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

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 nonprofit 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"

[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).

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.

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 July 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.

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,

---

[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.

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.

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

[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 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.

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 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. Edison Co.*, 419 U.S. 345, 351 (1974). In assessing whether a sufficient nexus exists, "the relevant inquiry is: (1) whether the

[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).

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 necessarily 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] *Cleaveland* demonstrates this point. While

[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

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.

---

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 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

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

---

engaging in activities." Thus, Yahoo was not dependent on the government to further its goals.

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 on three separate occasions 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

---

[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.").

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, 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 States v.*

[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 44, 46 (2d Cir. 2018). But *Ulbricht* also held, in the alternative, that even if the broad rule

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

---

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.

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 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 did not violate Defendant's right to privacy. 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.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. CARSTEN IGOR ROSENOW, Defendant.	CASE NO. 17CR3430 WQH ORDER (Filed Nov. 20, 2018)

HAYES, Judge:

The matters before the Court are the motion to suppress evidence (ECF No. 29) and the motion to dismiss indictment (ECF No. 34) filed by Defendant Carsten Igor Rosenow.

Background facts

On or about September 19, 2014, Yahoo, Inc. ("Yahoo") was alerted by Xoom.com ("Xoom"), an on-line money transfer service, that a number of Yahoo accounts were involved in buying and selling child pornography. Zoom indicated to Yahoo that individuals from Zoom had seen child pornography activities on the Yahoo platform. Zoom reported to Yahoo ten email addresses that Zoom personnel believed had been engaged in the sale of child exploitation materials over Yahoo instant messenger.

Yahoo E-Crime Investigations Team (ECIT) initiated an investigation of the ten Yahoo accounts

identified by Zoom in order to determine whether the accounts were engaged in activity that violated the Yahoo acceptable use policy or needed to be reported to the National Center for Missing and Exploited Children ("NCMEC"). The Yahoo investigation was lead by Sean Zadig, a senior manager for the Yahoo ECIT with supervisory responsibilities over investigations. Zadig is a former law enforcement agent.

The Yahoo ECIT conducts investigations involving the abuse of the terms of service of the Yahoo operating platforms. The Yahoo ECIT investigates activities prohibited by the Yahoo acceptable use policy and criminal activity on the Yahoo platform. Yahoo has policies against activities which the company does not want on Yahoo products, such as harassment, cyber intrusion, and child pornography. Yahoo privacy policies notify users that Yahoo will not share personal information unless "[w]e believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law." (ECF No. 49-4 at 3). Yahoo ECIT started with the ten accounts provided by Zoom. Yahoo ECIT looked at user information, contact lists for a particular user, subject lines of emails, snipets of chat conversations, and open source information, including Facebook and public records. Yahoo ECIT did not consult any outside agency or law enforcement agency in the investigation.

On October 3, 2014, Yahoo ECIT filed a supplement to an existing CyberTip with the NCMEC containing findings from the initial investigation of the seller and buyer accounts identified by Zoom to be engaged in the sale of child exploitation material. Yahoo ECIT made the initial report in order to provide information to NCMEC as quickly as possible because of the discovery of active child abuse. The report indicated that Yahoo ECIT found approximately 115 Yahoo accounts, operated from the Philippines, which were believed to be selling images, video, and live-streamed child exploitation materials via Yahoo mail and Yahoo messenger. Yahoo reported that the images were reviewed by Yahoo personnel and queued for reporting to NCMEC. Yahoo reported that a number of sellers had child sexual abuse images as their Messenger profile picture and the seller accounts appeared to be broadcasting video on commercial "camgirl" websites. Yahoo reported that Yahoo reviewed the header metadata and not the mail content on the buyer accounts. Yahoo reported that based upon the header analysis, some of the buyer accounts appeared to be traveling to the Philippines. Aside from the information provided by Zoom and open source information, Yahoo ECIT did not use any information provided by any outside agency in the October 2014 report.

Following the submission of the October CyberTip to NCMEC, Yahoo ECIT contacted the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) to notify these agencies that there was a supplement for their review at NCMEC. Zadig

testified that Yahoo wanted to be sure that law enforcement was aware of their investigation. Zadig testified that the investigation had determined that children were being actively exploited and that some users were traveling to abuse children. Zadig testified that there are hundreds or even thousands of Cybertips reported per month and that Yahoo wanted to be sure that law enforcement knew that there were children in danger and would prioritize the Yahoo report.

On October 6, 2014, representatives of Yahoo met with representatives of NCMEC, the FBI, and Homeland Security Investigations (HSI) in Alexandria, Virginia to discuss the initiation of the Yahoo investigation, provide an overview of the Yahoo investigation, and advise law enforcement of the Yahoo process for legal service.

In November 2014, the Yahoo ECIT began a second investigation into potential buyers and sellers of child exploitation materials beyond the accounts identified in the initial investigation. Zadig testified that the initial referral in October 2014 contained a small number of individuals directly linked to the ten accounts identified by Zoom. Zadig testified that Yahoo was concerned that there was more activity on the platform and potentially more children in danger. Zadig testified that Yahoo ECIT undertook a second investigation without any direction from the NCMEC or law enforcement in order to go out a few more levels from the initial set of buyers and sellers. The second investigation started with the buyers from the first

investigation linked to additional sellers through the same investigatory methods.

Yahoo ECIT used open source information associated with the Yahoo accounts under investigation, including searching public sex offender registries and Facebook. In the second investigation, the Yahoo ECIT identified casandrarophilipps@yahoo.com as a seller account associated either by email address or SMS number to other seller accounts containing child abuse imagery, and europe_120@yahoo.com as a potential traveler to the Philippines for the purpose of child abuse based upon chat snippets.

