FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. CARSTEN IGOR ROSENOW, AKA Carlos Senta, *Defendant-Appellant.*	No. 20-50052 D.C. No. 3:17-cr-03430-WQH-1 ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the Southern District of California
William Q. Hayes, District Judge, Presiding

Argued and Submitted June 8, 2021
Pasadena, California

Filed April 27, 2022
Amended October 3, 2022

Before: Susan P. Graber, Consuelo M. Callahan, and Danielle J. Forrest, Circuit Judges.

Order;
Opinion by Judge Forrest;
Dissent by Judge Graber

SUMMARY*

Criminal Law

The panel amended its Opinion filed April 27, 2022, affirming a conviction and sentence on one count of attempted sexual exploitation of a child, 18 U.S.C. § 2251(c), and one count of possession of sexually explicit images of children, 18 U.S.C. § 2252(a)(4)(B), in a case in which the defendant was arrested returning from the Philippines where he engaged in sex tourism involving minors.

The defendant arranged these illegal activities through online messaging services provided by electronic service providers (ESPs) Yahoo and Facebook. His participation in foreign child sex tourism was initially discovered after Yahoo investigated numerous user accounts that Yahoo suspected were involved in child exploitation.

The defendant argued that the evidence seized from his electrical devices upon his arrest should have been suppressed because Yahoo and Facebook were acting as government agents when they searched his online accounts. The panel rejected the defendant's arguments (1) that two federal statutes—the Stored Communications Act and the Protect Our Children Act—transformed the ESPs' searches into governmental action, and (2) that the government was sufficiently involved in the ESPs' searches of the defendant's accounts to trigger Fourth Amendment protection.

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

The defendant argued that the government's requests pursuant to 18 U.S.C. § 2703(f) directing Yahoo and Facebook to preserve records related to his private communications were an unconstitutional seizure of his property and, as a result, the evidence used to convict him was improperly obtained and his convictions should be reversed. The panel declined to reach the question of whether these preservation requests implicate the Fourth Amendment, because even assuming that they do, there is no basis for suppression given that the record establishes that the ESPs' preservation of the defendant's digital data had *no* effect on the government's ability to obtain the evidence that convicted him.

The defendant argued that because subpoenas to Facebook for the defendant's basic subscriber and IP information under 18 U.S.C. § 2703(c)(2) were issued without a warrant supported by probable cause, they were unconstitutional searches. The panel rejected this argument because the defendant did not have a legitimate expectation of privacy in the limited digital data sought in the government's subpoenas, given that the subpoenas did not request any communication content from the defendant's accounts and the government did not receive any such content in response to the subpoenas.

The defendant argued that the government's search warrant affidavit failed to establish probable cause because it did not include any images of child pornography or any reasonable factual descriptions of such images. Rejecting this argument, the panel concluded that the affidavit—which described Yahoo's internal investigation and the resulting findings, as well as the information Facebook provided to the National Center for Missing and Exploited Children after searching the defendant's accounts—established a fair

probability that child pornography would be found on the defendant's electronic devices.

The defendant argued that the jury was not properly instructed on the § 2251(c) count—attempted sexual exploitation of a child—because the instruction did not state that the "purpose" element of § 2251(c) was satisfied only if the government proved that he would not have acted *but for* his desire to produce a visual depiction of the sexually-explicit conduct. The panel saw no basis to conclude that "purpose," as used in § 2251(c), has a causal or results requirement.

The defendant, who was convicted of a single count of possession of child pornography involving the exploitation of several child victims, argued that the district court improperly sentenced him as if he had been convicted on multiple possession counts. The district court increased his base offense level pursuant to the Sentencing Guidelines' multiple-count instruction set forth in U.S.S.G. §§ 2G2.1(d)(1), 2G2.2(c)(1), which applies where more than one minor is exploited in an offense in which the defendant caused a minor to engage in sexually explicit conduct for the purpose of producing child pornography. Distinguishing *United States v. Chilaca*, 909 F.3d 289 (9th Cir. 2018), the panel wrote that there was no impermissible double counting here, as the enhancements were premised on separate exploitative acts.

In an amended partial dissent, Judge Graber parted ways with the majority only as to the question whether, in conducting its searches of the defendant's chat messages, Yahoo was acting as an instrument or agent of the government. Judge Graber applied the two-part test set forth in *United States v. Young*, 153 F.3d 1079 (9th Cir. 1998) (per

curiam). As to the first prong, she wrote that the government knew of and acquiesced in Yahoo's intrusive conduct, and she rejected the suggestion that this prong would be met only if Yahoo's conduct had been illegal. As to the second prong, she wrote that Yahoo's motivation to conduct the searches was intertwined with, and dependent on, the government's enforcement of criminal laws.

COUNSEL

Timothy A. Scott (argued), Nicolas O. Jimenez, and Marcus S. Bourassa, McKenzie Scott APC, San Diego, California, for Defendant-Appellant.

Mark R. Rehe (argued), Assistant United States Attorney; Daniel E. Zipp, Chief, Appellate Section, Criminal Division; Randy S. Grossman, United States Attorney; United States Attorney's Office, San Diego, California; for Plaintiff-Appellee.

Gregory L. Doll and Jamie O. Kendall, Doll Amir & Eley LLP, Los Angeles, California, for Amicus Curiae Oath Holdings Inc.

Mahesha P. Subbaraman, Subbaraman PLLC, Minneapolis, Minnesota, for Amicus Curiae Restore the Fourth, Inc.

ORDER

The Opinion filed on April 27, 2022, is amended as follows:

On slip opinion page 11	Delete <July> and insert <June>.
On slip opinion page 21	Delete <necessarily>.
On slip opinion page 28	Delete <on three separate occasions> and insert <and Facebook>.
On slip opinion page 28	After <Rosenow contends that these requests were an unconstitutional seizure of his property.> insert < and, as a result, the evidence used to convict him was improperly obtained and his convictions should be reversed. We decline to reach the question of whether these preservation requests implicate the Fourth Amendment because, even assuming that they do, there is no basis for suppression.>.
On slip opinion page 29	Delete <A "seizure" of property requires "some meaningful interference [by the government,] with an individual's possessory interests in [his] property." *Jacobsen*, 466 U.S. at 113. Here, the preservation requests themselves, which applied only retrospectively, did not meaningfully

	interfere with Rosenow's possessory interests in his digital data because they did not prevent Rosenow from accessing his account. Nor did they provide the government with access to any of Rosenow's digital information without further legal process. It also is worth noting that Rosenow consented to the ESPs honoring preservation requests from law enforcement under the ESPs' terms of use. Thus, we agree with the district court that these requests did not amount to an unreasonable seizure in violation of the Fourth Amendment.>.
On slip opinion page 29	Insert <A Fourth Amendment violation requires suppression of evidence only if the violation is the "but-for" cause of the government obtaining the evidence. *See Hudson v. Michigan*, 547 U.S. 586, 592 (2006) (explaining "but-for causality" is a necessary condition for suppression of evidence). Here, the record does not establish (and Rosenow does not argue on appeal), that without the challenged preservation requests, the government would not have discovered the child pornography videos and images used to convict him. These videos and images were found on external hard drives, thumb drives, and micro-SD cards in Rosenow's possession when he was arrested in June 2017—they were not found through Yahoo's or Facebook's preserved copies of his digital data. And the warrant under which this evidence was seized from Rosenow was based almost exclusively on

	information disclosed through CyberTips from the NCMEC. Additionally, there is no evidence in the record indicating that the government ever received any preserved copies of Rosenow's digital data from Yahoo. And although Facebook did produce Rosenow's digital data in response to a separate warrant, it was the month after Rosenow was arrested and searched upon returning from the Philippines. Given this timeline of events, any data that the government received from Facebook following issuance of a preservation request could not have resulted in the evidence that was previously obtained from Rosenow. Moreover, Rosenow has not demonstrated that the data that Facebook ultimately produced to the government came from a copy of his data maintained in response to a preservation request or that Rosenow deleted any of the information in his account such that it only could have come from a preserved copy. Accordingly, the record establishes that the ESPs' preservation of Rosenow's digital data had *no* effect on the government's ability to obtain the evidence that convicted him. And because Rosenow cannot show a causal connection to the government's preservation requests that would warrant suppression, we decline to reach the merits of his constitutional challenge to those requests>.

