FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff - Appellee*, v. JOHN HOLCOMB, *Defendant - Appellant*.	No. 23-469 D.C. No. 2:21-cr-075-RSL OPINION

Appeal from the United States District Court
for the Western District of Washington
Robert S. Lasnik, District Judge

Argued and Submitted September 10, 2024
Seattle, Washington

Filed March 27, 2025

Before: Susan P. Graber and Jennifer Sung, Circuit Judges,
and Jed S. Rakoff, District Judge.[*]

Opinion by Judge Rakoff;
Partial Concurrence and Partial Dissent by Judge Sung

[*] The Honorable Jed S. Rakoff, United States District Judge for the Southern District of New York, sitting by designation.

SUMMARY[**]

Criminal Law

The panel reversed the district court's ruling on John Holcomb's motion to suppress three videos found on his computer, vacated his conviction and sentence for producing child pornography, and remanded for further proceedings.

The panel held (1) the "dominion and control" provision of a second warrant to search Holcomb's computer was invalid because it was both overbroad and insufficiently particular; (2) the good-faith exception does not apply to the examiner's search of the computer; and (3) the plain view doctrine does not independently justify the examiner's seizure of the videos.

Judge Sung concurred in part and dissented in part. She concurred with the holding that the dominion and control provision is overbroad and insufficiently particular, but would find that the provision is severable from the remainder of the warrant. Because the record is not clear enough to make the necessary findings of fact in the first instance, she would remand for a determination whether the videos were permissibly seized pursuant to a lawful provision in the warrant, a threshold inquiry that also impacts the analysis of the good faith exception and plain view doctrine.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

COUNSEL

Matthew P. Hampton (argued), Teal L. Miller, and Jonas B. Lerman, Assistant United States Attorneys; Laura Harmon, Special Assistant United States Attorney, Criminal Division; Tessa M. Gorman, United States Attorney; Office of the United States Attorney, United States Department of Justice, Seattle, Washington; Jehiel I. Baer, McNaul Ebel Nawrot & Helgren PLLC, Seattle, Washington; for Plaintiff-Appellee.

Colin A. Fieman (argued) and Gregory Geist, Assistant Federal Public Defenders; Alan Zarky, Research and Writing Attorney; Office of the Federal Public Defender, Seattle, Washington; for Defendant-Appellant.

John C. Ellis Jr., Law Offices of John C. Ellis Jr. Inc., San Diego, California, for Amici Curiae Digital Forensic Examiners.

Jennifer S. Granick, Immigrants Rights Project, American Civil Liberties Union Foundation, San Francisco, California; Brett M. Kaufman, American Civil Liberties Union Foundation, New York, New York; Jazmyn Clark, American Civil Liberties Union of Washington Foundation, Seattle, Washington; for Amici Curiae American Civil Liberties Union and American Civil Liberties Union of Washington Foundation.

David B. Owens and Rachel Nowlin-Sohl, Attorneys; Averill L. Aubrey, Megan Haygood, Kayleigh McNiel, and Michael C. Orehek, Law Students; Civil Rights and Justice Clinic, University of Washington School of Law; for Amici Curiae Fourth Amendment Scholars.

OPINION

RAKOFF, District Judge:

This case raises a variation of the familiar but always troubling issue of whether someone can be prosecuted for despicable criminal conduct based on evidence obtained in violation of the United States Constitution. In the circumstances of this case, respect for the Constitution and the rule of law requires an answer of "no."

I.

In the early hours of January 28, 2020, officers of the Burlington Police Department, responding to a 911 call, came to the house of defendant John Holcomb. Holcomb lived at the house with his then-girlfriend Jill Liddle. When officers arrived at the scene, they spoke with Holcomb, who stated that he had recently rescued his ex-girlfriend, "J.J.," from sex slavery and that he had brought her to his house. Holcomb told officers that J.J. was "acting crazy" and that he wanted her to leave.

Officers then spoke with J.J., who claimed that Holcomb had sexually assaulted her. She stated that she and Holcomb had engaged in sexual relations the day before in his bedroom, during which Holcomb took photographs of her on his cellphone without her consent and uploaded them onto his computer. Later that evening, J.J. agreed to perform oral sex on Holcomb in his bedroom, but when she later indicated that she wanted to stop, Holcomb pushed her head down and forcibly inserted his finger into her anus, causing her significant pain. J.J. further claimed that, after being restrained by Holcomb against her will, she had finally

managed to break free, had said "I'm done," and had left the bedroom crying.

Officers proceeded to investigate the alleged sexual assault. That same day, they obtained a search warrant for Holcomb's house that authorized them to seize, but not search, his cellphone and computer.[1] When they executed that warrant, they discovered that Holcomb's computer was attached to a surveillance system, which included a video camera in his bedroom. Later that evening, officers returned to Holcomb's house and arrested him for rape.

Upon his arrest, Holcomb insisted that the sexual encounter was consensual and that a surveillance video on his computer would prove his innocence. Liddle, who was at the house when Holcomb was arrested, confirmed Holcomb's account. She explained that she had watched the video on Holcomb's computer before the police seized it and that it showed that his encounter with J.J. was consensual. Holcomb consented to a search of his computer, provided officers with his computer password, and told them how to find and play the video. However, just six days later, before officers had reviewed the video, Holcomb informed officers that he wished to withdraw his consent to search his computer.

On February 4, 2020, the state sought, and the Skagit County Superior Court granted, a warrant (the "second warrant") to search Holcomb's computer. That warrant

[1] Holcomb does not challenge the validity or execution of this first warrant.

authorized the Government to "search for and seize" five categories of evidence, as follows:

> (1) "Evidence of communications to or from J.J. and/or between JOHN HOLCOMB. [] This communication includes but is not limited to voicemails/audio recordings, SMS, MMS, emails, chats, social media posts/online forums, contact lists and call logs from June 1, 2019 to current.
>
> (2) Surveillance video or images depicting JJ or JOHN HOLCOMB and any other surveillance video or images from Jan[uary] 26th 2020 to current.
>
> (3) Any location data including GPS coordinates from Jan[uary] 26th 2020 to current.
>
> (4) User search history from the devices to include but not limited to searched words, items, phrases, names, places, or images from Jan[uary] 26[th] 2020 to current.
>
> (5) Files[,] artifacts or information including but not limited to[] documents, photographs, videos, e-mails, social media posts, chats and internet cache that would show dominion and control for the devices.

