No. _____

In The
Supreme Court of the United States

CARSTEN ROSENOW,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

TIMOTHY SCOTT
Counsel of Record
MARCUS BOURASSA
MCKENZIE SCOTT P.C.
1350 Columbia, Suite 600
San Diego, CA 92101
(619) 794-0451
tscott@mckenziescott.com

December 30, 2022

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTION PRESENTED

In the context of electronic communications, a series of statutes give companies permission to access their users' private correspondence, remove impediments to the companies' review of users' papers, and mandate they report certain findings to law enforcement. Here, law enforcement knew of and acquiesced to Yahoo's repeated review and disclosure of its customer's private correspondence. A divided panel of the Ninth Circuit held that this was not government action because the governing statutes rendered Yahoo's searches and disclosures legal and, where the underlying private searches were legal, only "*active participation or encouragement*" by government would implicate the Fourth Amendment.

However, this Court has held that the determination whether searches by a private party constitute government action for purposes of the Fourth Amendment depends upon "all the circumstances," including any statutory structure enabling (and thereby encouraging) searches. *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989).

The question presented here is whether the Ninth Circuit's rigid multi-pronged test for determining government action in relation to electronic communication service providers comports with the Fourth Amendment.

STATEMENT OF RELATED CASES

- *United States v. Rosenow*, No. 3:17-cr-3430-WQH, U.S. District Court for the Southern District of California. Judgment entered March 3, 2020.
- *United States v. Rosenow*, No. 20-50052, U.S. Court of Appeals for the Ninth Circuit. Opinion and order denying rehearing en banc entered October 3, 2022.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

OTHER AUTHORITIES

TABLE OF AUTHORITIES – Continued

PETITION FOR A WRIT OF CERTIORARI

Petitioner Carsten Rosenow respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINIONS BELOW

The Ninth Circuit's opinion is reported at 50 F.4th 715 (Pet. App. 1-53). The district court's opinion (Pet. App. 54-91) is unpublished.

JURISDICTION

The court of appeals entered judgment on October 3, 2022. Pet. App. 1. This Court has jurisdiction under 28 U.S.C. § 1254(1).

RELEVANT STATUTORY PROVISIONS

The relevant statutory provisions are lengthy and set forth verbatim in the appendix. Those statutory provisions include sections 2258A, 2258C, 2701, 2702, and 2703 of Title 18 as well as section 230 of Title 47.

STATEMENT OF THE CASE

1. More than a decade ago, electronic communication platforms were already "so pervasive" that people considered them "to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010). Thus, it has become "easier and easier for both government and private entities to amass a wealth of information" about ordinary people. *Riley v. California*, 573 U.S. 373, 408 (2014) (Alito, J., concurring). Major electronic communication service providers ("ESPs") now hold all "the privacies of life," for many people. *Riley*, 573 U.S. at 403. But whereas users may treat the digital storage holding their private communications as a "virtual home . . . Our most private information ends up being sent to private third parties." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209 (2004).

The business model of those private third parties, such as Yahoo, Google, and Facebook – which provide many of their communication platforms at no cost to consumers – frequently depend upon their ability to look at consumers' data. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. Telecomm. & High Tech. L. 359, 392 (2010) ("It is exceedingly difficult to monetize a data set that you cannot look at.").

The "virtual homes" holding private communications in this case were operated by Yahoo and

Facebook, two widely used ESPs.[1] This case presents a pressing question: what constitutes "government action" where ESPs hold and review users' most private communications, repeatedly meet with law enforcement to disclose and discuss it, and where law enforcement uses federal statutes to enable and encourage ESP searches and disclosures in support of law enforcement's investigative efforts targeting those users.

2. Realizing their unique access and incentives in relation to people's private communications, Congress has passed a series of interrelated laws aimed at empowering law enforcement while jointly deputizing ESPs to ferret out crime and report on their users.

One such law is the Stored Communications Act ("SCA"). The SCA "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Kerr, *Guide*, *supra*, at 1212. It does so by criminalizing "unlawful access to stored communications," while exempting the provider of the communication service. 18 U.S.C. § 2701. Additionally, the SCA limits ESPs' ability to voluntarily disclose customer communications

---

[1] *See Yahoo Inc. About*, YAHOO!, https://www.yahooinc.com/about/ (last visited December 20, 2022) [https://web.archive.org/web/20221219172533/https://www.yahooinc.com/about/] (boasting "platforms connect[ing] hundreds of millions of people around the world"); META, https://about.meta.com/company-info/ (last visited December 20, 2022) [https://web.archive.org/web/20221220041358/https://about.meta.com/company-info/] ("Our products empower more than 3 billion people around the world to share ideas and offer support").

to third parties, including law enforcement, except under narrow circumstances. 18 U.S.C. § 2702. The SCA further purports to grant law enforcement authority to compel ESPs to disclose the "modern-day equivalents of an individual's own 'papers'" without obtaining a warrant, a provision this Court has already said runs afoul of the Fourth Amendment. *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018). Finally, section 2703(f) of the Act enables law enforcement to order ESPs to preserve users' private communications.