On December 5, 2014, Yahoo ECIT sent a supplemental report to NCMEC, which outlined the results of the second investigation. Yahoo ECIT reported that it had observed 267 accounts, operated by at least 45 individuals, which appear to be selling child exploitation material. Yahoo indicated that the buyer list included 347 accounts which appeared to be purchasing images, video, or live streams from the seller accounts. Yahoo ECIT reported that 81 of the 347 buyer accounts appeared to be travelers who may be visiting the Philippines to abuse children. The buyer section of the report included information relating to email account europe_120@yahoo.com and included the name "Carsten Rosenow." *Id.* at 8. Yahoo provided a large batch of information to NCMEC, including subscriber and IP login information for the buyer accounts. Yahoo provided subscriber information for the email addresses europe_120@yahoo.com and crosenow@rocketmail.com. Yahoo identified these accounts as potential buyers

traveling to the Philippines from contacts with a Philippines based seller and chat snippets.

No outside agency provided any information included in the Yahoo December 2014 report, and Yahoo did not consult any agency during the investigation. Yahoo ECIT notified the FBI and HSI that there was additional information for their review for the same reasons that Yahoo notified law enforcement agencies of the October 2014 report.

On December 16, 2014, Yahoo ECIT personnel attended a second meeting with NCMEC, the FBI, and HSI in Alexandria, Virginia.

After receiving the information from Yahoo, FBI Major Crimes Coordination Unit (MCCU), and HSI Cyber Crimes Center Child Exploitation Investigations Unit in Washington, D.C. began conducting a joint investigation into child exploitation involving hundreds of users of Yahoo services purchasing child exploitation materials. Agent Yenesky of the FBI testified that the overall investigation, referred to as "Operation Swift Traveler" or "Philippines Webcam," included a number of different individuals. Agent Yenesky testified that the overall investigation originated with the Yahoo reports through NCMEC. Agent Yenesky testified that law enforcement had no role in directing or participating in the Yahoo investigation. Agent Yenesky testified that he spoke to Zadig at Yahoo from time to time and that Zadig would contact him directly in order to make sure that Agent Yenesky was aware of information Yahoo was providing to

NCMEC. Agent Yenesky testified that his investigation was separate from the Yahoo investigation, and that the meetings with Yahoo were necessary to review the large amounts of information as efficiently as possible. Agent Yenesky testified that the overall investigators would contact the particular appropriate field offices to investigate as the subjects of the investigation were identified.

Law enforcement served preservation requests on Yahoo accounts in October 2014, December 2014, and June 2015. Law enforcement collected wire transfer information from Western Union, Xoom, and Paypal pursuant to criminal summons issued by HSI for money transaction records associated with the seller accounts identified by Yahoo. This information included three transactions in which the email address crosenow@rocketmail.com transferred ten dollars to one of seller accounts identified by Yahoo. The shipping address listed was for Rosenow at a residential address in San Diego, California.

On February 19, 2015, FBI MCCU advised agents in the San Diego Division and the Chicago Division of the joint investigation and identified Carsten Rosenow as a potential suspect residing in the San Diego area. FBI MCCU summarized the information received regarding europe_120@yahoo.com and provided copies of the October and December 2014 NCMEC reports from Yahoo, copies of the HSI summons to PayPal, records checks, and Cybertip information related to the europe_120@yahoo.com account.

During 2015, government investigators placed travel alerts in the U.S. Customs and Border Patrol TECS system regarding Rosenow. Defendant was detained at the border several times and secondary searches yielded no evidence of wrongdoing.

In October 2015, the FBI executed federal search warrants on additional Yahoo account holders for the casandraroyphilipps@yahoo.com account. Yahoo returned records pursuant to the search warrants. On November 3, 2015, the FBI MCCU provided agents in San Diego FBI with the Yahoo records obtained through the search warrant for casandraroyphilipps@yahoo.com.

Emails in the record show that Zadig remained the point of contact for Yahoo with law enforcement throughout the investigation. Yahoo ECIT and Zadig continued to investigate and enforce user safety on the Yahoo platform. Zadig received calls and emails from local law enforcement agents who received leads generated from the broader investigation. Zadig answered questions about the information provided by Yahoo in the Cybertips and provided information on how to serve Yahoo with legal process. Yahoo ECIT assured that law enforcement complied with the Electronic Communications Act in order to protect the privacy of its users. Zadig did not receive any requests from law enforcement to retrieve information from particular Yahoo accounts without proper legal service and did not provide any information to law enforcement from particular Yahoo accounts without proper legal service.

After the December 2014 NCMEC report made by Yahoo, the Yahoo ECIT was advised by law enforcement that a U.S. based buyer included in the December 2014 report had been arrested in Texas. News regarding that arrest led Yahoo ECIT to further scrutinize the buyer's activity on Yahoo which revealed additional, previously unknown sellers in the Philippines who had been in contact with that buyer. A third investigation was opened by ECIT regarding new sellers and any buyers connected to those sellers. As a part of the third investigation, the europe_120@yahoo.com account was found to be in contact with some of the new sellers. While reviewing that activity, a series of chats from October and November 2015 were located in which the owner of the europe_120@yahoo.com account described upcoming travel plans to the Philippines and the abuse of children.

On December 2, 2015, ECIT filed NCMEC Cyber Tip Report #7431977 to report Yahoo Messenger chats related to europe_120@yahoo.com. (ECF No. 49-8). NCMEC processed the CyberTip on December 23, 2015 and forwarded the information to the FBI that same day. Portions of the content of messages sent between the europe_120@yahoo.com account and other Yahoo user screen names were later included in sealed search warrant affidavits for Defendant Rosenow's person, baggage and residence.

On January 21, 2016, at the completion of the third investigation, Yahoo ECIT sent another supplemental report to NCMEC.

In January 2017, Agent Cashman of the FBI San Diego, working investigations involving sexual exploitation of children, was assigned to work on the investigation involving Carsten Rosenow. During the investigation, Agent Cashman reviewed the NCMEC Cybertip from Yahoo for December 2014 and January 2016.