Although the first four provisions of the second warrant were limited to the time period surrounding the alleged sexual

assault in 2020,[2] the fifth provision, which concerned "dominion and control" of Holcomb's devices, did not contain any temporal limitation.

After the court granted the second warrant, a digital forensic examiner began a search of Holcomb's computer, which contained thousands of files stored across separate upper and lower hard drives. The upper and lower hard drives contained files created during different time periods. While the upper hard drive contained newer files, including surveillance footage from the camera in Holcomb's bedroom from January 2020, the lower hard drive contained older files, all of which were created before September 2018. Rather than use an available computer program that would have allowed him to filter the computer's files by date and time or to otherwise limit his search to the period surrounding the alleged assault, the examiner "pull[ed] up all [the] videos" and "start[ed] just scrolling through [them]."

The examiner soon found a video of Holcomb and J.J. from January 27, 2020, in the computer's upper hard drive. That video featured several sexual encounters, including one during which Holcomb took photographs of J.J. on his cellphone and another during which J.J. performed oral sex on Holcomb. During the latter encounter, Holcomb did not appear to restrain J.J., and J.J. did not appear to leave the room crying. However, Holcomb did "touch [J.J.'s] butt," and J.J. did say "I'm done." Although the examiner had not yet completed his search of the computer, he showed the

[2] Unlike the second, third, and fourth provisions, the first provision covered evidence from "June 1, 2019 to current" in order to account for a period during which Holcomb and J.J. exchanged messages to plan their January 2020 meeting.

video to the prosecuting attorney and a detective. After viewing the video together, the three men agreed that the encounter appeared to have been consensual. The detective then directed the Washington State Patrol Crime Laboratory to "stop all testing except for the required testing" because he expected that the case would shortly be dismissed.

Notwithstanding that expectation, the examiner resumed his search for footage of the alleged sexual assault, directing his attention to the lower hard drive. During this search, he viewed various videos that were uploaded years before the alleged assault occurred, including several videos of Holcomb and Liddle having consensual sex. He also discovered three videos that appeared to depict child sexual abuse. As he later explained, he first noticed a thumbnail for a video from November 2016 that "appeared similar" to the video of Holcomb and J.J. having sex from January 2020. He opened that video, which showed Holcomb raping a pre-pubescent girl, whom officers later identified as Holcomb's daughter. The examiner also observed, but did not open, two additional videos from November 2016 with thumbnails that appeared to depict pre-pubescent girls who were "posed for sex."

Based on the examiner's observations, the Burlington Police Department obtained a third warrant to search Holcomb's computer for child pornography. That warrant authorized the Burlington Police Department to open and view all three videos. After reviewing the three videos, the Burlington Police Department dropped the sexual assault charges against Holcomb, but the Island County Police Department charged him with rape of a child and related crimes. Holcomb moved to suppress the three videos. Without responding to that motion, the Island County Police Department dropped the charges against him. The Skagit

County Police Department then brought similar charges against Holcomb. When Holcomb again moved to suppress the videos, the Skagit County Police Department similarly dropped its charges. Local authorities then referred the case to the FBI.

On April 28, 2021, a federal grand jury indicted Holcomb on one count of producing child pornography in violation of 18 U.S.C. § 2251(a). Once again, Holcomb moved to suppress the three videos. In doing so, he raised various arguments about the validity of the "dominion and control" provision of the second warrant and the reasonableness of the search of his computer.

The district court initially granted Holcomb's motion to suppress.[3] Although the trial judge determined that probable cause supported the second warrant, he concluded that the dominion and control provision was both overbroad and insufficiently particular because it lacked any temporal limitation. The trial judge also concluded that the good-faith exception did not apply because "the dominion and control clause of the warrant was so facially deficient that no executing officer could reasonably presume it to be valid."

The Government, citing *Messerschmidt v. Millender*, 565 U.S. 535 (2012), moved for reconsideration, arguing that the district court had articulated a new constitutional

[3] It is undisputed that the second warrant issued by a state judge is, pursuant to the Fourteenth Amendment, subject to the limitations on searches and warrants set by the federal constitution. *See Stonehill v. United States*, 405 F.2d 738, 743 (9th Cir. 1968) (discussing *Mapp v. Ohio*, 367 U.S. 643 (1961) and *Elkins v. United States*, 364 U.S. 206 (1960)). Moreover, here, it was the federal government that made use of the fruits of the second warrant to bring the federal prosecution of Holcomb, so the Fourth Amendment would also come into play directly. *See* n.6, *infra*.

rule that dominion and control provisions must be temporally limited, and that, as a result, the "good-faith doctrine" permitted the temporally-unlimited search of Holcomb's computer because the dominion and control provision of the second warrant had authorized it and no existing precedent forbade it. In response, Holcomb argued that the Government had misread *Messerschmidt* and that it in fact stood only for the limited proposition that officers who obtain or rely on allegedly invalid warrants are not entitled to qualified immunity when the good-faith exception does not apply.

The district court granted the Government's motion for reconsideration. On the district court's reading of *Messerschmidt*, it was "unclear if the Supreme Court intended the road between *Leon*'s good-faith exception and qualified immunity to run both ways." However, because the Ninth Circuit appeared to embrace the Government's approach in *United States v. Needham*, 718 F.3d 1190 (9th Cir. 2013), and because the district court was unaware of a case specifically holding that dominion and control provisions must be temporally limited, the district court concluded that the good-faith exception applied and therefore denied Holcomb's motion to suppress. In reaching that conclusion, however, the district court reaffirmed its prior holding that the dominion and control provision was overbroad and insufficiently particular, emphasized that "[t]he state of the law [was] admittedly opaque," and stated that "district courts would be well-served by a Ninth Circuit opinion addressing the issues [raised] in [the case]."