Although the SCA gives ESPs access to, but precludes disclosure of, users' communications, 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" to the National Center for Missing and Exploited Children ("NCMEC") in the form of CyberTips. *United States v. Rosenow*, 50 F.4th 715, 725 (9th Cir. 2022). Congress enacted this reporting requirement in 2008 for the remedial goal of "securing adolescents from online exploitation." Pub. L. 110-401, 122 Stat. 4229 (Oct. 13, 2008). It further permits NCMEC to provide information to ESPs such as child pornography "hash values" or other information enabling ESP searches for such contraband. 18 U.S.C. § 2258C.

One "practical implication[]" of ESPs' access to and control over users' data and communications was a risk that "notice liability" might cause ESPs to "abstain from self-regulation." *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 333 (4th Cir. 1997). Thus, Congress

passed the Communications Decency Act ("CDA"). The CDA exempts ESPs from liability that might otherwise flow from criminal activity afoot in private communications over their platforms. *See, e.g.*, *Doe v. MySpace, Inc.*, 528 F.3d 413, 420 (5th Cir. 2008) (ESP was immune to suit stemming from sexual assault of minor facilitated by ESP's messaging service). In granting such immunity, one of the CDA's express objectives was "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity," 47 U.S.C. § 23(b)(5), by "encouraging voluntary monitoring" by private ESPs. *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003). To further the express objective of private monitoring of communications by ESPs, courts have repeatedly construed the CDA's grant of immunity "broadly." *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007).

The DOJ's Community Oriented Policing Guide ("COPS Guide") on combating Internet child pornography notes that Internet Service Providers ("ISPs") can be "crucial partners" in combatting child pornography offenses and the risk that ISPs are unaware of their obligations "makes is especially important for police to establish good working relations with ISPs to elicit their cooperation in the fight." Richard Wortley & Stephen Smallbone, *Child Pornography on the Internet* 36 (2006).

3. In this case, Yahoo, Facebook, the FBI, and the NCMEC repeatedly communicated about Carsten Rosenow over the course of years. The foregoing

statutory powers, permissions, immunities, reporting obligations, and relationships enabled Yahoo and Facebook to store, review, and repeatedly disclose the substance of Carsten Rosenow's private communications. In the process, both ESPs identified and turned over to Government via CyberTips, communications about travel for illicit sex with minors.

While attending a conference hosted by federal law enforcement, another private sector attendee informed the leader of Yahoo's "E-Crime Investigations Team," Sean Zadig, of possible child exploitation material on Yahoo's Messenger platform. U.S.C.A. Ans. Br. 11. A month later, that other private company had filed a CyberTip with NCMEC and provided information to Yahoo about ten of its users. *Rosenow*, 50 F.4th at 725. Zadig, who had prior experience in federal law enforcement, ensured Yahoo submitted a supplemental CyberTip identifying more than three hundred suspicious Yahoo account users. U.S.C.A. Ans. Br. 11. Yahoo separately notified both the FBI and Homeland Security Investigations ("HSI") of its CyberTip. *Rosenow*, 50 F.4th at 725. Yahoo's first pertinent CyberTip included "password protected" Yahoo Messenger chats that Yahoo had reviewed internally and subsequently disclosed. U.S.C.A. Ans. Br. 7, 11-12.

Zadig, Yahoo's in-house counsel, and agents from the FBI and HSI all met at NCMEC's headquarters in Virginia to discuss Yahoo's initial CyberTip. U.S.C.A. Ans. Br. 12-13. Meanwhile, the FBI opened its own investigation "to investigate Yahoo's evidence." *Rosenow*,

50 F.4th at 726. The foregoing CyberTips did not identify Rosenow or his Yahoo account as suspicious.

After this meeting, Yahoo continued to examine its users' data and communications. In December 2014, Yahoo made its second CyberTip, this time identifying Rosenow as communicating with others about traveling for illegal sex with minors abroad. *Id.* at 726. The foregoing CyberTip referring to Rosenow did not contain child pornography.

Federal agents with the FBI and HSI met a second time with Zadig at NCMEC headquarters to discuss Yahoo's second CyberTip findings. *Id.* Two days after that second meeting, Zadig sent the FBI agent involved a copy of the CyberTip so that the FBI could "cut and paste it into applications for warrants or other legal process." U.S.C.A. Ans. Br. 47.