On slip opinion page 29	After <come from a preserved copy.> insert Footnote 7, stating <A panel of this court recently made a similar point in an unpublished disposition denying suppression based on a preservation request made to Facebook under 18 U.S.C. § 2703(f) for lack of causation. *See United States v. Perez*, 798 F. App'x 124, 126 (9th Cir. 2020) (unpublished), *cert. denied*, 141 S. Ct. 425 (2020) ("The mere fact that a preservation request was made and granted does not in and of itself show that Facebook responded to the Government's subsequent search warrant with data from the preservation request, instead of simply creating a contemporaneous, new copy of the Facebook account at the time of the search warrant.").>.

The Petitions for Rehearing and Rehearing En Banc are otherwise **DENIED**, and no further petitions for rehearing will be accepted.

OPINION

FORREST, Circuit Judge:

Defendant Carsten Rosenow was arrested returning from the Philippines, where he engaged in sex tourism involving minors. Rosenow arranged these illegal activities through online messaging services provided by Yahoo and Facebook, and his participation in foreign child sex tourism was initially discovered after Yahoo investigated numerous user accounts that Yahoo suspected were involved in child sexual exploitation. Following a jury trial, Rosenow was

convicted on one count of attempted sexual exploitation of a child, 18 U.S.C. § 2251(c), and one count of possession of sexually explicit images of children, 18 U.S.C. § 2252(a)(4)(B).

On appeal, Rosenow argues that the evidence seized from his electronic devices upon his arrest should have been suppressed because, among other reasons, Yahoo and Facebook (which also searched his accounts on its platform) were government actors when they investigated his accounts without a warrant and reported the evidence of child sexual exploitation that they found to the National Center for Missing and Exploited Children (NCMEC), in supposed violation of Rosenow's Fourth Amendment rights. He further argues that the district court improperly instructed the jury on the required mental state for his sexual exploitation charge and miscalculated the sentence on his possession charge. We have jurisdiction under 28 U.S.C. § 1291, and we affirm Rosenow's conviction and sentence.

I. BACKGROUND

A. Electronic Communication Services and Mandatory Reporting

Yahoo and Facebook are electronic communication service providers (ESPs) that provide online private messaging services. These services allow users to share instant messages, images, and videos that only the sender and recipient can see. Both companies have policies governing user privacy.

Yahoo's privacy policy during the relevant period stated that Yahoo "stores all communications content" and reserves the right to share that information "to investigate, prevent, or take action regarding illegal activities . . . , violations of

Yahoo's terms of use, or as otherwise required by law." Yahoo's internal practice was to terminate or suspend user accounts that contained child pornography images or videos, but communication about child pornography unaccompanied by offending images did not trigger these actions. During the events of this case, Yahoo Messenger, the specific service that Rosenow used, did not transmit "photographs or videos or other files shared between two users" over Yahoo's servers, so Yahoo did not store them.

Facebook's privacy policy likewise stated that it has the right to "access, preserve and share information when [it] ha[s] a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity." And it was Facebook's internal policy to search users' accounts anytime it received legal process indicating a "child safety" concern or suggesting that child exploitation materials might exist on its platform. If Facebook found content violating its terms of use, including child pornography, it performed a more extensive investigation and took "appropriate action . . . including removing the offending content or disabling the account."

The Protect Our Children Act of 2008 requires ESPs to report "any facts or circumstances from which there is an apparent violation of" specified criminal offenses involving child pornography. 18 U.S.C. § 2258A(a)(1)–(2). ESPs report to the NCMEC, a non-profit organization that is statutorily required to operate the "CyberTipline," which is an online tool that gives ESPs "an effective means of reporting internet-related child sexual exploitation." 34 U.S.C. § 11293; *see* 18 U.S.C. § 2258A(a)(1). NCMEC is required to make every "CyberTip" it receives available to federal law enforcement. 18 U.S.C. § 2258A(c)(1). ESPs that fail to report "apparent violation[s]" of the specified

criminal statutes involving child pornography face substantial fines. *Id.* § 2258A(a)(1), (e).

B. Yahoo's Investigation and CyberTips

In September 2014, an online international money transfer company filed CyberTips and told Yahoo about ten Yahoo users who were selling child pornography produced in the Philippines. Yahoo connected those accounts to over a hundred other Yahoo user accounts selling child pornography and live-streaming sex acts with children in the Philippines. The following month, Yahoo filed a supplemental CyberTip report with the NCMEC and notified the FBI and Homeland Security Investigations (Homeland Security) about its report. Yahoo took the additional step of contacting law enforcement because it had determined "that there were children that were being actively exploited, and there were some users that seemed to be engaged in travelling to abused children or other types of activity like this that had some exigency" and Yahoo "wanted to be sure that law enforcement was aware that there were these children in danger and would be able to prioritize [Yahoo's] report over the other thousands of reports that [the government] might have received during that time period." That same month, Yahoo also met with the FBI and Homeland Security at the NCMEC to discuss Yahoo's internal investigation. Yahoo disclosed additional information regarding its suspicious users' accounts. The FBI's Major Case Coordination Unit (MCCU) subsequently opened its own investigation, "Operation Swift Traveler," to investigate Yahoo's evidence.

Yahoo remained suspicious that there were additional users involved in the criminal scheme it was uncovering. Continuing its own internal investigations, Yahoo later identified several hundred additional users who were selling

or buying child-exploitation content from the Philippines. Rosenow was one of the users identified in these efforts. Yahoo determined that Rosenow was a buyer who regularly communicated with sellers about his child sex tourism in the Philippines. In December 2014, Yahoo filed another CyberTip and arranged a second meeting with federal authorities to discuss its continued internal investigation. In December 2014 (and March 2015, and June 2015), the FBI requested that Yahoo preserve the communications of its users (including Rosenow) who were associated with Operation Swift Traveler.[1]

After filing its December 2014 CyberTip, Yahoo learned that Homeland Security had arrested a prolific buyer of child pornography through Operation Swift Traveler and did not intend to conduct any further investigations. Concerned that "a rather large portion of the Philippine webcam and sex trafficking activity" had been missed, Yahoo conducted further internal investigations of the arrested buyer's texts with sellers in the Philippines, and consequently discovered more conversations between the sellers and Rosenow. In these conversations, Rosenow repeatedly asked for pictures of children whom he was arranging to meet for sex in the Philippines. In some communications, he requested, and appears to have received, lewd pictures from an adolescent Filipina girl. Yahoo filed a CyberTip in December 2015 based on its additional information about Rosenow and other users, and it met with the FBI at the NCMEC again in February 2016 to discuss its recent internal investigations.

[1] Under the Stored Communications Act, an ESP, upon receiving a preservation request, "shall take all necessary steps to preserve records and other evidence in its possession" for up to 180 days "pending the issuance of a court order or other process." 18 U.S.C. § 2703(f).

C. FBI Agent Cashman's Investigation and Facebook's CyberTips

In early 2015, the FBI's MCCU sent a lead about Rosenow to Agent Colleen Cashman in the FBI's San Diego office. Between March 2015 and January 2017, Agent Cashman received Yahoo's initial CyberTips, but she did not receive the December 2015 CyberTip. At some point before January 2017, the FBI applied for a search warrant for Rosenow's Yahoo account, but the U.S. Attorney's Office stated that the basis for probable cause from Yahoo's earlier CyberTips "had become dated or stale."

In January 2017, the MCCU sent Agent Cashman Yahoo's December 2015 CyberTip, which renewed her investigation. Agent Cashman learned that Rosenow had a Facebook account under a different name, and she sent preservation requests to Facebook in January and May 2017 through its Law Enforcement Online Request System (LEORS). In March and June 2017, she filed administrative subpoenas through LEORS for Rosenow's "[b]asic subscriber information and IP log-in information" for both of his user accounts and indicated that the case involved "child safety." Because Facebook automatically reviewed user accounts whenever a LEORS request indicated a "child safety" concern or suggested that child exploitation materials might exist, Agent Cashman's subpoenas triggered Facebook's review of Rosenow's account activity, including his "messages, timelines, photos, IP addresses, and machine cookies." Facebook discovered child-exploitation content that violated its terms of use, immediately disabled Rosenow's accounts, and filed two CyberTips with NCMEC.