After the district court granted the Government's motion for reconsideration, Holcomb pleaded guilty to producing child pornography pursuant to a plea agreement. In his plea agreement, he reserved the right to appeal the district court's

order denying his motion to suppress. The district court then sentenced Holcomb to a term of 240 months of imprisonment, to be followed by a lifetime of supervised release. This appeal followed.

II.

We review the denial of a motion to suppress evidence *de novo*.[4] *United States v. Holmes*, 121 F.4th 727, 734 (9th Cir. 2024). The district court's factual findings are reviewed for clear error, while pure questions of law and mixed questions of law and fact are reviewed *de novo*. *See United States v. Estrella*, 69 F.4th 958, 964 (9th Cir. 2023), *cert. denied*, 144 S. Ct. 1049 (Mem) (2024).

On appeal, Holcomb argues, *inter alia*, that the second warrant's dominion and control provision, on the basis of which the examiner located the three videos that led to Holcomb's indictment, was invalid because it was both overbroad and insufficiently particular. He further argues that, under Ninth Circuit precedent, the good-faith exception does not apply to the examiner's search of his computer. The Government disputes each of these arguments and also argues that the plain view doctrine independently authorized the examiner's seizure of the three videos depicting child sexual abuse.

We agree with the district court that the dominion and control provision was invalid because it was both overbroad and insufficiently particular. However, unlike the district court, we conclude that the good-faith exception does not apply to the examiner's search. Furthermore, we conclude

[4] Unless otherwise indicated, case quotations omit internal alterations, brackets, citations, ellipses, and quotation marks.

that the plain view doctrine does not independently justify the examiner's seizure of the videos.

A.

We first consider the validity of the dominion and control provision of the second warrant. At the outset, we observe that evidence of dominion and control was not at all relevant to the state's investigation of the alleged assault. Officers sought to obtain and review footage of one sexual encounter between Holcomb and J.J. from Holcomb's computer to determine whether it supported J.J.'s account of the alleged sexual assault. Regardless of who owned or controlled that computer, that footage would reveal whether their encounter was consensual. Moreover, even if dominion and control had been relevant in this unusual situation, Holcomb never disputed that the computer belonged to him. Indeed, he initially provided officers with his computer password and instructed them on how to find and view the footage stored on it. The Government speculates that dominion and control evidence was nevertheless relevant because Holcomb, Liddle, or someone else may have altered or deleted footage from the computer or tampered with the date and time stamps associated with the footage or other files. However, there was no evidence to suggest that anyone tampered with Holcomb's computer in any way. And if the examiner had found evidence to that effect, then the state easily could have sought another warrant to investigate further.[5]

[5] We have previously observed that "[c]omputer files are easy to disguise or rename" and have therefore not required the government to "trust the suspect's self-labeling when executing a [search] warrant." *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006); *see also United States v.*

Even assuming, *arguendo*, that evidence of dominion and control was relevant to the state's investigation, the warrant's dominion and control provision still violated the Fourth Amendment's specificity requirement.[6] The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized." U.S. Const. amend. IV. Our cases have distinguished the Fourth Amendment's specificity requirement in two respects: breadth and particularity. Breadth is the requirement that a warrant "be limited by the probable cause on which the warrant is

Hill, 459 F.3d 966, 977–78 (9th Cir. 2006) (similar). However, naming and labeling conventions, like those discussed in *Adjani* and *Hill*, are distinct from date and time stamps, which are at issue here. Although a sophisticated computer user can technically alter the date and time associated with a computer file, she cannot change that file's internal metadata, which will always accurately reflect the actual date and time that file was created. As amici explain, digital forensic examiners can readily discern the actual date and time that a file was created, as well as a suspect's efforts to disguise that date and time. *See* Brief for Digital Forensic Examiners as Amici Curiae Supporting Defendant-Appellant, *United States v. Holcomb* (No. 23-469), at 7–12. That it was technically possible that someone could have altered the dates and times associated with Holcomb's files is insufficient to establish that dominion and control evidence was relevant to the investigation and prosecution in this case. And, in any event, the Government never offered any evidence to suggest that anyone had in fact altered the date and time stamps associated with Holcomb's files.

[6] As previously noted, the Fourth Amendment is, in relevant part, made binding on the states by the Fourteenth Amendment. *See Stonehill*, 405 F.2d at 743. In any case, the Fourth Amendment would apply to a federal prosecution based on a state warrant. *See, e.g.*, *United States v. Jobe*, 933 F.3d 1074, 1076–78 (9th Cir. 2019); *United States v. Bynum*, 362 F.3d 574, 578–79 (9th Cir. 2004); *United States v. Washington*, 797 F.2d 1461, 1467–71 (9th Cir. 1986).

based," while particularity is the requirement that a warrant "clearly state what is sought." *United States v. SDI Future Health Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) ("*SDI*"). Together, these requirements protect against "the principal evil" of general warrants, which allowed royal officials during the colonial era to "search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown." *Ashcroft v. al-Kidd*, 563 U.S. 731, 742–43 (2011); *see also United States v. Kahre*, 737 F.3d 554, 566 (9th Cir. 2013) (per curiam) ("The prohibition of general warrants imposes a particularity limitation, requiring warrants to specify the items to be seized and the locations to be searched."). "[G]iven the vast amount of data" stored on computers, a "heightened" specificity requirement applies "in the computer context." *United States v. Adjani*, 452 F.3d 1140, 1149 (9th Cir. 2006). "Evidence seized pursuant to illegal general warrants must be suppressed." *United States v. Espinosa*, 827 F.2d 604, 610 (9th Cir. 1987).