Meanwhile, the FBI, without obtaining a warrant, sent Yahoo an order to preserve digital copies of hundreds of users' communications over Yahoo's platform pursuant to 18 U.S.C. § 2703(f). *Id.* The FBI sent additional preservation orders to Yahoo aimed at Rosenow's account in March 2015 and June 2015. *Id.*

HSI arrested a purchaser of child pornography based upon information in Yahoo's second CyberTip and Yahoo began going through that user's contacts and messages in search of other suspects. U.S.C.A. Ans. Br. 16. By the fall of 2015, Zadig's team at Yahoo had reviewed Rosenow's chats via the Yahoo Messenger platform and identified messages in which he asked for pictures of children with whom he was arranging

to have sex in the Philippines. *Rosenow*, 50 F.4th at 726.

Yahoo submitted a third CyberTip in December 2015 reporting its specific findings about Rosenow (including his private Yahoo Messenger chats). U.S.C.A. Ans. Br. 16. As they had done before, Yahoo and the FBI met a *third* time at NCMEC in February 2016 to discuss the latest CyberTip. *Rosenow*, 50 F.4th at 726.

Throughout its review of Rosenow's messenger chats, Yahoo never found any child pornography images. U.S.C.A. Ans. Br. 17. Indeed, Zadig knew the Messenger platform did not save any files shared between two users. *Id.* But Yahoo's user policies only permitted it to close user's accounts where they identify actual child pornography files. *Id.* Thus, notwithstanding the content of Rosenow's private messages, Zadig knew he could not terminate Rosenow's account. *Id.* Instead, Zadig "hoped that filing CyberTips to the NCMEC on Rosenow's activity [and meeting in-person with law enforcement about the same] 'might be a way to get the activity to stop.' " U.S.C.A. Ans. Br. 17. "The only means by which to prevent [Rosenow's] unlawful conduct was (as the government puts it) 'inviting a law enforcement response' and ensuring a successful prosecution." *Rosenow*, 50 F.4th at 743 (Graber, J., dissenting). Thus, even Yahoo's business incentive to prevent unlawful uses of its platform was "not *independent*," but rather depended upon coordinating with and enabling federal law enforcement efforts. *Id.*

In 2016, the FBI sought a warrant for Rosenow's Yahoo account, but the U.S. Attorney's Office rejected it remarking that the information (which omitted Yahoo's December 2015 CyberTip) "had become dated or stale." *Rosenow*, 50 F.4th at 726. The applicant FBI agent then received Yahoo's December 2015 CyberTip and learned Rosenow had a Facebook account. *Id.* As with Yahoo, she sent preservation orders to Facebook in January and May 2017, each requiring that Facebook keep copies of Rosenow's account communications and data. *Id.* During that process, the FBI agent informed Facebook that the nature of the investigation involved "child exploitation." C.A. Op. Br. 23. The FBI agent also sent administrative subpoenas to Facebook for subscriber information relating to Rosenow's account, marking those similarly as involving "child safety." *Rosenow*, 50 F.4th at 726.

The FBI's child safety and exploitation markings on its correspondence caused Facebook, based upon its own policies, to automatically review Rosenow's "messages, timelines, photos, IP addresses, and machine cookies." *Rosenow*, 50 F.4th at 727. When Facebook uncovered content in violation of its terms of use, it disabled Rosenow's accounts and filed two CyberTips with NCMEC. *Id.* The CyberTips included child pornography and messages negotiating sexual encounters with underage girls abroad. *Id.* The FBI acknowledges that Facebook sent information to NCMEC because of the FBI's requests which the FBI could not otherwise have obtained without a warrant. *Id.*

Ultimately, the warrant for Rosenow's arrest as well as the search and seizure of critical evidence in June 2017 was "based almost exclusively on information disclosed [by Yahoo and Facebook] through CyberTips from the NCMEC." *Rosenow*, 50 F.4th at 721. Rosenow was arrested and charged with attempted sexual exploitation of a child (18 U.S.C. § 2251(c)) and possession of sexually explicit images of children (18 U.S.C. § 2252(a)(4)(B)).

Before trial, Rosenow sought to suppress evidence that was the fruit of Yahoo's and Facebook's review and disclosure of his private correspondence. The district court concluded that neither ESP was a government actor and that, since the searches were performed by private actors, the Fourth Amendment did not protect Rosenow against any perceived intrusion on his privacy. At trial, the government relied principally upon evidence seized by virtue of its arrest and search warrant, including child pornography videos and images found on devices Rosenow possessed when he was arrested. *Rosenow*, 50 F.4th at 736. After he was convicted and sentenced to 25 years in prison, Rosenow appealed.