NCMEC promptly forwarded Facebook's CyberTips to Agent Cashman. The CyberTips showed that Rosenow had

sent three files that Facebook classified as "child pornography" and provided excerpts from Rosenow's conversations negotiating sex acts with three underage girls in the Philippines. He told one girl that he wanted to video their encounter, and he told another that he loved the nude pictures he had taken of her during a previous encounter. When Agent Cashman submitted her initial subpoena in March 2017, she did not know that it would trigger Facebook's automatic internal searches. But she acknowledges that, because she submitted this subpoena, she received information from NCMEC about Rosenow's Facebook account that she could not otherwise have obtained without a warrant.[2]

In June 2017, Agent Cashman prepared affidavits seeking search warrants for Rosenow's person, baggage, and home, relying almost exclusively on evidence in Yahoo's and Facebook's CyberTips. The warrants sought evidence of child pornography offenses and child sex tourism. Two days later, with a search warrant in hand, the FBI arrested Rosenow when he returned from a trip to the Philippines. The FBI's searches of Rosenow's electronic devices revealed significant child pornography, including numerous videos of Rosenow himself performing sex acts on prepubescent Filipina girls ranging from approximately 10 to 15 years old.

[2] Agent Cashman's second subpoena issued to Facebook in June 2017 related to a different user account that Rosenow did not use for his illicit activities. This subpoena did not lead Facebook to file any additional CyberTips.

D. District Court Proceedings

Rosenow was indicted for attempted sexual exploitation of a child, 18 U.S.C. § 2251(c), possession of sexually explicit images of children, 18 U.S.C. § 2252(a)(4)(B), and travel with intent to engage in illicit sexual conduct, 18 U.S.C. § 2423(b). Rosenow moved to suppress all the evidence obtained from Yahoo's and Facebook's searches of his private online communications, arguing that the companies "searched at the government's behest" and, therefore, their conduct was government action that violated the Fourth Amendment's warrant requirement. Additionally, Rosenow claimed that the government's preservation orders and subpoenas were unlawful warrantless seizures under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and that the warrant used to search and seize his property was based on information obtained in illegal searches and lacked probable cause.

After a two-day evidentiary hearing, the district court denied his motions. The court concluded that Yahoo and Facebook both acted independently in investigating Rosenow "pursuant to legitimate business purposes" of excluding users involved in child abuse and exploitation and that the companies' compliance with the mandatory reporting statute did not convert them into government actors. As to the preservation orders, the court found no Fourth Amendment violation because they "did not interfere with [Rosenow]'s use of his accounts and did not entitle the [g]overnment to obtain any information without further legal process." The court similarly found no Fourth Amendment violation for the administrative subpoenas, concluding that, "[u]nlike the location information in *Carpenter*," Rosenow "had no reasonable expectation of privacy in the subscriber information and the IP log-in information [he] voluntarily

provided to [Facebook] in order to establish and maintain his account." Finally, the court concluded that the facts set forth in the search warrant affidavit were sufficient to support probable cause that evidence of child pornography offenses would be found, and Rosenow failed to identify any misrepresentations or material omissions to overcome this finding.

In August 2019, Rosenow's jury trial commenced on the charges of attempted sexual exploitation of a child and possession of sexually explicit images of children. Rosenow stipulated that he knowingly possessed five depictions of child pornography, including two video recordings of himself engaging in sexually explicitly conduct with minor girls. For the attempted exploitation charge, Rosenow requested a jury instruction stating that the "purpose" mental state element required for conviction was satisfied only if the government proved that he "would not have acted *but for* his desire to produce a visual depiction of the sexually-explicit conduct." The district court rejected his proposed instruction and instead instructed the jury that the government had to prove that "producing a visual depiction of a minor engaged in sexually explicit conduct" was Rosenow's "dominant, significant or motivating" purpose, not that it was his "sole purpose." The jury convicted Rosenow on both charges.

At sentencing, Rosenow objected to his Presentence Report's sentencing calculation as multiplicitous, arguing that he was convicted of only one count of possession but would be punished as if he had been convicted of four separate counts, in violation of *United States v. Chilaca*, 909 F.3d 289 (9th Cir. 2018), and the Sixth Amendment. The district court overruled Rosenow's objection and held that the multiple-count calculations were proper. Rosenow was

sentenced to 300 months' imprisonment and lifetime supervised release.

II. DISCUSSION

In reviewing a denial of a motion to suppress, we review the district court's factual findings for clear error and its legal conclusions de novo. *United States v. Vandergroen*, 964 F.3d 876, 879 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1696 (2021). We also review de novo "whether a jury instruction misstates the law," *United States v. Rodriguez*, 971 F.3d 1005, 1012 (9th Cir. 2020), and whether the district court correctly interpreted and applied the Sentencing Guidelines, *United States v. Martinez-Rodriguez*, 472 F.3d 1087, 1094 (9th Cir. 2007).

A. Search and Seizure Issues

1. Were the ESPs an "instrument or agent" of the government?

The Fourth Amendment guarantees the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV. The Fourth Amendment regulates only governmental action; it does not protect against intrusive conduct by private individuals acting in a private capacity. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The Constitution does, however, "constrain[] governmental action by whatever instruments or in whatever modes that action may be taken." *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 392 (1995) (internal quotation marks and citation omitted). Thus, a private search or seizure may implicate the Fourth Amendment where the private party acts "as an agent of the Government or with the participation or knowledge of any governmental official." *Jacobsen*,

466 U.S. at 113 (internal quotation marks and citation omitted).

"A defendant challenging a search conducted by a private party bears the burden of showing the search was governmental action." *United States v. Young*, 153 F.3d 1079, 1080 (9th Cir. 1998) (per curiam). "Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614–15 (1989) (internal quotation marks and citations omitted).

Rosenow argues that the evidence discovered by Yahoo and Facebook was obtained illegally and should be suppressed because they were acting as government agents when they searched his online accounts. His argument is two-fold: (1) two federal statutes—the Stored Communications Act and the Protect Our Children Act—transformed the ESPs' searches into governmental action, and (2) the government was sufficiently involved in the ESPs' searches that they constituted governmental conduct. Each argument fails.

a. Does federal law transform the ESPs' private searches into governmental action?

A federal regulatory scheme that authorizes and encourages private searches may transform a private search into governmental conduct. *Id.* at 614–16. *Skinner* considered a facial challenge to the Federal Railroad Administration's regulations governing employee drug testing by private railroads. *Id*. The regulations mandated drug testing following a "major train accident," but also

permitted railroads to drug-test employees in other specified circumstances. *Id.* at 609–11. The Supreme Court held that the regulations—even those that did not mandate drug testing—implicated the Fourth Amendment because they amounted to governmental "encouragement, endorsement, and participation" in an otherwise private search. *Id.* at 615–16. The Court emphasized that the regulations authorized private railroad companies to perform drug tests, preempted conflicting state laws and collective-bargaining terms, prohibited the railroad companies from contracting away their right to require the tests, required the companies to report certain evidence derived from the tests, and prohibited private employees from refusing to comply with the tests. *Id.* at 615–16. Thus, by removing "all legal barriers to the testing" and making "plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions," the Court held that the Federal Railroad Administration had transformed private searches by private companies into governmental action. *Id.* at 615–16.

Rosenow argues that, like the regulations in *Skinner*, federal regulation of ESP searches and disclosures trigger Fourth Amendment scrutiny because, taken together, the Stored Communications Act authorizes ESPs to conduct warrantless searches, *see* 18 U.S.C. § 2701(c), and the Protect Our Children Act requires private parties to report evidence derived from those searches to a government agent or entity, *see id.* § 2258A.[3] As explained below, Rosenow's argument is unconvincing.

[3] The district court did not address Rosenow's claim that the NCMEC is a governmental agent or entity for Fourth Amendment purposes. There is good reason to think that the NCMEC is, on the face of its authorizing statutes, a governmental entity under Fourth

The Stored Communications Act criminalizes unauthorized searches of stored electronic communications content, 18 U.S.C. § 2701(a)–(b), but expressly excepts ESPs from liability. *Id.* § 2701(c)(1). This exception makes sense; otherwise, ESPs would be unable to ensure that user content does not violate the ESPs' own terms of use. But unlike the regulations at issue in *Skinner*, which explicitly authorized railroads to administer drug and alcohol tests to their employees based on "reasonable suspicion," *Skinner*, 489 U.S. at 611, the Stored Communications Act does not authorize ESPs to do anything more than access information already contained on *their* servers as dictated by their terms of service. *See* 18 U.S.C. § 2701(c); Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212 (2004) ("[E]ven if the Fourth Amendment protects files stored with an [E]SP, the [E]SP can search through all of the stored files on its server and disclose them to the government without violating the Fourth Amendment.").