Starting with overbreadth, the Government has failed to identify any meaningful limitation on the scope of the dominion and control provision. As noted above, the dominion and control provision authorized the state to seize "[f]iles[,] artifacts or information including but not limited to[] documents, photographs, videos, e-mails, social media posts, chats and internet cache that would show dominion and control for the [computer]." Unlike the other provisions of the warrant—which were limited to communications between Holcomb and J.J., surveillance footage depicting Holcomb or J.J., location data, and the computer's search history—the dominion and control provision was not limited to a particular type of evidence. In addition, again unlike the other provisions, the dominion and control provision lacked any temporal limitation, thereby authorizing the state to open

and examine any file from any time period, including files that long predated the alleged assault. The Government conceded as much at oral argument, stating that "almost any file could be opened to determine if it was responsive" to the dominion and control provision.

In actuality, the affidavit underlying the second warrant set forth no grounds to find probable cause to conduct a search—much less a limitless search—for dominion and control evidence. In fact, apart from the portion of the affidavit restating the dominion and control provision, the affidavit does not otherwise mention dominion or control.[7] To the extent that the affidavit alludes to dominion and control at all, it simply recounts how Holcomb initially

[7] By contrast, each of the other provisions of the second warrant was tied to allegations in the affidavit. As for the first provision, which concerned communications between Holcomb and J.J. in the months leading up to the alleged assault, the affidavit explains that J.J. told officers that she had been communicating with Holcomb using various apps and websites for several months, that J.J. showed officers some of their messages on her phone, and that officers observed that similar messages were "plainly visible" on Holcomb's open computer when they recovered it pursuant to the first search warrant. As for the second provision, which concerned surveillance footage depicting Holcomb or J.J. on the day of and after the alleged assault, the affidavit describes Holcomb's "active surveillance system," which officers discovered while executing the first search warrant. As for the third provision, which concerned location data from the day of and after the alleged assault, the affidavit states that officers had already seized Holcomb's cellphone pursuant to the first search warrant, that people tend to keep their cellphones on their persons, and that cellphones can therefore be used to obtain location data. And finally, as for the fourth provision, which concerns Holcomb's search history on the day of and after the alleged assault, the affidavit stated that officers observed various search results on Holcomb's open computer and that evidence of a defendant's search history "can be used to corroborate or refute the details of [an] . . . alibi or the statements of a victim or witness."

"provided written permission to search for both *his* desktop and laptop computers," how Holcomb "advised police that he revoked his previous consent to search both *his* computers," and how the Government was "therefore applying for a search warrant in order to search [the] devices." Excerpts of Record 134 (emphases added). At most, these statements suggest that Holcomb had dominion and control over the computer. They do not establish probable cause to review all the files on Holcomb's computer to determine if they might bear on the issue of dominion and control. We therefore conclude that the second warrant's dominion and control provision was overbroad.

We similarly conclude that the dominion and control provision was insufficiently particular. As we have explained, "[t]he purpose of particularizing the items to be seized is to insure that when the warrant is executed, nothing is left to the officer's discretion." *United States v. Hurt*, 795 F.2d 765, 772 (9th Cir. 1986), *amended on denial of reh'g*, 808 F.2d 707 (9th Cir. 1987). Because Holcomb's computer contained thousands of files and because the dominion and control provision did not contain any temporal limitations, the examiner simply exercised his unfettered discretion in determining which files to scroll past and which files to open and examine pursuant to that provision. On that basis alone, we can conclude that the dominion and control provision was insufficiently particular.

It is true that in assessing whether a warrant provision is sufficiently particular, we also consider whether it would have been "reasonable" for the Government to "provide a more specific description of the items [to be searched] at that juncture of the investigation." *United States v. Banks*, 556 F.3d 967, 973 (9th Cir. 2009); *see also United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) ("Generic

classifications in a warrant are acceptable only when a more precise description is not possible."). Here, the Government was well aware of the relevant time period, as it was investigating a single incident that took place in a particular location on a specific date. Every provision of the second warrant except for the dominion and control provision therefore was limited to the period surrounding that incident. The Government has failed to put forth a persuasive reason why the dominion and control provision could not be similarly limited to that period. Accordingly, we conclude that the dominion and control provision was insufficiently particular.

Both because it was overbroad and because it was insufficiently particular, the dominion and control provision effectively transformed the second warrant into a general warrant. Although the other provisions of the warrant sought to limit the warrant's scope to narrow categories of evidence that were relevant to the alleged sexual assault of J.J. and for which there was probable cause to search, the dominion and control provision effectively allowed the Government to engage in the sort of "exploratory rummaging in a person's belongings" that the Fourth Amendment's warrant requirement was intended to prevent. *United States v. Wright*, 667 F.2d 793, 797 (9th Cir. 1982) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). Indeed, the examiner viewed footage uploaded years before the alleged assault, including several intimate videos of Holcomb and Liddle.

The partial dissent would hold that the dominion and control provision is severable from the rest of the second warrant. Indeed, we have "embraced the doctrine of severance, which allows us to strike from a warrant those portions that are invalid and preserve those portions that

satisfy the Fourth Amendment." *United States v. Flores*, 802 F.3d 1028, 1045 (9th Cir. 2015). If, after striking invalid provisions of a warrant, we conclude that others are valid, then evidence seized pursuant to the valid provisions need not be suppressed. *See United States v. Gomez-Soto*, 723 F.2d 649, 654 (9th Cir. 1984). In this case, the Government has argued only that "[t]he child-rape videos were dominion-and-control evidence." The Government has never asked us, or the district court, to conduct a severability analysis. Therefore, any such argument is waived or forfeited. *See United States v. Holmes*, 121 F.4th 727, 739 (9th Cir. 2024) (holding that arguments not raised to the district court are forfeited); *Bolin v. Davis*, 13 F.4th 797, 809 n.4 (9th Cir. 2021) (holding that arguments not raised in a party's opening brief are forfeited).

