No. 24-6254

ORIGINAL

IN THE
SUPREME COURT OF THE UNITED STATES

RYAN GALAL VAN DYCK
Petitioner,

vs.

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 WRIT OF CERTIORARI

RYAN G. VAN DYCK
41206-408
PO Box 1000
Petersburg, VA 23804

Pro Se Petitioner

QUESTION PRESENTED TO THE COURT

1. The Sixth Amendment is paramount to defendants in a criminal proceeding to ensure effective assistance of counsel. When this doesn't happen, there is no fair proceedings or justice. Here, trial counsel failed to raise a critical issue where police conducted a warrantless search of an email attachment which uncovered evidence used to support probable cause for a search warrant that allowed evidence that was key to my conviction. At the time, there was both binding and persuasive caselaw prohibiting this unconstitutional search. But for counsel's failure to research, the outcome of the case would have been different. Did the lower courts err by concluding th that trial counsel was strategic to abandon this ground - especially given that proof was provided trial counsel pursued the exact defense in state court after realizing his critical error?

PARTIES AND PROCEEDINGS

All parties to the proceedings are listed in the caption. The Petitioner is not a corporation.

This case arises from the following proceedings in the United States District Court for the District of Arizona and the United States Court of Appeals for the Ninth Circuit: VanDyck v. United States, No. 4:21-cv-00399-CKJ (D. Ariz. Dec, 15, 2022) and VanDyck v. United States, Ninth Cir. No. 23-15109 (9th Cir. 2024).

RELATED PROCEEDINGS

I am unaware of any other proceedings in any other court that are directly related to this case. However, this case had a direct impact in denying relief in my state case.

Table of Contents

Table of Authorities

Statutes

Other

Introduction

The Sixth Amendment protects the accused from unprofessional errors by defense counsel that leave defendants vulnerable to unfair prosecution. Here, defense counsel failed to research the facts and law related to Fourth Amendment protections of email content and Electronic Service Provider (ESP) cybertip processes.

In this case, law enforcement examined an email attachment flagged by America Online (AOL). AOL did not physically review the attachment. It was software, designed to detect files passing through AOL's network. It is unknown, who, when or why the file was flagged as illicit pornography. The software matches hash values, similar to a label, suggesting the file may be illegal. But no information about the content is available. The question is, does law enforcement have the right to open an email attachment file, not previously examined by AOL, without a warrant?

This Court answered this question over forty years ago. "The fact that the labels on the box established probable cause to believe the films were obscene clearly cannot excuse failure to obtain a warrant; for if probable cause dispensed with necessity of a warrant, one would never be needed." Walter v. United States, 447 U.S. 649, 657 n. 10 (1980).

The email attachment here had Fourth Amendment protections both under the digital property-trespass and expectation of privacy framework. There was no private search. AOL's terms of service indicated all content posted to their services (email) remained a user's property, buttressing property protections and excluding the application of the Third-party doctrine.

Law enforcement's search was illegal. The evidence should have been suppressed. The district court's findings conflicted with binding authority. At the time, the available caselaw favored this issue. The liklihood of success was strong because a similar case on this ground was successful in my Circuit. But for counsel's errors, the outcome of my case would have been different. I humbly pray for relief from this Court under the Fourth and Sixth Amedment.

Opinions Below

The Court of Appeals' opinion affirming the district court's denial of my 28 U.S.C §2255 motion is unreported and attached. Appendix A. The district court's order denying relief of my 28 U.S.C. §2255 motion is unreported and attached. Appendix B. The court of appeals' order denying my petition for rehearing is unreported and attached. Appendix C. The state of Arizona court of appeals opinion is unreported and attached for information purposes. Appendix F.

