, Government Code section 6111 provides, 'On and after July 1, 2021, the unpaid balance of any court-imposed costs pursuant to [Government Code] [s]ection 27712, subdivision (c) or (f) of [Government Code] [s]ection 29550, and [Government Code] [s]ections 29550.1, 29550.2, and

[8] Section 1465.9 originally provided: "(a) On and after July 1, 2021, the balance of any court-imposed costs pursuant to [s]ection 987.4, subdivision (a) of [s]ection 987.5, [s]ections 987.8, 1203, 1203.1e, 1203.016, 1203.018, 1203.1b, 1208.2, 1210.15, 3010.8, 4024.2, and 6266, as those sections read on June 30, 2021, shall be unenforceable and uncollectible and any portion of a judgment imposing those costs shall be vacated. [¶] (b) This section shall become operative on July 1, 2021." (Stats. 2020, Ch. 92, § 62.)

29550.3, as those sections read on June 30, 2021, is unenforceable and uncollectible and any portion of a judgment imposing those costs shall be vacated.' " (*Greeley*, at pp. 625–626.)

Based on this change in the law, we requested supplemental briefing from the parties on the effect of Government Code section 6111 on the criminal justice administration fee and section 1465.9 on the probation supervision fee ordered at Rowland's sentencing. In his supplemental letter brief, the Attorney General concedes that both Government Code section 6111 and section 1465.9 apply here and states that Rowland is no longer responsible for any unpaid balance (as of July 1, 2021) on the criminal justice administration fee and probation supervision fee. The Attorney General further contends that, under current section 1465.9, subdivision (a), Rowland is not entitled to recoup any portion of the probation supervision fee that he may have paid before July 1, 2021. Rowland agrees with the Attorney General (but notes "that this is the result only if [his] conviction is otherwise affirmed").

We agree that Government Code section 6111 and section 1465.9 apply to this matter, the unpaid balance of the criminal justice administration fee and probation supervision fee are unenforceable and uncollectible, and the portion of the judgment imposing those fees must be vacated. (See *Greeley*, *supra*, 70 Cal.App.5th at pp. 626–627; *People v. Lopez-Vinck* (2021) 68 Cal.App.5th 945, 953–954; *People v. Pacheco* (2022) 75 Cal.App.5th 207, 214–215.) Thus, we will modify the judgment as required by the new law and direct the trial court to prepare an amended minute order reflecting the modification.

III. DISPOSITION

The trial court's January 7, 2021 order imposing a $129.75 criminal justice administration fee (former Gov. Code, § 29550 et seq.) and a $50 monthly probation supervision fee (former Pen. Code, § 1203.1b) is modified to vacate any portion of the criminal justice administration fee and probation supervision fee that remained unpaid as

of July 1, 2021. In all other respects, the judgment is affirmed. The trial court shall prepare an amended minute order to reflect the vacatur of the criminal justice administration fee and probation supervision fee.

_____
Danner, Acting P.J.

WE CONCUR:

_____
Lie, J.

_____
Wilson, J.

H048799
People v. Rowland

Trial Court: County of Santa Clara

Trial Judge: Hon. Panteha E. Saban

Counsel: Law Offices of Beles & Beles, Robert J. Beles, Paul McCarthy, and Michah Reyner for Defendant and Appellant.

Rob Bonta, Attorney General, Lance E. Winters, Chief Assistant Attorney General, Jeffrey M. Laurence, Senior Assistant Attorney General, Donna M. Provenzano, Supervising Deputy Attorney General, and Victoria Ratnikova for Plaintiff and Respondent.