Additionally, the Protect Our Children Act disclaims any governmental mandate to search: § 2258A(f) provides that this statute "shall [not] be construed to require" an ESP to "monitor" users or their content or "affirmatively search, screen, or scan for" evidence of criminal activity. 18 U.S.C. § 2258A(f). Mandated *reporting* is different than mandated *searching*. Our caselaw is clear that a private actor does not become a government agent simply by complying with a

---

Amendment doctrine. *See United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) ("NCMEC's law enforcement powers extend well beyond those enjoyed by private citizens—and in this way it seems to mark it as a fair candidate for a governmental entity."). For purposes of this case, we assume, without deciding, that the NCMEC is a governmental actor.

mandatory reporting statute. *See Mueller v. Auker*, 700 F.3d 1180, 1191–92 (9th Cir. 2012) ("[Hospital] did not become a state actor simply because it complied with state law requiring its personnel to report possible child neglect to Child Protective Services."); *cf. Ferguson v. City of Charleston*, 532 U.S. 67, 81 (2001) (holding that disclosure by medical professionals of "information that under rules of law or ethics is subject to reporting requirements" does not ordinarily violate the Fourth Amendment). Under both the Stored Communications Act and the Protect Our Children Act, Yahoo and Facebook are free to choose not to search their users' data. Therefore, when they do search, they do so of their own volition.

Moreover, unlike the regulations in *Skinner*, which prohibited railroad companies from contracting away their right to require drug tests, 489 U.S. at 615–16, neither statute at issue here prevents an ESP from contracting away its right to search users' communications. *See United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013). Thus, the statutes do not have the "clear indices of the Government's encouragement, endorsement, and participation" sufficient to implicate the Fourth Amendment. *Skinner,* 489 U.S. at 615–16.

As a final note, persuasive authority also militates against Rosenow's argument: three of our sister circuits have explicitly rejected the analogy of 18 U.S.C. § 2258A to the railroad regulations at issue in *Skinner*. *See United States v. Miller*, 982 F.3d 412, 424 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021); *United States v. Ringland*, 966 F.3d 731, 736 (8th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021); *Stevenson*, 727 F.3d at 830; *United States v. Richardson*, 607 F.3d 357, 364–67 (4th Cir. 2010); *cf. United States v. Meals*, 21 F.4th 903, 907 (5th Cir. 2021)

(rejecting defendant's argument that § 2258A transformed Facebook into a government agent); *United States v. Cameron*, 699 F.3d 621, 636–38 (1st Cir. 2012) (holding that Yahoo's statutory duty under federal law to report to NCMEC "did not impose any obligation to *search* for child pornography," but "merely an obligation to *report* child pornography of which Yahoo[] became aware.").

Those courts compared the railroad regulations only to § 2258A of the Protect Our Children Act, and Rosenow points both to this statute and to the Stored Communications Act.[4] But as explained, the Stored Communications Act does not mandate, encourage, or endorse private searches, and the reasoning of our sister circuits reinforces our conclusion that an ESP's search of its users' communications does not result inevitably from governmental encouragement as opposed to "private initiative." *Skinner*, 489 U.S. at 615.

We hold that federal law did not transform Yahoo's and Facebook's private searches into governmental action.

b. Was there sufficient government involvement in the ESPs' searches to implicate the Fourth Amendment?

Even if federal law does not render searches performed by private actors to be government conduct, a private search still may implicate the Fourth Amendment if there is a "sufficiently close nexus" between the government and the private entity's challenged conduct. *See Jackson v. Metro.*

[4] Rosenow argues for the first time in reply that § 230 of the Communications Decency Act also encourages ESPs to locate and disclose criminal activity to the government. We decline to consider this new argument. *See CTIA-The Wireless Ass'n v. City of Berkeley*, 928 F.3d 832, 850 (9th Cir. 2019).

Edison Co., 419 U.S. 345, 351 (1974). In assessing whether a sufficient nexus exists, "the relevant inquiry is: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends." *See United States v. Cleaveland*, 38 F.3d 1092, 1094 (9th Cir. 1994) (internal quotation marks and citation omitted).

i. Government knowledge and acquiescence

To satisfy the first requirement, the government must be involved in the search "either directly as a participant or indirectly as an encourager of the private citizen's actions." *United States v. Walther*, 652 F.2d 788, 791 (9th Cir. 1981). The government's knowledge of a private search, by itself, does not turn that search into one protected by the Fourth Amendment—were that not the case, the Fourth Amendment's protections would cover a significant amount of private conduct of which the government was simply aware. Likewise, "[m]ere governmental authorization of a particular type of private search in the absence of more active participation or encouragement" does not trigger Fourth Amendment protection. *Id.* at 792; *see also Flagg Bros., Inc. v. Brooks*, 436 U.S. 149, 164 (1978) ("[M]ere acquiescence in a private action" does not transform a private actor into a government agent); *Cameron*, 699 F.3d at 637 ("We will not find that a private party has acted as an agent of the government simply because the government has a stake in the outcome of a search." (internal quotation marks and citation omitted)). Nor do "de minimis or incidental contacts" between the government and a private entity. *Walther*, 652 F.2d at 791.

Here, the FBI knew about Yahoo's ongoing internal investigations into the use of its platform for sexual

exploitation of children in the Philippines, but, as the district court found, there is no evidence that "law enforcement was involved in or participated" in Yahoo's investigations or that "law enforcement sought or received any assistance from Yahoo's personnel in conducting its investigation outside of legal process." Yahoo's conduct was permissible, and it did not need approval from law enforcement to search Rosenow's account and share any content it found that evidenced criminal activity. Yahoo had a contractual right under the terms of its privacy policy, to which Rosenow agreed, "to investigate, prevent, or take action regarding illegal activities" or "violations of Yahoo's terms of use." *See Cleaveland*, 38 F.3d at 1093–94 (finding insufficient governmental action because the private entity had the authority to search customer property under a customer service agreement); *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982).

Nor was this a situation in which Yahoo was spurred into investigating Rosenow by the government or in which the government incentivized, directed, or encouraged Yahoo to continue its investigatory efforts after Yahoo initially informed law enforcement about its concerns related to some of its users. Quite the opposite. The record shows that Yahoo initiated its investigation due to information that it received from another private company. And it continued in its efforts primarily, if not entirely, because it was concerned that the government might drop the ball and not take sufficient action to address the ongoing sexual exploitation of children that Yahoo had uncovered.

For its part, Facebook was not independently proactive in searching Rosenow's accounts in the same way that Yahoo was, but it nonetheless acted volitionally when it conducted its searches. As the district court found, the FBI

issued a preservation request stating that it had "child safety" concerns related to Rosenow's account, but it "did not request that Facebook conduct any search or initiate any internal investigation into Rosenow's accounts." Rather, Facebook's internal policies required it to review Rosenow's accounts for inappropriate material because Facebook had received notice from law enforcement that conduct threatening child safety could be occurring in Rosenow's accounts. The government's preservation request triggered Facebook's internal investigation policy, but Facebook independently chose to search Rosenow's accounts and take corrective action after discovering content that violated its terms of use. Accordingly, we conclude that the government's involvement with Yahoo's and Facebook's internal searches "was not so extensive as to trigger Fourth Amendment scrutiny." *Cleaveland*, 38 F.3d at 1094.

The dissent notes that the government did nothing to discourage Yahoo's internal searches and subsequent reports. True, but that is immaterial here. The Fourth Amendment does not require government officials to discourage private actors from conducting searches that they have a legal basis to perform. *Compare id.* ("There was no reason why the detective should have restrained [the employee] or discouraged him in his search because [the employee] never exceeded his authority under the Customer Service Agreement to go on to the property and inspect the meter." (cleaned up)); *Miller*, 688 F.2d at 657 ("Because [private actor] had not proposed to do anything illegal, we see no reason why the officers should have restrained him or discouraged him from visiting [suspect's] property.") *with Walther*, 652 F.2d at 793 & n.2 (finding acquiescence where the government did not discourage an informant from actively engaging in *illegal* searches with the expectation of a reward); *United States v. Reed*, 15 F.3d 928, 932 (9th Cir.

1994) (finding acquiescence where the government "made no attempt to discourage" a hotel owner from searching "beyond what was required to protect hotel property.").