4. A divided panel of the Ninth Circuit affirmed. The panel's analysis to determine whether Yahoo's or Facebook's searches should be treated as government action for purposes of the Fourth Amendment is divided into three sections.

The first section assesses whether "federal law transform[s] the ESPs' private searches into governmental action." *Rosenow*, 50 F.4th at 729. The Ninth Circuit, attempting to distinguish Rosenow's case from *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602 (1989), held that the SCA and Protect Our Children Act do not convert Yahoo and Facebook into government actors as a matter of law. *Rosenow*, 50 F.4th at 730. The panel found it significant that the SCA "does not authorize ESPs to do anything more than access information already contained on *their* servers." *Id.* Then, as it relates to the Protect Our Children Act, the panel distinguished the law's mandatory reporting requirements from mandatory searches, noting that the law does not *require* searches. *Id.* Freed of any express requirement to search, the Ninth Circuit held that when ESPs "do search, they do so of their own volition." *Id.* Thus, the court held "that federal law [does] not transform Yahoo's and Facebook's private searches into governmental action." *Id.* at 731.

Next, the panel set aside whatever effect the controlling statutory framework might have on ESPs and assessed whether there is a "sufficiently close nexus" with government to constitute government conduct. *Id.* at 731. In analyzing *that* question, the court turned to "(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.*

Regarding the first prong of its government action test, the Ninth Circuit embraced a new sub-prong:

"unless a private party's search is illegal or based on an illegitimate motive" there must be "active participation or encouragement" by the government for a private search to implicate the Fourth Amendment. *Id.* at 733. In dissent, Judge Graber parted ways with her colleagues arguing that the appropriate test was merely whether law enforcement "knew of and acquiesced in" the ESPs' searches. *Id.* at 742. The majority reasoned that insofar as the SCA and their own privacy policies permitted Yahoo and Facebook to examine Rosenow's private communications, thereby rendering the examination legal, "active" participation in the searches (other than the repeated responsive meetings, correspondence, preservation orders, subpoenas, and repeated admonishment to ESPs that the foregoing implicated child safety) was necessary. *Id.* at 733. For the dissenting judge, the government's "implied consent to Yahoo's intrusive conduct is the very essence of acquiescence." *Id.* at 742.

The panel's disagreement extended to whether Yahoo "intended to assist law enforcement efforts or further [its] own ends." The majority accepted the ESPs' desire to protect their commercial brands by purging criminal conduct from their platforms as sufficiently independent to evade Fourth Amendment concern. *Id.* at 733-34. However, applying a slightly different test, the dissent concluded that only if an ESP could accomplish its private objective without law enforcement assistance does such an objective qualify as "independent." *Id.* at 742. In this instance, since Yahoo could only stop Rosenow's use of its platform by

persuading law enforcement to intervene, Judge Graber argued in dissent that "Yahoo's legitimate motive was not *independent*." *Id.* at 743.

5. This petition follows.

REASONS FOR GRANTING THE PETITION

I. This Case Presents an Important Question on the Scope of Government Action in Relation to Electronic Communication Providers About Which the Ninth Circuit is Wrong.

Rosenow's case is not unique. Virtually all of NCMEC's more than 29 million CyberTips came from ESPs in 2021.[2] Meanwhile, virtually every major ESP has elected to search for reportable information that they then disclose to NCMEC. *Id.* Federal law enforcement command ESPs to preserve copies of data from "hundreds of thousands of Internet accounts" each year. Orin Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Louis Univ. L.J. 753, 756 (2021). As it relates to the investigation of Mr. Rosenow, over the course of multiple reports, meetings, and correspondence about its users' messages, Yahoo sent NCMEC, the FBI, and HSI hundreds of users' password protected communications even though its

[2] 2021 CyberTipline Reports by Electronic Service Providers ("ESP") (2022) [http://web.archive.org/web/20221220075238/https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf].

Messenger platform did not preserve child pornography.

A set of statutes enable such searches, encourage them, and compel disclosure of successful searches. Meanwhile, the FBI contemporaneously, repeatedly, and without warrants sent orders to ESPs compelling preservation of Rosenow's accounts. But because those searches and disclosures are legally permitted, the Ninth Circuit held that suppression is only available if the government does something *more active*. The Ninth Circuit's "active" participation prong fails to account for the surrounding statutory framework, ignores the ways in which law enforcement actively encourage the ESPs' search efforts, and would permit millions of users' private communications to be subject to warrantless review and disclosure without implicating the Fourth Amendment at all.