Based on information received from NCMEC via Yahoo, Agent Cashman began investigating whether Rosenow was involved in the abuse of children in the Philippines. While viewing public information on a Carlos Senta Facebook account, Agent Cashman concluded that Rosenow had two accounts on Facebook, including the Carlos Senta account in which Rosenow spoke primarily to Filipino girls.

On January 4, 2017, Agent Cashman sent a preservation request to Facebook, Inc. for Account #100000403405520, which was associated with the moniker "Carlos Senta" and had previously been associated with the moniker "Carl Europe". The preservation request was submitted via Facebook's Law Enforcement Online Request System (LEORS), and indicated that the request related to a child exploitation matter. When submitting legal process through LEORS, law enforcement must provide the type of legal process, the nature of the case, the signature date, the due date, and the relevant accounts.

Facebook acknowledged receipt of the preservation request via automatically generated email on the same day and preserved the account for 90 days. The

acknowledgment from Facebook did not indicate that Facebook would search the account.

On January 9, 2017, Agent Cashman emailed a request to NCMEC asking for any information available regarding the Defendant. The email stated in part "FBI San Diego attempted to get a search warrant for ROSENOW's Yahoo account but the U.S. Attorney's office declined our request and stated we needed additional updated information." (ECF No. 29-11 at 2).

On March 17, 2017, Agent Cashman served an administrative subpoena on Facebook for the Carols Senta account which stated "THIS IS A CHILD EXPLOITATION MATTER" and requested that Facebook not disclose the existence of the subpoena. The administrative subpoena sought basic subscriber information and IP log-in information. No content information was requested from the account and no request was made to Facebook to search the account. (ECF No. 29-12 at 5).

On April 10, 2017, Facebook Law Enforcement Response Team (LERT) made data responsive to the administrative subpoena available for download. No content information was received.

In April 17, 2017, Facebook LERT conducted a limited review of the Carlos Senta account and flagged the account for further review by the Community Operations team as possibly containing material constituting sexual exploitation of minors in violation of Facebook's Community Standards. Facebook Community Standards state "[w]e do not allow content that

sexually exploits or endangers children. When we become aware of apparent child exploitation, we report it to [NCMEC], in compliance with applicable law." (ECF No. 49-4 at 2). In reviewing legal process submitted via LEORS, Facebook LERT conducts a limited review of the account for violating material when the nature of the case selected by law enforcement indicates that conduct could be occurring on the platform in violation of Facebook Community Standards.

On April 27, 2017, the Community Operations team conducted a more thorough review and disabled the account for violation of Facebook's Community Standards.

On April 28 and May 1, 2017, the Community Operations team reported potential child sexual exploitation related to the Carlos Senta account to NCMEC. The first report (Cybertip report #207111118) identified three images that appeared to depict sexual exploitation of a minor, and the second report included additional facts and reported the discovery of evidence of possible child exploitation.

NCMEC passed the information from the Facebook Cybertip to the FBI. Agent Cashman subsequently reviewed the FBI report with chats. The report contained additional information which lead FBI San Diego to believe that both of the reported Facebook accounts and the Yahoo accounts europe_120@yahoo.com and crosenow@rocketmail.com were used by Defendant Rosenow.

On May 4, 2017, Facebook LERT received another preservation request from the FBI for carlos.senta account through LEORS, which triggered the automatic preservation of the account for 90 days.

On June 5, 2017, LERT received a subpoena from the FBI for the carsten.rosenow account, which indicated that the nature of the case was "Child Safety (Potential Harm)."

On June 12, 2017, LERT made data responsive to the subpoena available for download. On the same day, LERT conducted a limited review of the carsten. rosenow account for violating conduct and indicated that no violating content was located.

In June 2017 the F.B.I. requested search warrants from a magistrate judge for Rosenow's luggage and his home, including searches of his digital devices. The requests were supported by an affidavit of FBI Agent Dingle. In the affidavit, Agent Dingle stated that the facts set forth were based on his personal knowledge, knowledge obtained from other individuals during his participation in the investigation, including other law enforcement officers, review of documents and computer records related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through training and experience. Agent Dingle explained that the investigation led him to believe that Rosenow had traveled to the Philippines on multiple occasions over the course of several years for the purpose of engaging in criminal sexual activity,

illicit sexual conduct with minors, and the production and distribution and possession of images of minors engaged in sexually explicit conduct. Agent Dingle informed the Magistrate Judge that the investigation began when Yahoo identified Yahoo accounts, operating from the Philippines, selling pictures, videos and live-streamed images of sexual abuse on Yahoo Mail and Yahoo Messenger. Agent Dingle informed the Magistrate Judge that Yahoo identified one specific seller account, and that Yahoo found accounts purchasing the images from this seller account, including the user of the email account europe_120@yahoo.com. After detailing chat messages sent between the seller and the user of the email account europe_120@yahoo.com, Agent Dingle detailed information linking the user to Rosenow. The Magistrate Judge authorized the warrants.

On June 21, 2017, Rosenow arrived at the San Diego airport on a flight from San Francisco. Federal search warrants were executed on Defendant's person, baggage and residence and items of digital evidence were seized, including digital image and video files. Rosenow was arrested and placed into federal custody.

On July 14, 2017, FBI San Diego obtained a federal search warrant for the Carlos Senta Facebook account.

On July 19, 2017, a one-count information was filed charging Defendant Rosenow with one count of travel with intent to engage in illicit sexual conduct, in violation of 18 U.S.C. § 2423(b).