The constitution limits the *government*. Nothing in our precedent establishes that a private party becomes a government actor simply because the government knows about and does not prevent such party from engaging in legally permissible conduct. This is particularly true where government actors are not even present during the search. *Cf. Cleaveland*, 38 F.3d at 1094; *Reed*, 15 F.3d at 932 (noting the significance of a "legitimate motive" for "private searches done *in the presence of police officers*" (emphasis added)). In the circumstances presented here, the government simply was not a "participant" or an "encourager" of the ESPs' private conduct. *Walther*, 652 F.2d at 791. In so holding, we do not suggest that government knowledge and acquiescence is established only if a private party's conduct is illegal. We emphasize only that unless a private party's search is illegal or based on an illegitimate motive, our precedent requires "*active participation or encouragement*" by the government before state action will be found. *Id.* at 792 (emphasis added).

ii. Private party's intent

In analyzing the second requirement—the private party's intent in searching—we look to whether it acted to "assist law enforcement efforts," or whether it had a "legitimate, independent motivation to further its own ends." *Cleaveland*, 38 F.3d at 1094 (internal quotation marks and citation omitted). Under our precedent, a private party's interest in preventing criminal activity, on its own, is not a legitimate, independent motivation to search. *Reed*, 15 F.3d at 932 ("[I]f crime prevention could be an independent private motive, searches by private parties would never

trigger Fourth Amendment protection."); *but see Cameron*, 699 F.3d at 638 ("It is certainly the case that combating child pornography is a government interest. However, this does not mean that Yahoo cannot voluntarily choose to have the same interest."). However, as long as a legitimate, independent motivation is established, "that motivation is not negated by any dual motive to detect or prevent crime or assist the police, or by the presence of the police nearby during the search." *Cleaveland*, 38 F.3d at 1094.

Here, the record establishes that Yahoo and Facebook investigated Rosenow's accounts to further their own legitimate, independent motivations. *See Young*, 153 F.3d at 1080–81. As the district court found, both companies have legitimate business reasons for purging child pornography and exploitation from their platforms, and they acted in furtherance of those reasons when they investigated Rosenow. Yahoo's Director of Threat Investigations and Intelligence testified that it is "very bad for [Yahoo's] brand" if its services are viewed as "a haven for child pornography or child exploitation or sex trafficking." He also stated that "[r]idding our products and services of child abuse images is critically important to protecting our users, our products, our brand, and our business interests." Finally, he stated that Yahoo has a direct financial interest in keeping child pornography off its platforms because Yahoo does not want to lose advertising opportunities or be blocked from app stores.

A Facebook analyst familiar with that company's internal search policies likewise explained that Facebook "has a business purpose in keeping its platform safe and free from harmful content and conduct . . . that sexually exploits children," which is why Facebook prohibits "content that sexually exploits or endangers children." She testified that

Facebook's policy of conducting limited review of accounts in cases indicating child exploitation is "to keep [its] platform safe and so users will continue to use [its] platform."

This case is analogous to *Cleaveland*, where police waited while an electricity company's employee investigated the meter of a customer that was suspected of diverting power. 38 F.3d at 1093–94. The employee asked the police to accompany him to the customer's home because of safety concerns and, "if his inspection uncovered the likelihood of a power diversion, he wanted the police to be able to get a warrant to search the house to confirm the power theft." *Id.* at 1093. Although the police used evidence from the company's search to obtain a warrant, we found insufficient government action to implicate the Fourth Amendment because, in part, the motive "to recover money for [the electricity company's] loss of power" was a "legitimate, independent motive apart from" any interest in "assist[ing] the police in capturing the power thief." *Id.* at 1094.

So, too, the ESPs' desire to purge child pornography from their platforms and enforce the terms of their user agreements is a legitimate, independent motive apart from any interest that the ESPs had in assisting the government in apprehending Rosenow. In so holding, we again note that our decision is consistent with each of our sister circuits to have considered this issue. *See Miller*, 982 F.3d at 419 ("Companies like Google have business reasons to make these efforts to remove child pornography from their systems."); *Ringland,* 966 F.3d at 736 ("Google did not act as a government agent because it scanned its users' emails volitionally and out of its own private business interests. Google did not become a government agent merely because

it had a mutual interest in eradicating child pornography from its platform."); *Cameron*, 699 F.3d at 638.

The dissent argues that Yahoo did not have an *independent* motivation for searching Rosenow's account because, by failing to preserve images sent via its Messenger service, Yahoo could not close the account under its user agreement and, therefore, depended on law enforcement to further its interests. Dissent at 45–47. We disagree.

First, it was not a foregone conclusion at the outset of Yahoo's search that it would not find any images that would permit it to close Rosenow's account without law enforcement involvement. While Yahoo did not retain images sent through its Messenger service during the relevant period, it did retain its users' Messenger profile pictures and images sent by users through its email service. Yahoo's searches included these locations where images were retained. In fact, during the search activity that identified Rosenow, Yahoo found prohibited child-exploitation images in other users' email accounts and Messenger profile pictures, and it disabled those users' accounts without any involvement by law enforcement.

Second, a private party's otherwise legitimate, independent motivation is not rendered invalid just because law enforcement assistance may further its interests.[5]

[5] In arguing otherwise, the dissent relies primarily on *Ferguson*, 532 U.S. at 82–84. However, *Ferguson* concerned warrantless searches by state actors under the "special needs" exception to the warrant requirement. There, a state hospital adopted a "Management of Drug Abuse During Pregnancy" policy and attempted "to use the threat of arrest and prosecution in order to force women into [substance abuse] treatment." *Id.* at 71–72, 84. Law enforcement had "extensive involvement" in developing the policy. *Id.* at 84. Of course, under such

Cleaveland demonstrates this point. While the electric company had a legitimate business interest in preventing power theft, it specifically requested that law enforcement be present when it inspected its customer's meter in part because it "wanted the police to be able to get a warrant and search the house to *confirm* the power theft." 38 F.3d at 1093 (emphasis added). This suggests that further action beyond its inspection of the meter was needed to either prevent further theft, recover against the customer, or both. Had the electric company been able to accomplish its business objective without assistance, it would not have needed law enforcement at the ready to get a warrant and search the customer's home. Likewise, in *Miller* the private actor had an independent interest in recovering his stolen trailer, but he relied on law enforcement to act after he entered the defendant's property and located his trailer.[6] 688 F.2d at 657–58.

Our conclusion is also consistent with *Reed* because there the hotel owner expressly admitted that his *only*

---

circumstances, *the state* may not rely on the "ultimate goal" of substance abuse treatment to justify warrantless searches. But *Ferguson* is flatly distinguishable from this case where a private actor is searching its own platform consistent with the terms of its user contract.

[6] Even if were we to accept the dissent's position that reliance on government assistance invalidates an otherwise legitimate, independent motivation, law enforcement intervention was not Yahoo's only available means for preventing Rosenow from continuing to engage in prohibited conduct. Yahoo's Director of Threat Investigations and Intelligence testified that the company has several ways to prevent child exploitation on its platform: deactivating accounts; making law enforcement referrals for arrests; and pursuing civil remedies, including lawsuits and "direct requests that [it] serve[s] via process servers to get people to stop engaging in activities." Thus, Yahoo was not dependent on the government to further its goals.

motivation for searching the defendant's room was to "help police gather proof that [the defendant] was using his room to deal narcotics." 15 F.3d at 931. Unlike in *Cleaveland* and *Miller*, the hotel owner had no independent motivation for searching his customer's room. However, in invalidating the search in that case, we indicated that if the hotel owner had entered the room for an independent purpose—such as ensuring that hotel property had not been damaged—and had not searched "beyond what was required to protect hotel property," the search may not have been improper. *See id.* at 931.

For these reasons, we conclude that there was insufficient governmental involvement in Yahoo's and Facebook's private searches of Rosenow's accounts to trigger Fourth Amendment protection.

2. Did the government's preservation requests and subpoenas violate Rosenow's right to privacy?

Rosenow also argues that he had a right to privacy in his digital data and that the government's preservation requests and subpoenas, submitted without a warrant, violated the Fourth Amendment. We disagree.

a. Were the preservation requests unconstitutional seizures?

Acting pursuant to 18 U.S.C. § 2703(f), which requires an ESP "to preserve records and other evidence in its possession pending the issuance of a court order or other process," the government directed Yahoo and Facebook to preserve records related to Rosenow's private communications. Rosenow contends that these requests were an unconstitutional seizure of his property and, as a result, the evidence used to convict him was improperly

obtained and his convictions should be reversed. We decline to reach the question of whether these preservation requests implicate the Fourth Amendment because, even assuming that they do, there is no basis for suppression.