1. This Court should grant certiorari, in part, because the Ninth Circuit's mode of analysis is wrong. The Court has rejected rigid tests where the Fourth Amendment encounters diverse factual and legal circumstances. *Illinois v. Gates*, 462 U.S. 213, 232 (1983). Instead, where private searches might appropriately be treated as government searches, this Court has required "a fact-bound approach to this attribution question, one that uses 'different factors or tests in different contexts.'" *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020) (citing *Lugar v. Edmondson* Oil Co., 457 U.S. 922, 939 (1982)). Furthermore, advance government knowledge alone can invoke the Fourth Amendment's protections. *United States v. Jacobsen*, 466 U.S. 109,

113-14 (1984). Here, the Ninth Circuit's test runs afoul of this Court's precedent while inventing new, specific requirements that are ill-suited to analyzing the government's relationship to ESPs where those ESPs hold most peoples' private correspondence.

First, the Ninth Circuit's analysis examined the surrounding statutory framework in isolation. But the question of Government action "can only be resolved 'in light of all the circumstances.'" *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989). Thus, in *Skinner*, this Court rejected any analysis that would evaluate the question piecemeal or make any one factor dispositive.

Here, the Ninth Circuit erroneously analyzed the SCA and the Protect Our Children Act separate from one another and without regard to the CDA.[3] Furthermore, the Ninth Circuit overlooked the specific statutory interrelationships at issue in Rosenow's case – and the way the governing statutes impacted them. For example, the Ninth Circuit noted that the Protect Our Children Act expressly states that its provisions shall not be construed to require ESPs to search users' communications and that "Mandated *reporting* is different than mandated *searching*." *Rosenow*, 50 F.4th at 730.

---

[3] The Ninth Circuit declined to consider the CDA's role in encouraging ESPs to search their users' communications. *Rosenow*, 50 F.4th at 731 n.4. However, since it does not present a factual issue that might have been best developed in district court, it is appropriately before the Court here. *Hormel v. Helvering*, 312 U.S. 552, 557 (1941).

But this Court has never limited its government action analysis to situations where the statute *compels* a private search. Such a question hardly even arises where the law is so clear. *See, e.g.*, *Skinner*, 489 U.S. at 614 ("A railroad that complies with the provisions 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."). Similarly, the Court has expressly disapproved of any fixed line between private and government action that does not account for functional circumstances of the search in issue. *Lustig v. United States*, 338 U.S. 74, 78 (1949).

The Ninth Circuit's analysis belies the relationship between the various implicated laws and runs afoul of both *Lustig* and *Skinner*. Here, as in *Skinner*, the SCA, Protect our Children Act, and CDA reflect more than a "passive position toward the underlying" ESP searches of users' private communications. *Skinner*, 489 U.S. at 615. First, as in *Skinner*, the SCA removed legal barriers that would otherwise preclude ESPs from reading users' communications. 18 U.S.C. § 2701. Additionally, the law made clear government's hope to share in the fruit of ESPs' access – it empowered law enforcement to obtain private data without a warrant (which this Court has since held unconstitutional in *Carpenter v. United States*, 138 S. Ct. 2206 (2018)) and created powers such as the preservation orders used here. 18 U.S.C. § 2703. Of course, in isolation, the SCA may not clearly indicate the Government's desire to share in the fruit of ESPs' private searches insofar as it prohibits ESPs from disclosing

the content of users' communications to law enforcement except under limited, inapplicable circumstances. 18 U.S.C. § 2702. In that respect, the SCA standing alone differs meaningfully from *Skinner*.

But the Protect Our Children Act made plain the government's "desire to share the fruits of such intrusions." *Skinner*, 489 U.S. at 615. In fact, just like the regulations at issue in *Skinner*, the Protect Our Children Act gives NCMEC a "right to receive," *id.*, the fruit of the ESPs' searches in the form of mandatory CyberTips. 18 U.S.C. § 2258A.[4] Leaving little doubt about what Congress hoped ESPs would do, the Act also gave NCMEC authority to publish child pornography hash values for use by private parties searching digitally for child pornography. 18 U.S.C. § 2258C. There would have been little reason to give NCMEC such authority unless Congress hoped to encourage and enable effective private searches.

Nor does the Ninth Circuit's distinction between mandatory reporting and mandatory searching bear the weight placed upon it to distinguish the Protect

---

[4] Rosenow argued below that NCMEC is itself a government actor, such that its receipt of CyberTips, disclosures to the FBI, and encouragement of private searches implicate the Fourth Amendment. The government, for its part, did not dispute that NCMEC is a government actor. U.S.C.A. Ans. Br. 45 n.8. Neither the district court nor the Ninth Circuit decided whether NCMEC is a government actor, but the Ninth Circuit acknowledged "good reason to think" it is. *Rosenow*, 50 F.4th at 729 n.3 (citing *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) (Gorsuch, J.)).