On October 19, 2017, a three count indictment was filed against Defendant charging one count of attempted sexual exploitation of a child in violation of 18 U.S.C. § 2251(c); one count of travel with intent to engage in illicit sexual conduct, in violation of 18 U.S.C. § 2423(b); and one count of possession of images of minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

On March 19, 2018, Defendant moved the Court to suppress evidence. Defendant contends that all of the evidence against him "is the result of warrantless searches of his private communications – searches that were 'government action' on these facts." (ECF No. 29-1 at 9). Defendant moves the Court to suppress "all evidence described herein." *Id.* at 45.

On April 27, 2018, Plaintiff United States filed an opposition to the suppression of any evidence on the grounds that searches conducted by Yahoo and Facebook were private action not subject to Fourth Amendment constraints. Plaintiff United States asserts that Yahoo, Facebook, and law enforcement acted in conformance with all applicable laws. Plaintiff United States contends that there are no grounds to suppress any evidence.

On July 27, 2018 and August 8, 2018, the Court held an evidentiary hearing with testimony from Yahoo and Facebook personnel as well as law enforcement agents involved in the investigation.

Motion to suppress evidence

Yahoo investigation

Defendant asserts that the Government violated his Fourth Amendment rights by repeatedly accepting private communications from Yahoo in violation of law. Defendant asserts that the Cybertips to NCMEC from Yahoo went far beyond child pornography and were not authorized by 18 U.S.C. § 2258A. Defendant contends that information relating to travel for purposes of illicit sexual conduct is outside the scope of the statute authorizing Yahoo to disclose information to NCMEC. Defendant asserts that the interaction of NCMEC with the electronic service providers instigated the searches by Yahoo personnel, and Yahoo personnel acted as government agents investigating the materials on the Yahoo platform.

Plaintiff United States contends that any search by Yahoo personnel on the Yahoo platform was private action not subject to Fourth Amendment constraints. Plaintiff United States asserts that Yahoo was alerted to a complaint about Defendant's account by a non-law enforcement source before law enforcement became involved. Plaintiff United States asserts that Yahoo was not acting on behalf of the Government when ECIT personnel investigated the activities of their users on Yahoo servers. Plaintiff United States asserts that Yahoo was acting on behalf of its business interest. Plaintiff United States asserts that there is no evidence that the Government knew of or acquiesced in the Yahoo investigations while they were occurring. Plaintiff

United States contends that the communications received by NCMEC from Yahoo complied with existing statutes and legal precedent.

In *Carpenter v. United States*, the United States Supreme Court stated,

> The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). . . .

138 S.Ct. 2206, 2213 (2018). The United States Supreme Court "has consistently construed [Fourth Amendment] protection as proscribing only government action; it is wholly inapplicable 'to search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with participation or knowledge of any governmental official.'" *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)); *see United States v. Al Nasser*, 555 F.3d 722, 725 (9th Cir. 2009) ("The Fourth Amendment protects people from unreasonable 'seizures,' and the Supreme Court 'has consistently construed this protection as proscribing only government action.'") (quoting *Jacobsen*, 466 U.S. at 113.).

However, the Fourth Amendment does prohibit unreasonable intrusions by private individuals who are acting as government instruments or agents. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *United States v. Walther*, 652 F.2d 788, 792-93 (9th Cir. 1981).

The defendant has the burden of showing government action. *United States v. Gumerlock*, 590 F.2d 794 (9th Cir. 1979) (en banc), *cert. denied*, 441 U.S. 948 (1979). In *United States v. Reed*, 15 F.3d 928 (9th Cir. 1994), the Court of Appeals stated,

> The general principles for determining whether a private individual is acting as a governmental instrument or agent for Fourth Amendment purposes have been synthesized into a two part test. *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982). According to this test, we must inquire:
>
> > (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.

Id. at 931. (quoting *Miller*, 688 F.2d at 657).

In this case, the evidence at the evidentiary hearing established conclusively that Yahoo, an electronic service provider, was alerted to information about certain accounts involved in buying and selling child pornography by another internet service provider, Xoom. Yahoo ECIT initiated an investigation in October of

2014 based solely upon the information provided by Zoom. Yahoo ECIT discovered buyer and seller accounts on the Yahoo platform with child sexual images. Yahoo ECIT concluded that their investigators had discovered active child abuse and expeditiously reported to NCMEC as required by law. Law enforcement was not involved in any way until after this investigation was completed and the October 2014 report was sent to NCMEC.

After meeting with law enforcement to review the October 2014 report, Yahoo ECIT began a second investigation. Yahoo ECIT remained concerned that there was more activity on their platform that violated the Yahoo terms of service, and investigated additional suspected buyers and sellers of child exploitation materials. There is no evidence in the record that law enforcement was involved in any way with the decision by Yahoo ECIT to undertake a second investigation or that law enforcement was involved in or participated in the second investigation by Yahoo ECIT. After identifying additional buyers and sellers, Yahoo filed a second Cybertip with NCMEC in December 2014 and again met with law enforcement.

After the second report, law enforcement undertook an investigation. There is no evidence that law enforcement sought or received any assistance from Yahoo personnel in conducting this investigation outside of legal process. During the investigation, Zadig remained in communication with FBI Agent Zelensky receiving information from the FBI when available to the public. After learning of an arrest in Texas of a

Yahoo user included in the December 2014 Cybertip, Yahoo ECIT began a third investigation into users of its platform. There is no evidence in the record that law enforcement was involved with the decision by Yahoo ECIT to undertake a third investigation or that law enforcement was involved in or participated in third investigation by Yahoo ECIT. The evidence in the record shows that Yahoo ECIT acted on behalf of Yahoo. Yahoo took no direction from law enforcement and law enforcement had no involvement in any Yahoo investigation.