A Fourth Amendment violation requires suppression of evidence only if the violation is the "but-for" cause of the government obtaining the evidence. *See Hudson v. Michigan*, 547 U.S. 586, 592 (2006) (explaining "but-for causality" is a necessary condition for suppression of evidence). Here, the record does not establish (and Rosenow does not argue on appeal), that without the challenged preservation requests, the government would not have discovered the child pornography videos and images used to convict him. These videos and images were found on external hard drives, thumb drives, and micro-SD cards in Rosenow's possession when he was arrested in June 2017—they were not found through Yahoo's or Facebook's preserved copies of his digital data. And the warrant under which this evidence was seized from Rosenow was based almost exclusively on information disclosed through CyberTips from the NCMEC.

Additionally, there is no evidence in the record indicating that the government ever received any preserved copies of Rosenow's digital data from Yahoo. And although Facebook did produce Rosenow's digital data in response to a separate warrant, it was the month after Rosenow was arrested and searched upon returning from the Philippines. Given this timeline of events, any data that the government received from Facebook following issuance of a preservation request could not have resulted in the evidence that was previously obtained from Rosenow. Moreover, Rosenow has not demonstrated that the data that Facebook ultimately produced to the government came from a copy of

his data maintained in response to a preservation request or that Rosenow deleted any of the information in his account such that it only could have come from a preserved copy.[7]

Accordingly, the record establishes that the ESPs' preservation of Rosenow's digital data had *no* effect on the government's ability to obtain the evidence that convicted him. And because Rosenow cannot show a causal connection to the government's preservation requests that would warrant suppression, we decline to reach the merits of his constitutional challenge to those requests.

b. Was the subpoena an unconstitutional search?

In addition to the preservation requests, the government issued subpoenas to Facebook for Rosenow's basic subscriber and IP information under 18 U.S.C. § 2703(c)(2). Relying on *Carpenter*, Rosenow contends that, because these subpoenas were issued without a warrant supported by probable cause, they were unconstitutional searches.

In addition to cabining "physical[] intru[sions] on a constitutionally protected area," the Fourth Amendment protects "certain expectations of privacy." *Carpenter*, 138 S. Ct. at 2213 (internal quotation marks and citation omitted). "When an individual seeks to preserve something as private,

[7] A panel of this court recently made a similar point in an unpublished disposition denying suppression based on a preservation request made to Facebook under 18 U.S.C. § 2703(f) for lack of causation. *See United States v. Perez*, 798 F. App'x 124, 126 (9th Cir. 2020) (unpublished), *cert. denied*, 141 S. Ct. 425 (2020) ("The mere fact that a preservation request was made and granted does not in and of itself show that Facebook responded to the Government's subsequent search warrant with data from the preservation request, instead of simply creating a contemporaneous, new copy of the Facebook account at the time of the search warrant.").

and his expectation of privacy is one that society is prepared to recognize as reasonable, we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Id.* (internal quotation marks and citation omitted). However, in what is commonly referred to as the third-party doctrine, the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (holding that the defendant had no reasonable expectation of privacy in the phone numbers he dialed from his home phone because he necessarily shared those numbers with the phone company to make a call); *see United States v. Miller*, 425 U.S. 435, 440–442 (1976) (holding that the defendant had no reasonable expectation of privacy in his banking business records because he voluntarily shared that information with the bank).

In *Carpenter*, the Court declined to extend *Smith* and *Miller* to a warrantless subpoena of cell phone site records, which revealed the defendant's location over the course of 127 days whenever he used his cell phone. 138 S. Ct. at 2212–14, 2217. Instead, the Court held that the subpoena seeking this information required a warrant, explaining that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell phone surveillance technology]" even if that information is shared with third parties. *Id.* at 2217. Recognizing the intersection between the third-party doctrine and a separate line of cases addressing a person's expectation of privacy in physical location and movements, the Court established that, "in the rare case where the suspect has a legitimate privacy interest in records held by a third party," the government must obtain a warrant before issuing

a subpoena absent exigent circumstances. *Id.* at 2215–16, 2222–23. Rosenow argues that, under *Carpenter*, the government's subpoenas directing Facebook to disclose his basic subscriber and log-in information violated the Fourth Amendment because he has a legitimate expectation of privacy in this digital data.[8]

But *Carpenter* is distinguishable.[9] Unlike cell-site location, which implicates a long line of precedent recognizing a defendant's reasonable "expectation of privacy in his physical location and movements," *id.* at 2215, a defendant "ha[s] no expectation of privacy in . . . IP addresses" or basic subscriber information because internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information," *United States. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *see also United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017), *abrogation on other grounds recognized by United States v. Zodhiates*, 901 F.3d 137, 143–44 (2d Cir. 2018);[10] *United*

[8] Rosenow also argues that he has a reasonable expectation of privacy in his private online messages. Because we conclude that Yahoo's and Facebook's searches of his messages were not governmental action, we need not reach this issue. *See Jacobsen*, 466 U.S. at 113.

[9] The Court in *Carpenter* emphasized that its holding was narrow, limited to the specific question presented in that case. 138 S. Ct. at 2220. We decline to broaden the application of *Carpenter* to the novel circumstances presented here.

[10] In *Ulbricht*, the Second Circuit held first that it was bound by the broad rule that a party has no privacy interest in any information disclosed to third parties. 858 F.3d at 96–97. That court later recognized that the Supreme Court has abrogated that rule, in part, in *Carpenter*. *See Zodhiates*, 901 F.3d at 143–44; *United States v. Chambers*, 751 F. App'x

States v. Caira, 833 F.3d 803, 806 (7th Cir. 2016). Specifically, in *Forrester* we analogized IP addresses and email to/from lines to the "information people put on the outside of mail," which the Supreme Court has long held can be searched without a warrant because it "is voluntarily transmitted to third parties"; therefore, there is no legitimate expectation of privacy in such information. 512 F.3d at 511. This basic information differs from the content of email messages and other private communications, which are analogous to the sealed contents of mail, which the government does need a warrant to search. *Id.*

Here, the subpoenas did not request any communication content from Rosenow's accounts, and the government did not receive any such content in response to its subpoenas. Everyone involved knew that additional legal process was required before the government could obtain that information. Thus, as in *Forrester*, Rosenow did not have a legitimate expectation of privacy in the limited digital data sought in the government's subpoenas.

3. Did the search warrant lack probable cause?

Finally, Rosenow argues that the government's search warrant affidavit failed to establish probable cause because it did not include any images of child pornography or any reasonable factual descriptions of such images.

Probable cause exists if, "based on the totality of the circumstances, there is a 'fair probability' that evidence of a

---

44, 46 (2d Cir. 2018). But *Ulbricht* also held, in the alternative, that even if the broad rule were abrogated in the future, the disclosure of IP addresses does not raise privacy concerns because "no reasonable person could maintain a privacy interest in that sort of information." 858 F.3d at 97. We cite *Ulbricht* for that holding, which still stands.

crime may be found." *United States v. Perkins*, 850 F.3d 1109, 1119 (9th Cir. 2017) (citation omitted). Inclusion of illicit images is not required to establish probable cause. "[A] judge may properly issue a warrant based on factual descriptions of an image." *United States v. Battershell*, 457 F.3d 1048, 1052 (9th Cir. 2006).

Here, the government's affidavit included excerpts from Rosenow's messages with adolescent girls in the Philippines, demonstrating that he took and kept illicit pictures and videos of his sex tourism. For example, in one of Rosenow's Facebook chats, he sends a girl nude photos he had previously taken of her and states, "I am always looking at your pictures on my phone . . . and I want more." In another chat, he negotiates sex acts with a girl and states, "baby, I want to take a video too."

The affidavit also described Yahoo's internal investigation and the resulting findings that Rosenow was negotiating, purchasing, and producing images and videos of child sexual exploitation, as well as the information that Facebook reported to NCMEC after searching Rosenow's accounts. These descriptions include an account of Rosenow's communications with girls in the Philippines, wherein Rosenow describes in graphic detail the sexual activities that he wanted to do with them and confirms that he wanted to record those activities.