Jurisdiction

The judgement of the United States Court of Appeals for the Ninth Circuit was April 5, 2024. Appendix A. My petition for rehearing was denied by that court April 22, 2024. Appendix C. On June 27, 2024, the Honorable Justice Kegam extended time for filing my petition in this Court until September 19, 2024 (23A1161). Appendix D. On September 18, 2024, I attempted to mail this Petition legal mail from my prison but was deprived access. After speaking to this Court's clerk office, I submit it for consideration. This Court's jurisdiction is invoked under 28 U.S.C. § 1241(1).

Constitutional Provisions Involved

The Fourth Amendment to our Constitution provides:

> The right of the people to be secure in their papers, houses papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Sixth Amendment of our Constitution provides:

> In all criminal prosecutions, the accused shall enjoy the right... to have the Assistance of Counsel.

Statement of Case

Procedural History

I was convicted of conspiracy to produce child pornography and possession of child pornography following a bench trial. [District of Arizona 4:15-cr-00742]. I appealed to the Ninth Circuit [Ninth Cir. No. 10524] and they affirmed.[1] I filed a petition for certiorari to this Court [Scotus No. 19-8596], which was denied October 5, 2020.[2]

On October 4, 2021, I filed a motion under 28 U.S.C. §2255 to vacate, set aside or correct a sentence. [District of Arizona no. 4:21-cv-00399]. The district court denied my request for an evidentiary hearing, denied the motion, and dismissed the case with prejudice. The court issued a certificate of appealability on the claim of ineffective assistance of trial counsel (the issue raised in this petition), but didn't on my second claim. Appendix B.

1. United States v. VanDyck, 776 Fed. Appx. 495 (9th Cir. 2019)
2. VanDyck v. United States, 141 S.Ct. 295 (Mem) (2020)

On August 14, 2023, I appealed to the Ninth Circuit. [Ninth Cir. No. 23-15198]. The court affirmed the district court's denial of my 28 U.S.C. §2255 motion. App. B.

Facts Relevant to Review

In March of 2014, America Online (AOL) detected an email attachment suspected of containing child pornography. The attachment was sent from AOL account: "doudykid@aim.com." The attachment was detected with softare using a method called Image Detection Filtration Process (IDFP).[3] AOL maintains a database of hash values that at some point, someone opined may be child pornography.[4] AOL also blindly receives hash values from other ESP's.[5] When AOL detects a file passing through its network with a corresponding hash in their database, a cybertip is automatically generated to the National Center for Missing and exploited Children (NCMEC). However, no AOL employee reviews the file prior to the cybertip submission. This determination is made soley on software.[6]

Once NCMEC receives the tip, they conduct a preliminary review and find the origin of the email IP address. In this case, the email was geolocated to Comcast Cable in Tucson, Arizona. Tucson Police Department (TPD) received the cybertip and email attachment and opened it without a warrant. TPD then drafted a warrant affidavit and provided a graphic description

3. IDFP is a program that compares file properties that pass through a network by matching "hash values" of files previously suspected to be illicit. See United States v. Keith, 980 F.Supp.3d 33 (D. Mass. 2013) Below, the government did not dispute the cybertip process as dilineated in Keith.
4. Id.
5. Id.
6. Id.

of this suspect email attachment to support probable cause. It was the fruits of this warrant that is the basis for this case.

REASONS FOR GRANTING THE WRIT

Consistent with Rule 10 (a)&(c) of this Court, there are compelling reasons to grant this petition for writ of certiorari.

The Circuit Court's ruling departed from this Court's framework under Strickland v. Washington, 466 U.S. 668 (1984) by concluding trial counsel strategically omitted this claim. Specifically, clear evidence was submitted proving that trial counsel pursued this ground in state court but could not do so in federal court because it was too late. The Circuit court ignored this pivotal evidence.

Now, recently affirmed by the Ninth Circuit, the Arizona district court concludes: emails "generally" have Fourth Amendment protections; however, the mere presence of contraband eliminates it. In other words, a warrantless search can be justified by the discovery of evidence. This departs from clearly established federal law and puts our nation's citizens at great risk by validating otherwise illegal searches. Additionally, other courts may find this approach persuasive to deny relief to other defendants. This incorrect ruling has already effected my state relief efforts. See App. E, ¶¶ 3, 11. This Court's supervisory supervisory authority is necessary to resolve it.