Yahoo ECIT conducted its investigations involving the activity on Yahoo platforms in order to determine whether users were violating the Terms of Service and Community Guidelines. Yahoo has a business interest in enforcing its terms of service and ensuring that its products are free of illegal conduct, in particular, child sexual abuse material. The evidence in the record shows that Yahoo ECIT was acting to enforce the Yahoo terms of service and to ensure that Yahoo products were free of illegal content. Yahoo ECIT was acting in compliance with internal policies, business interests, and all existing laws. The Court concludes that Yahoo ECIT acted in a private capacity not subject to Fourth Amendment constraints. *See Jacobsen*, 466 U.S. at 115 (concluding that the Fourth Amendment does not protect against "invasions . . . occasioned by private action.").

The Stored Communications Act, 18 U.S.C. § 2701 et al., generally prohibits remote computing services from disclosing records, information, and contents of

accounts, except under certain circumstances. 18 U.S.C. § 2702(a). 18 U.S.C. § 2702(b) provides in part:

> (b) Exceptions for disclosure of communications. – A provider described in subsection (a) may divulge the contents of a communication –
>
> (5) as may be necessarily incident to the rendition of the service or to protect the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;
> . . .
>
> (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency[.]

§ 2702(b). In this case, Yahoo ECIT discovered material on the Yahoo platform indicating that sellers and buyers, including Defendant, were suspected of using the Yahoo messenger to seek commercial sex with minors and to exchange sexual images of minors. Yahoo personnel reasonably concluded that facts and circumstances existed to support suspected child abuse involving the sellers of images, videos, and livestreams located in the Philippines in violation of section 2252.

The investigation of Yahoo ECIT pursuant to legitimate business purposes lead Yahoo to a duty to report under 18 U.S.C. § 2258A, which provides in part:

> a) Duty to report. –
>
> (1) In general. – Whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any facts or circumstances described in paragraph (2) shall, as soon as reasonably possible-
>
> (A) provide to the CyberTipline of the National Center for Missing and Exploited Children, or any successor to the CyberTipline operated by such center, the mailing address, telephone number, facsimile number, electronic mail address of, and individual point of contact for, such electronic communication service provider or remote computing service provider; and
>
> (B) make a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by such center.
>
> (2) Facts or circumstances. – The facts or circumstances described in this paragraph are any facts or circumstances from which there is an apparent violation of –
>
> (A) section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography; or
> . . .

> (b) Contents of report. – To the extent the information is within the custody or control of an electronic communication service provider or a remote computing service provider, the facts and circumstances included in each report under subsection (a)(1) may include the following information:
>
> (1) Information about the involved individual. – Information relating to the identity of any individual who appears to have violated a Federal law described in subsection (a)(2), which may, to the extent reasonably practicable, include the electronic mail address, Internet Protocol address, uniform resource locator, or any other identifying information, including self-reported identifying information.

§ 2258A. Compliance with this duty to report did not convert Yahoo ECIT into a government actor subject to Fourth Amendment warrant requirements. Yahoo personnel investigated the use of its business platform as a private actor in furtherance of its business interest in excluding users of its service perpetrating child abuse and child exploitation. Compliance with the reporting requirements of § 2258A, standing alone, did not transform Yahoo, an internet service provider, into a government agent. *See United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) ("A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."); *United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) ("[T]he statute did not impose any

obligation to *search* for child pornography, merely an obligation to *report* child pornography of which Yahoo! became aware."); *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010) ("We conclude that the statutory provision pursuant to which AOL reported Richardson's activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes.").

Unlike the regulatory scheme in *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602 (1989), the actions taken by Yahoo were the result of private initiatives. In *Skinner*, the Supreme Court considered whether the regulatory scheme imposed by the Federal Railroad Administration for mandatory and permissive drug testing by private railroads implicated the Fourth Amendment. Because the regulations mandated the means, methods and procedures for testing, the Court concluded that "[a] railroad that complied with the provision of Subpart C of the regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment." *Id.* at 614. In this case, the government played no role in instigating or participating in Yahoo's investigation. Section 2258A imposed no duty on Yahoo to monitor its platform for child exploitation materials. The duty imposed to report when facts and circumstances of apparent violations of child pornography laws are found does not transform Yahoo's investigation into government action.

Preservation Requests

Defendant asserts that the Government committed unconstitutional searches and seizures of his private communications by issuing preservation requests to third-parties pursuant to 18 U.S.C. § 2703(f). Defendant contends that the Government unlawfully seized and held his private communications through preservation and subpoena requests. Defendant asserts that this seizure of his private communications was subject to the warrant requirement of the Fourth Amendment based upon the recent decision of the United States Supreme Court in *United States v. Carpenter*.

Plaintiff United States contends that preservation requests issued by the Government pursuant to Section 2703(f) are not seizures under the Fourth Amendment. Plaintiff United States asserts that the preservation of Defendants' accounts under § 2703(f) is not a meaningful interference with Defendant's possessory interests in his account. Plaintiff United States asserts that Defendant was free to continue to use his account and only prevented by the preservation request from manipulating the copy made by the service provider. Plaintiff United States asserts that the Fourth Amendment does not require probable cause for this minimal intrusion authorized by Congress in Section 2703(f).

The record in this case shows that law enforcement sought the preservation of Defendant's Yahoo

and Facebook accounts in compliance with 18 USC § 2703(f)which provides

> Requirement to preserve evidence. – (1) In general. – A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention. – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

§ 2703(f).[1]

In *Carpenter*, prosecutors applied for court orders under the Stored Communications Act, 18 U.S.C. § 2703(d), to obtain cell phone records for Carpenter and several other suspects in a robbery investigation. 138 S.Ct. at 2206. Carpenter was charged with six counts of robbery and moved to suppress the cell-site records provided by the wireless carriers. Carpenter argued that the government's seizure of the records violated the Fourth Amendment because the records had been obtained without a warrant supported by probable cause. The Court of Appeals held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI "because he had

[1] *See also* 18 U.S.C. § 2258A(h) Preservation.

shared that information with his wireless carriers." *Id.* at 2214. The Court of Appeals concluded that the resulting business records were not entitled to Fourth Amendment protection.