In these circumstances, the omission of pornographic images was not an intentional misrepresentation or material omission. *See Perkins*, 850 F.3d at 1118–19 (finding agent acted improperly by withholding images in his possession and misrepresenting their content where there was a question whether the images were pornographic). Nor were the FBI agent's multiple, detailed statements analyzing Rosenow's messages and travel patterns merely "boilerplate

description[s]" or "generalized statement[s]" of "a child pornography collector." *Id.* at 1120. Thus, we conclude, as did the district court, that the affidavit supporting the search warrant established a "fair probability" that child pornography would be found on Rosenow's electronic devices. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983).

B. Jury Instructions

Rosenow argues that the jury was not properly instructed on Count 1—attempted sexual exploitation of a child in violation of 18 U.S.C. § 2251(c) and (e). A defendant violates § 2251(c)(1) if he "employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct outside of the United States . . . *for the purpose of* producing any visual depiction of such conduct." 18 U.S.C. § 2251(c)(1) (emphasis added). Rosenow requested an instruction stating that the "purpose" element was satisfied only if the government proved that he "would not have acted *but for* his desire to produce a visual depiction of the sexually-explicit conduct." The district court rejected Rosenow's proposed instruction and instead instructed the jury that the government must prove that "producing a visual depiction of a minor engaged in sexually explicit conduct" was Rosenow's "dominant, significant or motivating" purpose, not that it was his "sole purpose."

Rosenow argues that the statutory phrase "for the purpose of" requires proof of both motive and but-for causation. He analogizes § 2251(c) to laws prohibiting adverse employment actions "because of" or "based on" discriminatory motives. *See, e.g.*, *Burrage v. United States*, 571 U.S. 204, 213–14 (2014) (noting statutory phrases in discrimination statutes indicate "but-for" causal links).

But-for causation is required "when a crime is defined in terms of conduct causing a particular result." *Id*. at 211 (internal quotation marks and citation omitted). In *Burrage*, the Court analyzed a statutory penalty enhancement for drug offenses where "death or serious bodily injury results from" a defendant's conduct. *Id.* at 206 (internal quotation marks and citation omitted). The Court concluded that the "results from" phrase required a causal link between the harm (death or injury) and the proscribed conduct (drug offense). *See id.* at 211–13. Likewise, employment statutes often link the harm (adverse employment action) taken "because of" the proscribed conduct (discriminatory motives). *Id.* But here, the harm (production of obscene content) and the proscribed conduct (enticing children to engage in it) are not connected by any causal link in the text of the statute; rather, the harm and the conduct are connected by the defendant's "purpose." 18 U.S.C. § 2251(c). Thus, we see no basis to conclude that "purpose," as used in § 2251, has a causal or results requirement.

Our precedent further undermines Rosenow's reading of *Burrage*. In *Rodriguez*, albeit interpreting another statute, we held that the "'results from' language evaluated in *Burrage* differs materially from the 'for the purpose of' language . . . . The latter phrase concerns motive whereas the former concerns causation." 971 F.3d at 1010. Similarly, in *United States v. Lindsay*, we found no "obvious error" where the district court instructed the jury to apply the "dominant, significant, or motivating" standard to an offense prohibiting travel "for the purpose of" engaging in illicit sex. 931 F.3d 852, 864 (9th Cir. 2019).

In sum, we conclude that the jury was properly instructed on Count 1.

C. Sentencing Calculation

Finally, Rosenow argues that the district court improperly sentenced him as if he had been convicted on multiple counts of possession of child pornography when he was convicted on only one count.

When more than one minor is exploited in an offense where the defendant "caus[ed], transport[ed], permit[ed], or offer[ed] or s[ought] by notice or advertisement, a minor to engage in sexually explicit conduct for the purpose of producing [child pornography]," the Sentencing Guidelines direct the district court to apply the guidelines applicable to multiple counts "as if the exploitation of each minor had been contained in a separate count of conviction." U.S.S.G. §§ 2G2.1(d)(1), 2G2.2(c)(1). At trial, Rosenow stipulated that he knowingly possessed five depictions of child pornography, including two videos showing *himself* engaging in sexually explicit conduct with four different minors. The jury convicted Rosenow of one count of knowing possession "with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction" of child pornography. 18 U.S.C. § 2252(a)(4)(B).

The district court found, based on Rosenow's stipulations at trial, that in committing the possession offense, Rosenow caused a minor to engage in sexually explicit conduct "for the purpose of producing a visual depiction of that conduct." U.S.S.G. § 2G2.2(c)(1). Accordingly, the court applied the Sentencing Guidelines' multiple-count instruction and calculated Rosenow's sentence based on the exploitation of four separate victims, which increased Rosenow's base offense level and doubled his guideline range.

In arguing that this calculation was error, Rosenow relies primarily on *Chilaca*, where we interpreted § 2252(a)(4)(B)'s prohibition against possession of "1 or more" depictions of child pornography "to mean that the simultaneous possession of different matters containing offending images at a single time and place constitutes a single violation of the statute." 909 F.3d at 295. The defendant in that case was charged with four counts under § 2252(a)(4)(B), but it was undisputed that he simultaneously possessed all the images identified in the four separate counts. *Id.* at 291, 295. Thus, we vacated three counts as multiplicitous. *Id.* at 295, 297.

Chilaca does not control this case. The defendant in *Chilaca* was charged with and convicted of four counts for the single act of possessing "1 or more" depictions of child pornography. *Id.* at 295. Here, Rosenow was convicted of a single offense of possession which involved the exploitation of several child victims. That is, there was no double counting when the district court applied the Sentencing Guidelines' instructions regarding multiple minor victims, as the enhancements were premised on separate exploitative acts.

The Sentencing Commission "plainly understands the concept of double counting, and expressly forbids it where it is not intended." *United States v. Reese*, 2 F.3d 870, 894 (9th Cir. 1993) (quoting *United States v. Williams*, 954 F.2d 204, 208 (4th Cir. 1992)). But applying multiple enhancements based on the same conduct is presumptively permissible under the Sentencing Guidelines. *See* U.S.S.G. § 1B1.1 comment. n.4(B) ("Absent an instruction to the contrary, enhancements . . . are to be applied cumulatively . . . [and] may be triggered by the same conduct."). And here, the enhancement imposed is not only permitted by the

Sentencing Guidelines—it is *required*. *Id.* § 2G2.1(d)(1). The Sentencing Guidelines' application notes explain that "each minor exploited is to be treated as a separate minor," "multiple counts involving the exploitation of different minors are not to be grouped together," and "each such minor shall be treated as if contained in a separate count." *Id.* § 2G2.1 comment. 7.

Because the Sentencing Guidelines are clear that punishment is to account for the number of child victims exploited in the production of child pornography, we find no error in the district court's sentencing calculation.

AFFIRMED.

GRABER, Circuit Judge, dissenting in part:

With one exception, I concur in full in the majority opinion. I agree with the majority opinion's analysis of Defendant's challenges to the jury instructions and to the sentencing calculation. I also agree with most of the majority opinion's analysis of the Fourth Amendment issues. In particular, I agree that federal law alone did not transform Yahoo's or Facebook's searches into governmental action; that the government did not actively participate in Yahoo's or Facebook's searches; that Facebook's searches did not implicate the Fourth Amendment; and that the government's preservation requests and subpoenas do not require suppression. I part ways only as to the question whether, in conducting its searches of Defendant's chat messages, Yahoo was acting as an instrument or agent of the government. On that issue, I respectfully dissent.

"The Fourth Amendment limits searches conducted by the government, not by a private party, unless the private party acts as an 'instrument or agent' of the government." *United States v. Young*, 153 F.3d 1079, 1080 (9th Cir. 1998) (per curiam). "Whether a search is governmental or private depends on: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further the party's own ends." *Id.*

1. *Did the government know of and acquiesce in Yahoo's intrusive conduct?*

Here, the government knew of and acquiesced in Yahoo's searches of chat messages. Beginning early in the course of Yahoo's investigation, government agents hosted several meetings with Yahoo's lead investigator, who relayed to the government agents detailed and extensive search results and independent analysis. In the very first meeting, Yahoo's investigator described to the government agents the tools that Yahoo was using to view snippets of private chat messages sent by individual users. The government agents took no action to discourage the searches or reports. Notably, the district court did not find that the government lacked knowledge about, or failed to acquiesce in, Yahoo's searches.