Many recent decisions of this Court have demonstrated a concern for the Fourth Amendment and its application to emerging technology. See Carpenter v. United States, 138 S.Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014); City of Ontario v. Quon,

560 U.S. 746 (2011). In Carpenter, each Justice on this Court contributed to or was in agreeance that our Fourth Amendment protects digital information. Id. at 2206, 2222, 2230, 2262, 2269.

There are signifigant concerns that need to be resolved. Are lower courts correct to justify warrantless searches based on discovery of contraband? How far does the private search exception apply, especially when law enforcement clearly establish probable cause based on their examination of evidence; not the private parties. Does the Third-Party doctrine really apply to emails: when the account belongs to the user. Given these critical concerns of our nation's privacy, this Court should grant this petition to resolve these issues.

1. Trial Counsel Rendered Ineffective Assistance of Counsel for His Ignorance of the Law and Failure to Conduct Research

The standard for ineffective assistance of counsel is in Strickland v. Washington, 466 U.S. 668 (1984). First, whether counsel's performance fell below an objectively reasonable standard (deficiency); and second, that the deficiency prejudiced the Petitioner (a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. Id. at 688, 694.

"An attorneys ignorance of a point of law that is fundamental to his case combined with his failure to perform basic research on that point is a quintessential example of unreasonable performance under Strickland." Hinton v. Alabama, 571 U.S. 263, 274, (2014)

In my case, trial counsel simply did not research the law on

Fourth Amendment protections of email content or AOL's cybertip processes. The fruits of the email content illegally examined by law enforcement was basis for the entire case. There were binding cases in my Circuit that established email protections and another case that provided direct foundation to the illegality of law enforcement's search. These cases would have led to other authority that supported this ground.

Without analysis, the Ninth Circuit accepted the district court's ruling that trial counsel strategically abandoned this ground in favor of stronger arguments. VanDyck v. United States, 2024 WL 1477398 (9th Cir. 2024) at *2. However, this finding is contrary to the evidence provided. During the pendency of my federal appeal, trial counsel pursued this exact ground in state court as it was in pre-trial posture. (FER-27-59)[7] The district and appellant court do not acknowledge this evidence.

Regarding Fourth Amendment issues, this Court has acknowledged that "a single, serious error may support a claim of ineffective assistance of counsel." Kimmelman v. Morrison, 477 U.S. 365, 383 (1986) (citation omitted). This was my strongest ground for relief. The Circuit Court conceded at oral argument that the warrantless search of the email attachment was "the key to the door" to my entire case. There is no doubt that this failure was "unreasonable" and not "sound strategy." Strickland, 466 U.S. at 688-89.

7. In this Petition, district court records are referenced. Excerpts of Record "ER" (Doc. No. 18) and Further Excerpts of Record "FER" (Doc. No. 36) are found in Ninth Circuit Appellant Docket, Case No. 23-15198.

This failure also harmed me. Because trial counsel failed to research the protection of emails and the cybertip process, evidence came into trial that was unconstitutionally seized. The first search warrant of my home was invalid because the information supplying probable cause was obtained in an unconstitutional search of my email. Without evidence seized from my home, there would be no second (federal) search warrant. All evidence would require suppression under fruits of the poisonous tree. Wong Sun v. United States, 371 U.S. 471, 488 (1963). Thus, "there is a reasonable probability that the verdict would have been different absent excludable evidence." Kimmelman, 477 U.S. at 375.

Prejudice is established by demonstrating a strong liklihood of success had this issue been raised. I did so below and herein. The Circuit Court did not conduct any analysis. This analysis is relevant to establish prejudice.