The Supreme Court concluded that the location information obtained from the "[g]overnment's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment." *Id.* at 2220. The Supreme Court stated, "while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records." *Id.* at 2216-17. The Supreme Court found that the collection of Carpenter's cell phone location information was an "entirely different species of business records – something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." *Id.* at 2222. The Supreme Court concluded that the protections of the Fourth Amendment "should extend to a detailed log of a person's movements over several years." *Id.* The Supreme Court went on to state, "[t]his is certainly not to say that all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party." *Id.* "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interest in

the property." *Jacobsen*, 466 U.S. at 113. A preservation request pursuant to Section 2703(f) notifies the online provider to "take all necessary steps to preserve records" of an account for 90 days. 18 U.S.C. § 2703(f). The preservation requests in this case did not interfere with the Defendant's use of his accounts and did not entitle the Government to obtain any information without further legal process. Law enforcement may, generally, seize items without warrant when the items are found under circumstances where the risk of destruction of the evidence before a warrant may be obtained outweighs the interest in possession. *See United States v. Place*, 462 U.S. 696, 701-02 (1983). The statutory authorization to preserve a wire or electronic communications account held by a third-party online provider recognizes that the information is easily and readily destroyed and allows its preservation for a short period in order to allow law enforcement to seek further legal process. The Court concludes that the preservation requests in this case did not amount to an intrusion subject to Fourth Amendment requirements.

However, "subpoenas trigger Fourth Amendment concerns and may be challenged under Fourth Amendment grounds." *See Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1088 n.1 (9th Cir. 2016); *see also Carpenter*, ("[T]his Court has never held that the Government may subpoena third parties for records in which the suspect as a reasonable expectation of privacy."). The Stored Communication Act, § 2703(c), provides in part that

"A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity – (B) obtains a court order for such disclosure under subsection (d) of this section;

. . .

(d) Requirements for court order. – A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(c)(d).

The United States Supreme Court has "consistently 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 (1979) (pen register for phone numbers from the phone company do not acquire the contents of communications and are not subject to Fourth Amendment warrant requirements*); see also United States v. Miller*, 425 U.S. 435 (1976) (subpoena for bank records not search because bank records were not respondent's private papers); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (warrantless government surveillance of email to/from addresses and IP addresses do not constitute search because defendant voluntarily turned over the information in order to direct the third party server).

In this case, the Government received subscriber information and IP log-in information from Yahoo and Facebook[2] pursuant to § 2703 administrative subpoenas. This information disclosed by third-parties Yahoo and Facebook did not reveal any contents of the account pursuant to the administrative subpoenas. The Court concludes that Defendant had no reasonable expectation of privacy in the subscriber information and the IP log-in information Defendant voluntarily provided to the online service providers in order to establish and maintain his account. The Court concludes

---

[2] Subpoena requested the "name associated with [the carlos.senta account], length of service, credit card information, email address, and recent login/logout IP addresses, if available." (ECF No. 29-12 at 5).

that Defendant did not have a legitimate expectation of privacy in the information provided pursuant to the administrative subpoenas. Unlike the location information in *Carpenter*, the information requested by the subpoenas is not subject to reasonable expectation of privacy and not a search within the meaning of the Fourth Amendment.

Facebook investigation

Defendant contends that the Facebook personnel acted as government agents when they investigated his account and reported to NCMEC. Defendant asserts that Facebook acted because of the preservation requests and subpoenas by the law enforcement. Defendant asserts that every time Facebook investigates an account after receiving a "child exploitation" preservation request or subpoena, Facebook is acting on behalf of law enforcement. Defendant asserts that the search by Facebook, instigated by law enforcement, led directly to the compelled disclosure of evidence under Section 2258A. Defendant contends that "a *Carpenter* search and seizure" resulted "on these facts." (ECF No. 76 at 31).

Plaintiff United States contends that law enforcement did not request that Facebook conduct any search or initiate any internal investigations into the Defendant's accounts. Plaintiff United States asserts that Facebook conducted its review of Defendant's account in compliance with its own internal policies and reported the information found in compliance with applicable

law. Plaintiff United States asserts that law enforcement acted within normal investigative procedures at all times.

The evidence established that the Government submitted a preservation request and subpoena for the carlos senta Facebook account indicating a potential child exploitation matter. Facebook internal policy provided that subpoenas which indicated a child exploitation matter trigger a limited content review by Facebook LERT in order to investigate suspected violations of the acceptable use policy. There is no evidence that the FBI acted outside normal investigative procedures in order to prompt an investigation by Facebook. Facebook acted pursuant to its internal policies and procedures regarding the review of the accounts of their users. FBI San Diego did not request that Facebook conduct any search or initiate any internal investigation into Defendant's accounts. The Facebook investigation was initiated pursuant to internal Facebook policies in order to advance Facebook business interests. The Court concludes that Facebook search was private action not subject to Fourth Amendment constraints.

Franks

Defendant contends that the affidavit in support of the search warrants for his luggage and his home contained material misrepresentations and omissions requiring suppression or a *Franks* hearing. Defendant asserts that the affidavit in support of the search

warrant lacked probable cause and that Agent Dingle had no personal knowledge of the facts contained in the affidavit. Plaintiff United States asserts that the search warrant did not contain material omissions or misrepresentations which would require suppression and that all search warrants in this case were supported by probable cause.

In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court examined the circumstances under which a defendant may "attack the veracity of a warrant affidavit after the warrant has been issued and executed." *Id.* at 164. "A defendant is entitled to a *Franks* hearing only if he makes a two-fold showing: intentional or reckless inclusion or omission, and materiality." *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000). To make this showing, a defendant "must make specific allegations that indicate the portions of the warrant claimed to be false" and "[t]he allegations must be accompanied by a detailed offer of proof, preferably in the form of affidavits." *United States v. Kiser*, 716 F.2d 1268, 1271 (9th Cir. 1983). Defendant failed to identify any misrepresentations or material omissions at the evidentiary hearing necessary to a finding or probable cause.