The partial dissent insists that the Government preserved a severability argument by arguing in the alternative that the examiner could have found the three videos depicting child sexual abuse pursuant to the second warrant's separate surveillance footage provision, which authorized the Government to search for and seize "[s]urveillance video or images depicting JJ or JOHN HOLCOMB and any other surveillance video or images from Jan[uary] 26th 2020 to current." We disagree. On its face, the surveillance footage provision is limited to material created on and after January 26, 2020, and each of the three videos was uploaded in November 2016. The Government nevertheless argues that the surveillance provision's temporal limitation "limited what the police could seize, not what they could search." However, that argument also contravenes the text of the surveillance footage provision, which explicitly allowed the state to "search for and seize" surveillance footage evidence. Moreover, that argument implicitly recognizes that, if the

temporal limitation had applied to the search, as well as to the seizure of any evidence, then the surveillance footage provision would not have authorized the search of files from November 2016. Because we do not agree that the date-restricted surveillance footage provision allowed for an unrestricted search for surveillance footage, we do not accept the Government's surveillance provision argument as a meaningful argument in the alternative that served to preserve a separate severability argument.

Even if the Government had preserved such an argument, the severability doctrine would not save the examiner's search because it is clear that the examiner discovered the disputed evidence pursuant to the dominion and control provision alone. The only alleged crime that justified the issuance of the second warrant was the alleged sexual assault on January 27, 2020. The second warrant limited all search categories *except* dominion and control to the period surrounding the alleged sexual assault. Search for communications was limited to the period on or after June 1, 2019, while search for surveillance footage, location data, and search history was limited to the period on or after January 26, 2020. The search of the upper hard drive uncovered the relevant video of the sexual encounter on January 27, 2020. The *later* search that yielded the three videos depicting child sexual abuse appeared on the lower hard drive, which contained *only* materials created before September 2018. Accordingly, the only provision of the warrant that could have justified the search of the lower hard drive was the dominion and control provision—the only portion of the warrant that allowed for an unlimited search for evidence from before the period surrounding the alleged sexual assault.

In holding that the dominion and control provision transformed the second warrant into a general warrant, we do not mean to suggest that dominion and control provisions must always contain temporal limitations.[8] As we have explained, "[t]he specificity required in a warrant varies depending on the circumstances of the case and the type of items involved." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). As indicated above, we have stated that warrants describing "generic categories of items" are "not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Id.* Consistent with these principles, we have upheld search warrants, including search warrants for computers, that contained broad provisions lacking temporal limitations. *See, e.g.*, *United States v. Schesso*, 730 F.3d 1040, 1046–47 (9th Cir. 2013); *Adjani*, 452 F.3d at 1147–50; *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997). However, on the facts of this case, where the Government has failed to establish that evidence of dominion and control was relevant to its search, where the Government knew the exact time period surrounding the incident it sought to investigate, where the affidavit did not establish probable cause to search for evidence outside that period, and where every other warrant provision sought to limit the scope of the warrant to that period, the unlimited dominion and control provision plainly violated the Fourth Amendment's specificity requirement. Any other holding would allow *any* warrant with a dominion and control

[8] Nor do we mean to suggest that the Government must always exercise time-limited warrant provisions in a particular way. In this case, the parties dispute whether the examiner was required to use date and time filters to ensure that he did not open any files produced outside the period for which there was probable cause to search. Our holding concerns only the impermissible scope of the second warrant, not the means by which the Government sought to execute it, so we do not reach that issue.

provision to function as a general warrant. The Fourth Amendment forecloses that result. *See United States v. Bridges*, 344 F.3d 1010, 1014 (9th Cir. 2003) ("The [Fourth] Amendment is to be liberally construed and all owe the duty of vigilance for its effective enforcement lest there shall be impairment of the rights for the protection of which it was adopted.").

B.

Having determined that the dominion and control provision was invalid twice over, we proceed to consider whether the examiner nevertheless complied with the Fourth Amendment by executing the second warrant in good faith. Under the good-faith exception, if officers conduct a search pursuant to a search warrant that is later invalidated, they still satisfy the Fourth Amendment so long as they acted in "objectively reasonable reliance" on that warrant. *United States v. Barnes*, 895 F.3d 1194, 1201 (9th Cir. 2018).

The Supreme Court has recognized "four situations that *per se* fail to satisfy the good faith exception." *United States v. Underwood*, 725 F.3d 1076, 1085 (9th Cir. 2013) (discussing *United States v. Leon*, 468 U.S. 897 (1984)).

> The four situations are: (1) where the affiant recklessly or knowingly placed false information in the affidavit that misled the issuing judge; (2) where the judge wholly abandons his or her judicial role; (3) where the affidavit is so lacking in indicia of probable cause as to render official belief in its existence utterly unreasonable; and (4) where the warrant is so facially deficient—i.e., in failing to particularize the

> place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.

Id. In each of these situations, an officer "will have no reasonable grounds for believing that the warrant was properly issued. *Id.*

All four exceptions to good-faith reliance are well-established in our case law, but the overall standard governing the "objectively reasonable reliance" inquiry is not. The Government argues that, under the Supreme Court's decision in *Messerschmidt*, the standard governing the "objectively reasonable reliance" inquiry is the same as the "reasonable officer" standard in the qualified immunity context. *See Longoria v. Pinal County*, 873 F.3d 699, 704 (9th Cir. 2017) (discussing the qualified immunity doctrine). As our qualified immunity cases make clear, an officer is immune from civil suit where the plaintiff's rights were not "clearly established" at the time of his alleged misconduct. *Ballentine v. Tucker*, 28 F.4th 54, 64 (9th Cir. 2022). "To be clearly established, the contours of the right must be sufficiently clear that a reasonable official would understand that what he [was] doing violate[d] that right." *Id.* "While there need not be a case directly on point, existing precedent must have placed the statutory or constitutional question beyond debate." *Id.* Application of qualified immunity therefore hinges on the existence of analogous Supreme Court or Ninth Circuit precedent.