Prejudice is especially established here because this claim was successful in my Circuit. Prejudice can be evaluated with the benefit of hindsight. Lockhart v. Fretwell, 506 U.S. 364, 372 (1993). My Circuit reversed a district court's denial of a motion to suppress on the same ground. See United States v. Wilson, 13 F.4th 961 (9th Cir. 2021).[8] But for counsel's mistake, the leading case in my Circuit may have well been "United States v. Van Dyck.

8. See VanDyck v. United States, 2022 WL 17689168 (D. AZ 2022) at *6 (district court conceding "Under Wilson, the record in [my] case would support suppression of the evidence gathered pursuant to the warrantless search of the email attachment."

Therefore, counsel's mistake to not investigate, research and not raise this issue was ineffective assistance of counsel.

2. Law Enforcement Violated My Fourth Amendment Rights by Conducting a WarrantlessSearch of my Email Contents.

The Fourth Amendment prohibits unreasonable searches and seizures. The "basic purpose of this Amendment ... is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." Carpenter, 138 S.Ct. at 2213 (citation omitted). "Warrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of wrongdoing." Id. at 2221 (citation omitted).

A Fourth Amendment search can occur in either of two occassions. First, a "search" can also occur when law enforcement intrudes or trespasses upon a constitutioally protected area - "papers, houses, papers, [or] effects" - for the purpose of obtaining information." United States v. Jones, 565 U.S. 400, 404 (2012). Second, there is a "search" within the Fourth Amendment when law enforcement infringes on "an expectation of privacy that society is prepared to consider reasonable[.] United States v. Jacobsen, 466 U.S. 109, 113 (1984). In my case, law enforcement violated my Fourth Amendment rights both by trespassing on my digital property and searching email content that I had a reasonable expectation of privacy.

There was substantial authority to support this claim. As demonstrated below, trial counsel was Constitutionally deficient for failing to protect my Fourth Amendment rights.

A. Law Enforcement Violated My Property Rights in Email Content

Over a century ago, this Court established property principles in mail, stating, "[l]etters and sealed packages ... in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding to their own domiciles." Ex Parte Jackson, 96 U.S. 727, 733 (1877). Therefore, it's "[t]he constitutional guaranty of the right of the people to be secure in their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant as is required when papers are subjected to search in one's own household." Id.

This concept has been applied to email around this country for over a decade because email "is the technological scion of tangible mail, and it plays a indispensable part in the Information Age." United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010). This is because email is used to "send sensitive and intimate information instantaneously, to friends, family, and colleagues half a wold away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button." Id. at 284. And for over a decade, this Court has "consider[ed] [email] to be essential means or necessary instruments for self-expression, even self identification." City of Ontario v. Quon, 560 U.S. 746, 760 (2010).

Critically, in this case, the Ninth Circuit was very explicit about the protection of emails holding "[email] implicates the Fourth Amendment's specific guarantee of the people's right to

be secure in their 'papers.' The express listing of papers' reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas - what we might call freedom of conscience - from invasion by the government." United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (citation omitted).

As now-Justice Gorsuch wrote, "an email is a 'paper' or 'effect' for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more." United States v. Ackerman, 831 F.3d 1292, 1304 (10th Cir. 2016) (citing Cotterman, 709 F.3d at 964). Therefore, when law enforcement conducts a warrantless search of emails and their attachments, "that seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." (Id. at 1307). Though "the framers were concerned with the protection of physical mail rather than virtual correspondence[,] a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have already applied common law's ancient trespass to chattels doctrine to electronic, not just written, communications. (Id. at 1308) (citing cases).

In this case, trial counsel had various cases available to him to support that emails and their enclosures had property interests under the Fourth Amendment. This failure to research the law was deficient and this error harmed me because it permitted illegally obtained evidence to secure a conviction against me.

The government never contested that emails have property protections under the Fourth Amendment and did not contest that my trial counsel was deficient for failing to raise this issue or that it harmed me under Strickland. The Ninth Circuit did not provide any analysis on the substance of this argument.

i. The Third Party Doctrine Does Not Apply to Email Content

Emails have property and possessory interests that belong to the user. This remains true even if a user sends email through third-party internet service providers (ISP).