Our Children Act from other laws implicating the Fourth Amendment. As this Court held in *Lustig*:

> [i]t surely can make no difference whether [private party] turns up the evidence and hands it over to a federal agent for his critical inspection with the view to its use in a federal prosecution, or the federal agent himself takes the articles out of a bag. It would trivialize law to base legal significance on such a differentiation.

Lustig, 338 U.S. at 78. Elsewhere, the Court has similarly rejected "attempts to disaggregate the taking and testing of [private matter] from the reporting of the results to the police." *Ferguson v. City of Charleston*, 532 U.S. 67, 77 n.9 (2001).

Here, as in *Lustig*, government actors specifically identified the evidence they sought from ESPs' searches. Congress did so when determining what ESPs would be required to report to NCMEC. 18 U.S.C. § 2258A. Furthermore, federal law enforcement encouraged such efforts by repeatedly meeting with Yahoo to discuss and sift through what Yahoo was turning over in its CyberTips. The FBI did the same when it repeatedly sent orders to Facebook regarding its users' data labeled "child exploitation." Although neither NCMEC nor the FBI appear to have helped "empty the [digital] containers" of users' communications, they nonetheless "share[d] in the critical examination of the uncovered articles" as the ESPs' searches proceeded, *Lustig*, 338 U.S. at 78.

Finally, removing any doubt about the government's desire that ESPs aggressively police (and then report) unlawful activity on their platforms, the CDA removed a practical barrier to ESPs' searches by immunizing them from civil liability. In *Skinner*, the Court found it significant that the law prevented railroads from contracting away the authority to perform the discretionary searches of employees. *Skinner*, 489 U.S. at 615. A similar practical concern about how ESPs might behave motivated the CDA. Courts have broadly construed ESPs' immunity pursuant to the CDA precisely because it was meant to *encourage* ESPs to proactively analyze communications on their platforms. 47 U.S.C. § 23(b)(5); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003). More specifically, Congress expressly hoped "to ensure vigorous enforcement of Federal criminal laws" like those with which Mr. Rosenow was convicted. 47 U.S.C. § 230(b)(5). Just like the regulations in *Skinner* "preempted conflicting state laws," *Rosenow*, 50 F.4th at 729, the CDA preempts state laws that might otherwise permit private suit against ESPs based upon communications through their platforms.

The foregoing combination of laws and the surrounding circumstances of the years' long investigation between Yahoo and the FBI in this case offer "clear indices of the Government's encouragement, endorsement, and participation," implicating the Fourth Amendment, *Skinner*, 489 U.S. at 615. But the Ninth Circuit analyzed each law individually, testing whether any specific law "transform[s] the ESPs'

private searches into governmental action." *Rosenow*, 50 F.4th at 729. That is not the test this Court articulated in *Skinner* and *Lustig*.

2. Contrary to *Skinner*, in its subsequent analysis of whether the government knew of and acquiesced to the ESPs' searches, the Ninth Circuit construed the foregoing legal framework as weighing *against* a finding of government action. Specifically, the Ninth Circuit concluded that because the ESPs' searches were "legally permissible" under the prevailing statutory framework, Rosenow was required to prove "active participation or encouragement." *Id.* at 733.

However, that is not the law.

As an initial matter, the ESP's privacy policy claiming to afford the ESP some modicum of access to Rosenow's communications did not vitiate his reasonable expectation of privacy in his communications. This Court has left users' reasonable expectations of privacy in voluminous, private data held by ESPs undisturbed, notwithstanding the fact that users could be said to have voluntarily disclosed that data to modern communications companies. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). Even the dissent in *Carpenter* seemed to concede that private communications – as opposed to mere location data – would not be governed by the third-party doctrine. *See id.* at 2230 (Kennedy, J., dissenting) ("*Miller* and *Smith* [the leading third-party cases] may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those

papers or effects are held by a third party.") (citing *Ex parte Jackson*, 96 U.S. 727, 733 (1878) (letters held by mail carrier)).

Nor does Rosenow's acquiescence to ESPs' privacy policies imply consent insofar as the Court's Fourth Amendment doctrine is concerned. *Bumper v. North Carolina*, 391 U.S. 543, 548-49 (1968).

If the Ninth Circuit were correct that lawful private searches can only be government action where government agents took an active role, the discretionary searches at issue in *Skinner* would fail the Ninth Circuit's test. In *Skinner*, the law at issue made the railroad's searches and subsequent disclosures legal. Considering a facial challenge to the law, there was no evidence that law enforcement engaged in "active participation or encouragement" other than structuring the law to enable the searches in the first place. Thus, the Ninth Circuit below weighed the surrounding legal permissions in precisely the opposite way than those in *Skinner*. In *Skinner*, the prevailing legal permissions weighed in favor of Fourth Amendment scrutiny, but here the Ninth Circuit held Rosenow to a heightened burden considering the legal permissions granted to ESPs.