The majority opinion, while agreeing that the government knew about and failed to discourage Yahoo's searches, asserts that these facts are "immaterial." Op. at 26. Not so. *Young* asks "whether *the government* knew of and *acquiesced in* the intrusive conduct." 153 F.3d at 1080 (emphases added). *The government's* implied consent to Yahoo's intrusive conduct is the very essence of acquiescence.

The majority opinion also seems to suggest—despite its assertion to the contrary—that this prong is not met because Yahoo's searches were legal and that the test would be met only if Yahoo's conduct had been illegal. Op. at 26–27. That proposition is illogical; the government is more likely to acquiesce in legal conduct than in illegal conduct. Perhaps more to the point, the majority opinion's suggestion is contradicted by our precedents. In *United States v. Cleaveland*, 38 F.3d 1092 (9th Cir. 1994), the employee's search was legal; nonetheless we held that "the police knew of and acquiesced in [the employee's] search of the meter at Cleaveland's house." *Id.* at 1094. That is, the first prong was met. The same is true of *United States v. Miller*, 688 F.2d 652 (9th Cir. 1982). The private party's search was legal, but we agreed that the police officers "knew of and acquiesced in [the private person's] conduct." *Id.* at 657. That is, the first prong was met.

2. *Did Yahoo intend to assist law enforcement or to further its own ends?*

The second prong queries the private party's motivation. If the private party "had a 'legitimate, independent motivation' to further its own ends," then the search does not implicate the Fourth Amendment. *Cleaveland*, 38 F.3d at 1094 (citing *United States v. Walther*, 652 F.2d 788, 792 (9th Cir. 1981); *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994)). That conclusion remains true even if the private party had a "dual motive to detect or prevent crime or assist the police." *Id.* But if the private party had no "legitimate independent motivation," then the second prong—an intention to aid law enforcement—is met. *Reed*, 15 F.3d at 932.

Here, as the majority opinion explains, Facebook had a legitimate, independent motivation in conducting its

searches. Op. at 28–29. Facebook's terms of use prohibit content that sexually exploits or endangers children, and Facebook may close any account that violates the terms of use. Indeed, as a result of Facebook's searches of Defendant's account, Facebook did close his account.

The analysis of Yahoo's searches of Defendant's chat messages differs. As the district court properly found, Yahoo had a legitimate reputational interest in preventing its services from being used to exploit or abuse children. But, under the specific facts of this case, that legitimate interest was dependent on—not independent from—governmental action.

It is undisputed that, during the relevant period, Yahoo did not store "photographs or videos or other files shared between two users" via its Messenger chat application. Indeed, any videos or images sent via the Messenger chat application were "never transmitted [to] Yahoo servers, so there was no record of any file transfer of videos or images that would have been available for [Yahoo's] review." At all relevant times, Yahoo's policy allowed Yahoo to terminate a user's account on the ground of child exploitation *only* if it discovered actual images or videos of child pornography. Despite that clear limitation, Yahoo's investigators used internal tools to review Defendant's "full chat history on the Yahoo Messenger" and reported many chat snippets verbatim to the government. Yahoo's investigators "determined that pulling the content, reviewing it, and then filing [reports to the government] might be a way to get the [suspected child-abuse] activity to stop." When asked whether the mechanism for stopping the activity was helping to provide "probable cause" to federal law enforcement, Yahoo's lead investigator replied in the affirmative. And he acknowledged that, although his team

did not exist "only . . . to have a bad guy arrested," that is one of the outcomes that the team strives for.

Putting it together, Yahoo's review of Defendant's chat messages could not possibly have led to Yahoo's termination of Defendant's account. The *only* means by which to prevent Defendant's unlawful conduct was (as the government puts it) "inviting a law enforcement response" and ensuring a successful prosecution. As the government concedes in its brief: "Despite his misuse of its platform, Yahoo never terminated [Defendant's] Yahoo Messenger account since no actual child pornography images were found on it." In other words, protecting Yahoo's legitimate reputational interest *required* the assistance of the federal government. *Cf. Ferguson v. City of Charleston*, 532 U.S. 67, 82–84 (2001) (rejecting, as part of an analysis of the "special needs" exception, the government's attempt to define the purpose of a search in terms of its "ultimate goal" of helping women and children rather than its "immediate objective" of generating "evidence for law enforcement purposes"). The majority opinion states that Yahoo had other available means to prevent Defendant from continuing his activities on Yahoo. Op. at 31 n.6. That may be so in theory, but Yahoo's representative testified that Yahoo could not shut down Defendant's account for violating the platform's terms and conditions because there were no images or videos of child pornography on any of his accounts. The facts in some other case could differ and could yield a different result, but in this instance Yahoo's legitimate motive was not *independent*. Yahoo could not, on the particular facts of this case, *achieve* its legitimate corporate objective without the prosecutorial efforts of law enforcement.

Our decision in *Cleaveland*, 38 F.3d at 1093–94, supports that conclusion. The power company in *Cleaveland* suspected that a customer was diverting electricity illegally, thus preventing the company from collecting the full amount that the customer owed. *Id.* at 1093. An employee for the power company entered the defendant's property to inspect the electricity meter, and he discovered wires diverting electricity. *Id.* The employee "had authority to do this pursuant to [the power company's] Customer Service Agreement." *Id.* We concluded that the private search did not implicate the Fourth Amendment for the following reason: "While [the employee] may have had dual motives for conducting the search—to recover money for [the company's] loss of power on the one hand, and to assist the police in capturing the power thief (and perhaps uncovering a marijuana grow) on the other—his motive to recover for [the company's] loss of power was *a legitimate, independent motive apart from crime detection or prevention*." *Id.* at 1094 (emphasis added). Unlike in *Cleaveland*, Yahoo's reputational motive here in searching Defendant's chat messages was necessarily dependent on law enforcement efforts. *See also Reed*, 15 F.3d at 932 (holding that, in opening a briefcase and dresser drawer, the private party "had no legitimate independent motive within the meaning of [this court's] cases; 'snooping' is not a legitimate motive and finding evidence of criminal activity is not independent").

The majority opinion suggests that *Cleaveland* and *Miller* support its holding. Op. at 29–32. But the power company in *Cleaveland* and the victim of theft in *Miller* didn't care—as far as the opinions suggest—whether the government prosecuted the criminals. They just wanted the money they were owed or the return of their stolen trailer. What makes this situation different is that Yahoo had no way

to advance its reputational interest unless the government prosecuted Defendant. And what makes this case more like *Reed* is that, in *practical* terms, Yahoo's motivation was to help law enforcement gather proof for a prosecution. That is, while Yahoo's motive was without question legitimate, in the circumstances it was *not independent*. Because Yahoo's motivation to conduct the searches was intertwined with, and dependent on, the government's enforcement of criminal laws, the second prong of the "instrument or agent" analysis is met with respect to Yahoo's searches of Defendant's chat messages.

3. *Conclusion*

Because I conclude that Yahoo's searches of Defendant's chat messages implicated the Fourth Amendment, I would vacate the district court's order denying Defendant's motion to suppress and remand for the court's consideration, in the first instance, all related issues, including whether any error was harmless, whether the good-faith exception applies, and whether suppression is an appropriate remedy in this case.

In analyzing whether Yahoo acted as an "agent or instrument" of the government, we are bound by our precedents that establish the two-part test described above. *Miller v. Gammie*, 335 F.3d 889, 899–900 (9th Cir. 2003) (en banc). As a three-judge panel, we therefore may not consider Defendant's assertion that our test is too rigid and fails to account for the considerable intrusiveness of Yahoo's searches. In an appropriate case, the en banc court might consider whether our test—which developed in the context of searches of, for example, a briefcase, an electricity meter, or a single parcel of property—warrants reconsideration in light of technological developments in the intervening decades. *Cf. Carpenter v. United States*, 138 S. Ct. 2206,

2217–18 (2018) (considering in detail the differences for Fourth Amendment purposes between cell phone tracking in "the digital age" as "compared to traditional investigative tools"); *Riley v. California*, 573 U.S. 373 (2014) (rejecting the argument that prior precedent controlled the Fourth Amendment analysis as to cell phones because "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon").[1]

[1] As an example pertinent here, in 1982, we held that the government's acquiescence in a private person's physical search of a parcel of land in Montana for a stolen trailer did not violate the Fourth Amendment. *Miller*, 688 F.2d at 656–58. I wonder whether we likewise would approve, as consistent with the Fourth Amendment, the government's acquiescence in a private person's plan to use a bevy of drones to search thousands of private parcels throughout the state.