Holcomb, for his part, contests the Government's reading of *Messerschmidt*. Although he acknowledges that there is a "relationship" between the good-faith doctrine and the qualified-immunity doctrine, he insists that it goes "only in one direction." In his view, while an officer who acts in

good faith is entitled to qualified immunity from civil suit, that fact has no bearing on whether the officer acted in good faith for purposes of adjudicating a motion to suppress in a criminal case. Rather than apply the heightened qualified immunity standard to determine whether the defendant's rights were "clearly established" at the time of the violation, courts simply should ask whether a reasonably well-trained officer would have understood the warrant to be invalid. *See United States v. King*, 985 F.3d 702, 710 (9th Cir. 2021) ("The central question is whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.").

The parties' disagreement over the appropriate standard arises from uncertainty surrounding the relationship between *Messerschmidt* and two of our own cases. *Messerschmidt* was a qualified immunity case. The plaintiff brought a section 1983 claim against two police officers, alleging that they had violated his Fourth Amendment rights by executing an invalid search warrant. *See Messerschmidt*, 565 U.S. at 544. The Supreme Court was tasked with determining whether the officers were nevertheless entitled to qualified immunity. *Id.* at 546. The plaintiff argued that the officers were not entitled to qualified immunity because the warrant was not supported by probable cause and no reasonable officer could have presumed that the warrant was valid. *See id.* at 548. Reversing an *en banc* panel of this court, the Supreme Court disagreed, reasoning that, "[e]ven if the warrant . . . were invalid, it was not so obviously lacking in probable cause that the officers [could] be considered plainly incompetent for concluding otherwise." *Id.* at 556. In reaching that conclusion, the Supreme Court observed in a footnote that "the same standard of objective reasonableness that [it had] applied in the context of a suppression hearing

in *Leon* defines the qualified immunity accorded an officer who obtained or relied on an allegedly invalid warrant." *Id.* at 546 n.1.

The following year, we decided *United States v. Needham*, 718 F.3d 1190 (9th Cir. 2013). In that case, the defendant appealed the denial of his motion to suppress, arguing, among other things, that the district court had erred in applying the good-faith exception. *See id.* at 1193–94. Quoting *Messerschmidt*, we stated that "the same standard of objective reasonableness that the United States Supreme Court applied in the context of a suppression hearing in *Leon* defines the qualified immunity accorded to an officer who obtained or relied on an allegedly invalid warrant." *Id.* at 1194 (quoting *Messerschmidt*, 565 U.S. at 546 n.1). "It therefore follows," we continued, "that if an officer is granted qualified immunity in a civil suit for relying on a warrant alleged to be lacking probable cause, then reliance on the existence of probable cause in that warrant must also have been objectively reasonable under the *Leon* doctrine." *Id.* Because we had recently held that officers were entitled to qualified immunity in a case strongly resembling *Needham*, we concluded that the district court had not erred in denying the defendant's motion to suppress. *See id.* at 1194–95 (discussing *Dougherty v. City of Covina*, 654 F.3d 892 (9th Cir. 2011)). Simply put, because the officers would have been entitled to qualified immunity, the good-faith exception applied. In explaining our reasoning, we repeated that "the standard for granting qualified immunity is the same as the standard for objective reasonableness under *Leon*." *Id.* at 1195.

More recently, however, in *Manriquez v. Ensley*, 46 F.4th 1124 (9th Cir. 2022), we specifically distinguished the good-faith and qualified-immunity doctrines. After

conducting a search of a suspect's motel room pursuant to a search warrant, officers called the magistrate judge who had issued the warrant and asked her to expand its scope to include the suspect's home address. *See id.* at 1127–28. The magistrate judge agreed and instructed the officers to physically amend the warrant to include the new address before conducting the search. *See id.* at 1128. The officers disregarded that instruction and proceeded to search the suspect's house without amending the warrant. *See id.* When the defendant later filed a section 1983 claim alleging that the officers had violated his Fourth Amendment rights, the Government argued that the officers had acted in good faith and were therefore entitled to qualified immunity. *See id.* at 1127–29.

We agreed in part and disagreed in part. Because any reasonable officer would have noticed that the warrant did not authorize a search of the house, we concluded that the good-faith exception did not apply. *See id.* at 1130 & n.1. However, given the "novel facts" of the case, we further concluded that the officers had violated a right that was not "clearly established" at the time of the search and were therefore entitled to qualified immunity. *Id.* at 1130. In reaching these conclusions, we observed in a footnote, without discussing or even citing *Needham*, that "[w]hile there is admittedly substantial overlap" between the reasonableness analysis in the good-faith and qualified-immunity contexts, "the qualified immunity standard is more forgiving than the requirements of the Fourth Amendment." *Id.* at 1130 n.1. We added that, although "a court may hold that an officer's search does not fall within the good-faith exception based on analogous case law or even directly relevant authority from a sister

circuit[,] . . . there still might not be clearly established case law in our circuit to withstand qualified immunity." *Id.*

As the district court acknowledged in this case, it remains unclear whether the Supreme Court intended for "the road between *Leon*'s good-faith exception and qualified immunity to run both ways." *Needham* and *Manriquez* point in different directions on that question. While *Needham* suggests that courts should import the heightened qualified immunity standard, *Manriquez* rejected that approach in favor of the "reasonable officer" standard. Moreover, this three-judge panel cannot clarify the applicable standard without calling for *en banc* review. *See Antonio v. Wards Cove Packing Co.*, 810 F.2d 1477, 1478–79 (9th Cir. 1987) (en banc).