The surrounding legal permissions were especially important here because Yahoo could not close Rosenow's account without provoking a law enforcement response. Whereas the SCA "places limits on the ability of ISPs to voluntarily disclose information about their customers and subscribers to the

government," Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209 (2004), the Protect Our Children Act both exempted disclosures of certain information and mandated such disclosures. Thus, insofar as the SCA generally prohibits disclosure of users' communications to law enforcement, the Protect Our Children Act's mandatory reporting requirements told Yahoo one of the only things that it should search for – thereby encouraging such a search.

Still worse, rather than considering all the attendant actions by law enforcement, the Ninth Circuit's narrow view of what constitutes "active" involvement by government contradicts this Court's teaching that "search is a functional, not merely a physical process" and that government action occurs where a federal agent joined the search "before it had run its course." *Lustig*, 338 U.S. at 78. Here, the FBI repeatedly met with Zadig during Zadig's review of Rosenow's communications at Yahoo and ordered both Yahoo and Facebook to save copies of his accounts. That law enforcement hoped to encourage ESP searches is further revealed by their repeatedly using the statutory tools available to inform Facebook that it was investigating child exploitation. *Rosenow*, 50 F.4th at 726 & 732.

Here, the years of law enforcement cooperation, acquiescence, and follow-up administrative orders can only be "characterized as the proverbial 'wink and a nod'" to the ESPs. *United States v. Jarrett*, 338 F.3d 339, 343 (4th Cir. 2003); *see* Eugene L. Shapiro,

Governmental Acquiescence in Private Party Searches: The State Action Inquiry and Lessons from the Federal Circuits, 104 Ky. L.J. 287, 321 (2016) (noting that cues from law enforcement will often evade constitutional restraints absent court acknowledgement that law enforcement encourages private searches in subtle ways). But in the Ninth Circuit's mode of analysis, none of these facts or the surrounding law constitute an "active" role by government because they occurred *after* Yahoo began its search of Rosenow's chats and the FBI was not physically present with Yahoo's investigators while they performed their initial review. *See Rosenow*, 50 F.4th at 733 ("government actors are not even present during the search").

3. Finally, analyzing the ESPs' motives for searching, the Ninth Circuit's test asks only whether some independent objective might ultimately be served by the private party's search. *Id.* at 735. Under that test, only entirely selfless acts aimed solely at helping law enforcement might implicate the Fourth Amendment. But, as the dissent argued below, this provision of the Ninth Circuit's gauntlet of requirements runs afoul of *Ferguson v. City of Charleston*, 532 U.S. 67, 82-84 (2001).

In *Ferguson*, the Court analyzed a program for drug testing women and disclosing positive urine screens to law enforcement as a means of coercing patients into substance abuse treatment. *Id.* at 80. Law enforcement defended the searches and associated policy on grounds that a "special need" justified warrantless searches. *Id.* at 79. Examining "all the available

evidence to determine the relevant primary purpose," this Court held that:

> [w]hile the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence for law enforcement purposes in order to reach that goal. The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose of [the] policy was to ensure the use of those means. In our opinion, this distinction is critical.

Id. at 82-84.

This Court noted that the state hospital employees in *Ferguson* may have duties to disclose certain things they inadvertently learn in the course of their work for patients, just "like other citizens" who are not employed in government. *Id.* at 84-85. But what made the state hospital employees' different from private citizens was that they sought evidence "*for the specific purpose of incriminating those patients*." *Id.* at 85 (emphasis original). That the effort might be a means to some other arguably independent motivation was of no moment. *Id.* So it was here.

Here Yahoo acknowledged, and the government conceded, that the immediate objective of its searches of Rosenow's message records (which Yahoo knew would not contain child pornography files permitting it to close the account) was to cause an arrest and prosecution. *Rosenow*, 50 F.4th at 743. Thus, *Ferguson*

should have counseled in favor of a finding of government action because Yahoo's "immediate objective" was to "generate evidence for law enforcement purposes in order to reach [its] goal." *Ferguson*, 532 U.S. at 83.

Nor is the Ninth Circuit correct that *Ferguson* is "flatly distinguishable" as merely concerning the "special needs" doctrine rather than a question of private searches, *Rosenow*, 50 F.4th at 736 n.5. The Court's "special needs" doctrine frequently involves an analysis of the searching-party's intent and attendant association to law enforcement analogous to courts' assessment of private searches. As in the private search context, the Court has focused on whether those performing the search were "acting alone and on their own authority" rather than "at the behest of law enforcement." *New Jersey v. T.L.O.*, 469 U.S. 325, 342 n.7 (1985); *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 666 (1989) (drug-testing program was "not designed to serve the ordinary needs of law enforcement"); *Ferguson*, 532 U.S. at 81 n.17 ("Under our precedents, if there was a proper governmental purpose other than law enforcement, there was a 'special need.' ").