Probable cause exists when "there is a fair probability that contra band or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The Court finds that the affidavit in support of search warrant sworn by Agent Dingle set forth facts sufficient to support probable cause as to the alleged child pornography violations.

Conclusion

The record in this case shows that Yahoo and Facebook conducted investigations in accordance with their internal policies and procedures. The record shows that Yahoo and Facebook reported information to NCMEC pursuant to applicable law based upon facts and circumstances supporting an apparent violation of child pornography laws. The record further shows that law enforcement conducted an investigation independent of Yahoo and Facebook. Law enforcement utilized information provided by Yahoo and Facebook in compliance with all applicable laws and issued preservation requests and subpoenas to obtain limited information from third parties as provided by applicable statutory authorization. Defendant's motion to suppress evidence is denied.

Motion to dismiss indictment

On October 19, 2017, the grand jury returned an indictment charging Defendant in Count One with attempted sexual exploitation of a minor in violation of 18 U.S.C. § 2251(c); in Count Two with travel for the purposes of engaging in illicit sexual conduct of 18 U.S.C. § 2423(b); and in Count Three with possession of images of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252 (A)(4)(B) and (b)(2).

Defendant moves to dismiss the charges in Count One and Count Three on the grounds that the statute violates the First Amendment, the charge lacks any

allegation of culpable scienter, and the statute is unconstitutionally vague and overbroad. Defendant contends that the federal child pornography laws defining a minor as an individual under the age of 18 are substantially overbroad and violate the first Amendment. Defendant asserts that the age of consent for sexual relationships in federal law and in many states is 16 years old. Defendant asserts that prohibiting all sexually explicit depictions of 16 and 17 year olds is not consistent with the First Amendment principle that Congress may not suppress lawful speech as a means to suppress unlawful speech. Defendant further asserts that the charge in Count Two of travel for the purposes of engaging in illicit sexual conduct must be dismissed on the grounds that the phrase "commercial sex act" is unconstitutionally vague and that the statute lacks mens rea.

Plaintiff United States asserts that the offenses charged in Count One and Three are constitutionally sound. Plaintiff United States further asserts that the term "commercial sex act" as used in 18 U.S.C. § 2324(b) is not unconstitutionally overbroad.

In *United States v. X-Citement Video, Inc.*, 513 U.S. 64 (1994), the United States Supreme Court upheld the constitutionality of § 2252 "conclud[ing] that the term 'knowingly' in § 2252 extends both to the sexually explicit nature of the material and to the age of the performers." 513 U.S. at 78. The Supreme Court further stated:

> As an alternative grounds for upholding the reversal of their convictions, respondents reiterate their constitutional challenge to 18 U.S.C. § 2256. These claims were not encompassed in the question on which this Court granted certiorari, but a prevailing party, without cross-petitioning, is "entitled under our precedents to urge any grounds which would lend support to the judgment below." *Dayton Bd. of Ed. v. Brinkman*, 433 U.S. 406, 419, 97 S.Ct. 2766, 2775, 53 L.Ed.2d 851 (1977). Respondents argue that § 2256 is unconstitutionally vague and overbroad because it makes the age of majority 18, rather than 16 as did the New York statute upheld in *New York v. Ferber, supra*, and because Congress replaced the term "lewd" with the term "lascivious" in defining illegal exhibition of the genitals of children. We regard these claims as insubstantial, and reject them for the reasons stated by the Court of Appeals in its opinion in this case.

513 U.S. at 78-79. The Court of Appeals had stated, "we would not lightly hold that the Constitution disables our society from protecting those members it traditionally considered to be entitled to special protections – minors." *United States v. X-Citement Video, Inc.*, 982 F.2d 1285, 1288 (9th Cir. 1992), *rev'd on other grounds*, 513 U.S. 64 (1994). The Court of Appeals recognized a "series of Supreme Court cases that permit 'adult' treatment of 16- and 17-year-olds" noting that these "Supreme Court cases . . . merely permit, rather than require, adult treatment of 16- and 17-year-olds." 982

F.2d at 1288. The Court of Appeals concluded that the Supreme Court cases "indicate nothing about the substantiality (or lack thereof) of the overbreadth of section 2256" and concluded that the defendant's arguments are "far from sufficient to overcome the presumption against invalidating a statute on its face for overbreadth." *Id.*

In this case, Count One and Count Three allege the production and possession of depictions of sexually explicit conduct involving minors. Minor is defined as "any person under the age of eighteen years." 18 U.S.C. § 2256(1). This court applies the holding of the Supreme Court in *X-Citement Video* that § 2256 is not "unconstitutionally vague and overbroad because it makes the age of majority 18, rather than 16." 513 U.S. at 78. The Court further concludes that Count One and Count Three are not unconstitutional on the grounds that the statutes lack an element of scienter or violate the foreign commerce clause. *See United States v. Jayavarman*, 871 F.3d 1050, 1059-60 (9th Cir. 2017).

Count Three charges Defendant with travel for the purpose of engaging in any illicit sexual conduct in violation of 18 U.S.C. § 2423(b). The term "illicit sexual conduct", as used in Section 2423(b), is defined in 18 U.S.C. § 2423(f) to include "any commercial sex act (as defined in section 1591) with a person under 18 years of age[.]" 18 U.S.C. § 1591(a)(3) provides, "The term 'commercial sex act' means any sex act, on account of which anything of any value is given to or received by any person." 18 U.S.C. § 1591(a)p(3). Section 1591(e)(3) provides that an item of value given or received must

have been "on account of" a sexual act with a minor. The Court concludes that this statute is not unconstitutionally vague.