Interesting though this question may be, however, we need not resolve the tension between *Needham* and *Manriquez* in this case because we conclude that the good-faith exception does not apply under either standard. To begin with, our existing precedents clearly establish that warrant provisions like the second warrant's dominion and control provision violate a defendant's Fourth Amendment rights. Most notably, in *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995), a case involving charges of tax fraud and profit skimming, we considered the validity of a search warrant that authorized the Government to seize fourteen separate categories of business records. Pursuant to that warrant, the Government seized "essentially all of the [defendant] business's records, computer hardware and software, files, ledgers, and invoices." *Id.* at 425. We held that the warrant was overbroad and insufficiently particular because the Government "did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place," even though the Government was aware

of the relevant time period when it sought the warrant. *Id.* at 427; *see also United States v. Banks*, 556 F.3d 967, 973 (9th Cir. 2009) (explaining that *Kow* "invalidat[ed] a warrant where the affidavit indicated that the criminal activity began at a specific time period but the warrant was not limited to a particular time frame"); *United States v. Noushfar*, 78 F.3d 1442, 1447 (9th Cir. 1996) (similarly explaining that *Kow* invalidated a warrant on overbreadth grounds because the warrant "set no time limits and allowed seizure of essentially all the business's records, computer hardware and software, files, ledgers, and invoices"). Although the warrant in *Kow* delineated various categories of evidence, it "contained no limitations on which documents within each category could be seized or suggested how they related to criminal activity" and therefore the warrant was "indistinguishable from the general warrants repeatedly held by this court to be unconstitutional." *Kow*, 58 F.3d at 427 (citing *Ctr. Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 750 (9th Cir. 1989), and *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989)).

In *Kow*, moreover, while the Government argued that its officers had nevertheless acted in "objectively reasonable reliance" on the warrant, we were not persuaded. In rejecting the Government's argument, we explained that "[w]e have been vigilant in scrutinizing officers' good faith reliance on . . . illegally overbroad warrants." *Id.* at 428. Therefore, "when a warrant is facially overbroad, absent *specific assurances* from an impartial judge or magistrate that the defective warrant is valid despite its overbreadth, a reasonable reliance argument fails." *Id.* at 429 (emphasis in original). Because "[t]he [*Kow*] warrant should have been limited by time, location, and relationship to specifically described suspected criminal conduct," it was "wholly

deficient" and could not be salvaged by the good-faith exception. *Id.* at 430.

More recently, in *SDI*, we drew on our reasoning in *Kow* to invalidate several provisions of a search warrant as overbroad. In *SDI*, the Government sought to investigate allegations of Medicare fraud associated with a series of sham sleep studies. *See SDI*, 568 F.3d at 691–92. As part of its efforts to investigate the fraud scheme, the Government executed a search warrant authorizing the seizure of various categories of documents. *See id.* at 693. We determined that five of those categories were invalid because they lacked limitations that would have restricted the scope of the Government's search to the relevant studies. *See id.* at 704–05. For example, one of the five categories was for "[d]ocuments relating to non-privileged internal memoranda and E-mail." *Id.* at 704. Because internal memoranda "typically cover" a wide array of subjects, we concluded that the Government's failure to "limit the search team's reach to internal memoranda related to the sleep studies" constituted "an invitation to a general, exploratory rummaging in a person's belongings" and, therefore, violated the Fourth Amendment. *Id.* at 704–05. We similarly concluded that various other categories authorizing the seizure of documents relating to bank and payroll records were unconstitutionally overbroad because, "by failing to describe the crimes and individuals under investigation," they "provided the search team with discretion to seize records wholly unrelated to the finances of [the defendants]." *Id.* at 705. As in *Kow*, we determined that the good-faith exception was inapplicable because the offending provisions were overbroad under our existing precedents. *See id.* at 706.

Together, *Kow, SDI*, and the cases on which they rely stand for two clearly established principles. First, when

probable cause to search is limited to a particular location, suspect, time period, or type of evidence, any warrant provision that is wholly lacking in any corresponding limitation is overbroad and therefore facially deficient under the Fourth Amendment. Second, an officer who relies on any such provision while executing a search warrant does not act in good faith.

In this case, the officers had probable cause to search for evidence concerning Holcomb's alleged assault of J.J. in January 2020, but the second warrant authorized them to search for evidence of dominion and control without limitation. Pursuant to the clearly established law of this circuit, the dominion and control provision thereby rendered the second warrant a facially deficient general warrant. Therefore, even assuming that the Government's reading of *Messerschmidt* is correct, we conclude that the examiner did not act in "objectively reasonable reliance" on the second warrant when he discovered the videos depicting child sexual abuse from November 2016.

C.

The Government also argues that the seizure of the three videos depicting child sexual abuse was independently authorized by another exception to the warrant requirement: the plain view doctrine. Under that doctrine, the government may seize evidence without a valid warrant so long as government officials are "lawfully searching the area where the evidence is found" and "the incriminatory nature of the evidence [is] immediately apparent." *United States v. Stafford*, 416 F.3d 1068, 1076 (9th Cir. 2005). The burden of demonstrating that both requirements are satisfied lies with the Government. *See United States v. Chesher*, 678 F.2d 1353, 1356 (9th Cir. 1982). In this case, the

Government argues that both requirements are satisfied because the second warrant authorized officers to examine all of Holcomb's files to determine whether they fell under one of the warrant's provisions and because the illegality of videos was immediately apparent, as evidenced by the examiner's conclusion that two of the three videos depicted child sexual abuse based solely on their thumbnails.

We disagree. The Government was not "lawfully searching the area where the evidence was found" because it found the three videos while executing a general warrant. Where "the plain view seizure was in the context of officers executing an essentially general warrant," the "justification for the plain view is . . . absent." *Spilotro*, 800 F.2d at 968. The Government thus fails to satisfy the first requirement of the plain view doctrine.

* * *

For the reasons stated above, the district court's ruling on Holcomb's motion to suppress is **REVERSED**, Holcomb's conviction and sentence are **VACATED**, and the case is **REMANDED** for further proceedings consistent with this opinion.