Despite the clear application of *Ferguson*, the Ninth Circuit held to the contrary that a party's "otherwise legitimate, independent" objective would not be rendered invalid just because law enforcement may further that objective. But, where ESPs specifically search their users' private communications to cause an arrest or prosecution to serve some private end, the ESPs' objective is "dependent on – not independent

from" a law enforcement objective. *Rosenow*, 50 F.4th at 742 (Graber, J., dissenting).

The agency question "ensconced in the law at the time of the founding" would have usually asked "simply whether the agent acts with the principal's consent and (in some way) to further the principal's purpose." *United States v. Ackerman*, 831 F.3d 1292, 1301 (10th Cir. 2016). The combination of the SCA, Protect Our Children Act, CDA, and years of coordination between the FBI and ESPs plainly manifested the government's consent to both Yahoo's and Facebook's searches of Rosenow's private messages. Nor is there meaningful dispute that Yahoo and Facebook acted to further the government's purpose. The Ninth Circuit's requirement of "active" effort by the government *before* the searches in issue and notwithstanding the prevailing legal structure already in place before the searches "depart[s] from and demand[s] more than the common law did to establish an agency relationship," *id.* It also departs from *Skinner*, *Lustig*, and *Ferguson*. This Court should correct the Ninth Circuit's error on such an important issue of federal law.

II. The Court Should Also Grant Review to Resolve Circuits' Increasingly Divergent Agency Tests.

The Ninth Circuit's requirement that law enforcement have "active" participation or encouragement and disregard of Yahoo's multiple intentions place it at

odds with other circuits, which have expressed a broad range of tests for agency in relation to searches.

In the Tenth Circuit, as Justice Gorsuch explained in *United States v. Ackerman*, the prevailing test remains "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends." 831 F.3d 1292, 1301 (10th Cir. 2016).

In *Ackerman*, the Tenth Circuit confronted whether a review of someone's email by NCMEC staff constituted government action and had little trouble concluding that it did. *Id.* at 1308. But unlike the Ninth Circuit here, the *Ackerman* court did not inquire whether federal law enforcement had played some "active" part in NCMEC's discretionary decision to search the emails. Nor did the Tenth Circuit conclude that the legality of the searches in issue militated against a finding of government action. On the contrary, applying *Skinner*, the Tenth Circuit concluded that the "comprehensive statutory structure" themselves illustrated government "knowledge of and acquiescence in" the possibility NCMEC would read emails in its possession. *Id.* at 1302.

In further contrast to the Ninth Circuit's newly minted requirements, the Tenth Circuit expressly rejected a test wherein "a private party who bears *any* private purpose cannot serve as a governmental agent." *Id.* at 1303. Whereas the Ninth Circuit deemed Yahoo's profit-motive as wholly independent even

though it acknowledged hoping to help law enforcement prosecute Rosenow, *Rosenow*, 50 F.4th at 743 (Graber, J., dissenting), the Tenth Circuit "recognized that agents routinely intend to serve their principals with the further intention to make money for themselves." *Ackerman*, 831 F.3d at 1303. In fact, as the *Ackerman* court observed, the private railroads had similar economic reasons to seek to curb drug abuse by employees, but that fact did not preclude an agency finding in *Skinner*. *Id.*

Although the Tenth Circuit's decision in *Ackerman* is in an analogous context and flatly contravenes the analysis by the Ninth Circuit here, the Tenth Circuit is not the only one to reject the requirements now embraced as dispositive by the Ninth Circuit. *See, e.g.*, *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997) ("any specific 'standard' or 'test' is likely to be oversimplified or too general to be of help, and [. . .] all of the factors mentioned by the other circuits may be pertinent in different circumstances"); *United States v. Miller*, 982 F.3d 412, 422 (6th Cir. 2020), *cert. denied*, 210 L. Ed. 2d 929 (2021) (asking whether any of three tests is met: (1) whether the party performs a public function, (2) whether it was subject to compulsion, or (3) whether a private party's intent and "government acquiesce[nce]" reveal that the private party "cooperated with the government").

This Court should grant review resolve the appropriate agency test in relation to ESPs given the wide variety of tests, including "more stylized agency tests," that appear to "depart from and demand more than

the common law did to establish an agency relationship." *Ackerman*, 831 F.3d at 1301.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

TIMOTHY SCOTT
Counsel of Record
MARCUS BOURASSA
MCKENZIE SCOTT P.C.
1350 Columbia, Suite 600
San Diego, CA 92101
(619) 794-0451
tscott@mckenziescott.com

December 30, 2022