The Court concludes that the offenses charged in the indictment are constitutional and Defendant's motion to dismiss the indictment is denied.

IT IS HEREBY ORDERED that Defendant's motion to suppress evidence (ECF No. 29) is denied and Defendant's motion to dismiss indictment (ECF No. 34) is denied.

DATED: November 20, 2018

/s/ William Q. Hayes
WILLIAM Q. HAYES
United States District Judge

18 U.S.C. § 2258A
Reporting requirements of providers

(a) Duty to report. –

(1) In general. –

(A) Duty. – In order to reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children, a provider –

(i) shall, as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(A), take the actions described in subparagraph (B); and

(ii) may, after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(B), take the actions described in subparagraph (B).

(B) Actions described. – The actions described in this subparagraph are –

(i) providing to the CyberTipline of NCMEC, or any successor to the CyberTipline operated by NCMEC, the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider; and

(ii) making a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by NCMEC.

(2) Facts or circumstances. –

(A) Apparent violations. – The facts or circumstances described in this subparagraph are any facts or circumstances from which there is an apparent violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography.

(B) Imminent violations. – The facts or circumstances described in this subparagraph are any facts or circumstances which indicate a violation of any of the sections described in subparagraph (A) involving child pornography may be planned or imminent.

(b) Contents of report. – In an effort to prevent the future sexual victimization of children, and to the extent the information is within the custody or control of a provider, the facts and circumstances included in each report under subsection (a)(1) may, at the sole discretion of the provider, include the following information:

(1) Information about the involved individual.– Information relating to the identity of any individual who appears to have violated or plans to violate a Federal law described in subsection (a)(2), which may, to the extent reasonably practicable, include the electronic mail address, Internet Protocol address, uniform resource locator, payment information (excluding personally identifiable information), or any other identifying information, including self-reported identifying information.

(2) Historical reference. – Information relating to when and how a customer or subscriber of a

provider uploaded, transmitted, or received content relating to the report or when and how content relating to the report was reported to, or discovered by the provider, including a date and time stamp and time zone.

(3) Geographic location information. – Information relating to the geographic location of the involved individual or website, which may include the Internet Protocol address or verified address, or, if not reasonably available, at least one form of geographic identifying information, including area code or zip code, provided by the customer or subscriber, or stored or obtained by the provider.

(4) Visual depictions of apparent child pornography. – Any visual depiction of apparent child pornography or other content relating to the incident such report is regarding.

(5) Complete communication. – The complete communication containing any visual depiction of apparent child pornography or other content, including –

(A) any data or information regarding the transmission of the communication; and

(B) any visual depictions, data, or other digital files contained in, or attached to, the communication.

(c) Forwarding of report to law enforcement. – Pursuant to its clearinghouse role as a private, nonprofit organization, and at the conclusion of its review in furtherance of its nonprofit mission, NCMEC shall make available each report made under subsection

(a)(1) to one or more of the following law enforcement agencies:

(1) Any Federal law enforcement agency that is involved in the investigation of child sexual exploitation, kidnapping, or enticement crimes.

(2) Any State or local law enforcement agency that is involved in the investigation of child sexual exploitation.

* * *

(e) Failure to report. – A provider that knowingly and willfully fails to make a report required under subsection (a)(1) shall be fined –

(1) in the case of an initial knowing and willful failure to make a report, not more than $150,000; and

(2) in the case of any second or subsequent knowing and willful failure to make a report, not more than $300,000.

* * *

---

18 U.S.C. § 2258C

Use to combat child pornography of technical elements relating to reports made to the CyberTipline

(a) Elements. –

(1) In general. – NCMEC may provide elements relating to any CyberTipline report to a provider for the sole and exclusive purpose of permitting

that provider to stop the online sexual exploitation of children.

(2) Inclusions. – The elements authorized under paragraph (1) may include hash values or other unique identifiers associated with a specific visual depiction, including an Internet location and any other elements provided in a CyberTipline report that can be used to identify, prevent, curtail, or stop the transmission of child pornography and prevent the online sexual exploitation of children.

(3) Exclusion.– The elements authorized under paragraph (1) may not include the actual visual depictions of apparent child pornography.

(b) Use by providers. – Any provider that receives elements relating to any CyberTipline report from NCMEC under this section may use such information only for the purposes described in this section, provided that such use shall not relieve the provider from reporting under section 2258A.

(c) Limitations. – Nothing in subsections[1] (a) or (b) requires providers receiving elements relating to any CyberTipline report from NCMEC to use the elements to stop the online sexual exploitation of children.

* * *

---

[1] So in original. Probably should be "subsection".

18 U.S.C. § 2701
Unlawful access to stored communications

(a) Offense. – Except as provided in subsection (c) of this section whoever –

> **(1)** intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> **(2)** intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. – The punishment for an offense under subsection (a) of this section is –

> **(1)** if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State –
>
> > **(A)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
> >
> > **(B)** a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case –

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions. – Subsection (a) of this section does not apply with respect to conduct authorized –

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

---

18 U.S.C. § 2702
Voluntary disclosure of
customer communications or records

(a) Prohibitions. – Except as provided in subsection (b) or (c) –

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service –

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications. – A provider described in subsection (a) may divulge the contents of a communication –

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency –

(A) if the contents –

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[**(B)** Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

* * *

---

18 U.S.C. § 2703
Required disclosure of customer communications or records

* * *

(c) Records concerning electronic communication service or remote computing service.

* * *

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the –

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

* * *

(f) Requirement to preserve evidence. –

(1) In general. – A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention. – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

* * *

---

47 U.S.C. § 230
Protection for private blocking and
screening of offensive material

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States –

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of –

> **(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> **(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[1]

* * *

[1] So in original. Probably should be "subparagraph (A)".