SUNG, Circuit Judge, concurring in part and dissenting in part:

I concur with the holding that the dominion and control provision is constitutionally infirm because it is overbroad and insufficiently particular. However, I would find that the dominion and control provision is severable from the remainder of the warrant. "Our conclusion that [one provision] is impermissibly general does not, however, require invalidation of the entire…warrant. This court has embraced the doctrine of severance, which allows us to strike from a warrant those portions that are invalid and preserve those portions that satisfy the fourth amendment. Only those articles seized pursuant to the invalid portions need be suppressed." *United States v. Gomez-Soto*, 723 F.2d 649, 654 (9th Cir. 1984), *see also United States v. Spilotro*, 800 F.2d 959, 967 (9th Cir. 1986) ("In this circuit we follow the rule that where invalid portions of a warrant may be stricken and the remaining portions held valid, seizures pursuant to the valid portions will be sustained."). Here, only one of the warrant's five provisions is overbroad and insufficiently particular, and it is therefore "practicable" to sever the dominion and control provision and "uphold the portion that remains." *Gomez-Soto*, 723 F.2d at 654. *Compare Spilotro*, 800 F.2d at 967 (declining to apply the severance doctrine because only an insignificant, ancillary portion of the warrant was sufficiently specific and particular); *United States v. Kow*, 58 F.3d 423, 428 (9th Cir. 1995) (declining to apply the severance doctrine because

only one of the warrant's fourteen provisions was arguably not overbroad).[1]

I respectfully disagree with the majority's conclusion that "it is clear that the examiner discovered the disputed evidence pursuant to the dominion and control provision alone." Majority Opinion at 19. It is undisputed that the search warrant authorized the police to examine the Defendant's computers to look for surveillance videos of the alleged sexual assault. According to a police report, the detective tasked with searching the computers first found surveillance videos of Defendant and J.J. that were relevant to the sexual assault investigation and within the scope of the valid provisions of the search warrant. The detective was then advised to "continue processing the other hard drives as per standard procedures and to continue looking for additional surveillance videos or angles that may be present." "[W]hile he was still busy processing the hard drives for the video evidence in [the sexual assault] case," the detective saw a "thumbnail image" of a video that was "a black and white video file which appeared similar" to the first surveillance video. The detective further stated that "when he first saw the video file as a thumbnail image, he believed it to contain additional surveillance video from the [defendant's] residence which is why he played it." It was

[1] The majority argues that because the Government "has argued only that '[t]he child-rape videos were dominion-and-control evidence'" and did not ask the court to conduct a severability analysis, it waived or forfeited any severability argument. Majority Opinion at 18. I respectfully disagree. The Government argued in the alternative that law enforcement could have permissibly conducted the search pursuant to the provision authorizing the seizure of surveillance videos. Addressing whether the unlawful provision of the warrant is severable from the remainder is a necessary antecedent to addressing the Government's argument that the search was permissible pursuant to the surveillance video provision.

only after viewing the video that the detective realized it was not additional surveillance video of the alleged sexual assault, but apparent child sex abuse material. The detective also noted that this second video was "listed as having been created" on a date outside the date range of the valid provisions of the search warrant.

The government argues that, despite the apparent creation date, the detective found the second video while searching under the valid provisions of the warrant, and in the alternative, that the detective could view the video under the plain view exception. The majority rejects those arguments, arguing that there are no circumstances under which the detective could view the second video under the valid provisions of the search warrant. The district court likewise assumed that "[i]f the videos were located while searching pursuant to a different clause of the warrant, the search would have been unreasonable as outside the temporal scope of the clause."

In my view, the merits of the government's arguments depend on facts that should be determined after an evidentiary hearing. The majority assumes that it would have been clear to law enforcement that the lower hard drive only contained materials created before September 2018, but that is a question of fact that we cannot resolve in the first instance. The reasonableness of the search also depends on a number of other factors that are not fully developed on the record before us, including the standard procedures used by law enforcement to conduct digital forensic searches as of February 2020; the actual protocol, if any, employed during the search; the extent to which the video thumbnails resembled the surveillance footage of J.J.; and whether the file dates and metadata were readily ascertainable by law enforcement. *See United States v. Hurd*, 499 F.3d 963, 966

(9th Cir. 2007) ("Whether a search exceeds the scope of a search warrant is an issue we determine through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search.") (cleaned up).

Whether law enforcement conducted the search pursuant to the lawful provisions of the warrant is a threshold inquiry that also impacts the analysis of the good faith exception and plain view doctrine. *See United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978) ("Where evidence is uncovered during a search pursuant to a warrant, the threshold question must be whether the search was confined to the warrant's terms…[i]t must not be a general exploratory search.") (cleaned up). If, while searching for additional surveillance videos, officers saw a thumbnail that appeared to depict evidence related to J.J.'s allegations, they could validly review the video to determine whether it was responsive to the warrant. *See United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("[A]ll items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search."); *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) ("The government should not be required to trust the suspect's self-labeling when executing a warrant."). Alternatively, the good faith exception could apply if officers conducted the search in objectively reasonable reliance on the lawful provisions of the warrant. *See United States v. Leon*, 468 U.S. 897, 918 n. 19 (1984) ("Our discussion of the deterrent effect of excluding evidence obtained in reasonable reliance on a subsequently invalidated warrant assumes, of course, that the officers properly executed the warrant and searched only those

places and for those objects that it was reasonable to believe were covered by the warrant."); *see also United States v. Hill*, 459 F.3d 966 (9th Cir. 2006) (upholding a broad search of electronic devices), *Adjani*, 452 F.3d at 1140 (same). Finally, the applicability of the plain view doctrine depends on a factual determination of whether law enforcement was "lawfully searching the area where the evidence is found," which is disputed by the parties. *United States v. Stafford*, 416 F.3d 1068, 1076 (9th Cir. 2005).

Because the record is not clear enough for us to make the necessary findings of fact in the first instance, I would remand to the district court to determine whether the videos were permissibly seized pursuant to a lawful provision in the warrant. *See United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994) ("We remand to the district court the limited question of what evidence was obtained under the overbroad portion of the warrant and direct the suppression of that evidence.").