AOL specifically states that "the owner of any content that [is] posted to [AOL's] service retains ownership of all rights, titles and interests of that content." See AOL Terms of Service (2-ER-178-197). This is because AOL does not use the content of emails for any legitimate business purpose. The content posted to their service (such as email) is done for the explicit purpose of delivery to an intended recipient. Therefore, email content does not fall under the third-party doctrine.

The "third-party doctrine" found its roots in United States v. Miller, 425 U.S. 435, 437-439 (1976). In Miller, the government subpoenaed the defendant's bank records. This Court declined Miller's Fourth Amendment claim as he could demonstrate "neither ownership nor possession" of the bank's business records. Id. at 440. These records were used in commercial transactions and exposed to employees in the ordinary course of business. Id. Because these records were used and generated by the bank, this Court concluded that no personal Fourth Amendment

rights were infringed upon. Id. However, Miller is not applicable to communications content as explained below.

The defendant in Miller had no expectation of privacy in the content of bank records, checks, or deposit slips since it was voluntarily shared with the bank for the regular course of business. Warshak, 631 F.3rd at 288. Warshak distinguished "simple business records" from "confidential communications" such as email. Id. Therefore, Miller is inapplicable to email.

The second case this Court evaluated is Smith v. Maryland, 442 U.S. 735, 743-45 (1979), where the precepts of Miller were applied to telephone communications. This Court determined that phone numbers dialed should not expect to remain private because its used for business purposes, such as routing calls. Id. This Court ultimately held that the use of a pen register which only records phone numbers dialed, did not offend the Fourth Amendment. Id. at 745-46.

Following this Court's framework in Smith, the Ninth Circuit arrived at a constitutional distinction. United States v. Forrester, 512 F.3d 500, 509-510 (9th Cir. 2008). Forrester distinguished pen registers from more intrusive surveillance techniques because "pen registers do not acquire the content of communications." Id. (citations omitted). Phone numbers are shared for the normal course of business for switching equipment to route calls. Id. In this way, IP addresses were distinguished from email content. Like the content of phone calls, email content does not fall under the third party doctrine because that content is not used for business purposes.

This protection remains in tact even if the third-party has the physical ability to monitor or record contents sent by the user. Warshak, 631 F.3d at 285, 287 (citing Smith, 442 U.S. at 735) (telephone communications are protected by the Fourth and Fourteenth Amendment despite ability to monitor or listen). An ISP is the "functional equivalent" of a post office because "emails must pass through an ISP's server to reach their intended recipient." Id. at 286. See also Grand Jury Subpoena v. Kitzhaber, 828 F.3d 1083, 1090 (9th Cir. 2016) ("emails are to be treated like physical mail for expectation of privacy purposes and current possession of the emails not vitiate that claim").

To this end, this Court has said, "few doubt that email should be treated like the traditioal mail it has largely supplanted - as a bailment in which the owner retains a vital and protected legal interest." Carpenter, 138 S.Ct. 2269. (Gorsuch, J. dissenting). Other courts have already recognized this approach. See Ajemian v. Yahoo!, 478 Mass. 169, 170 (2017) (an email account is a "form of property often referred to as a 'digital asset.'"); United States v. Kernell, 2010 U.S. LEXIS 36477, **13-15 (E.D. Tenn 2010) (an individual has a property right to the exclusive use of information and pictures contained in her email account).

Therefore, the fact my emails were bailed to a third-party doesn't matter. I still "enjoyed the same Fourth Amendment protections as [I] d[id] 'when the papers are subjected to search in one's own household.'" Carpenter, 138 S.Ct. at 2269 (quoting Ex Parte Jackson, 96 U.S. at 733).

In my case, the district court simply stated that law enforcement did not intrude into my emails; instead AOL did and provided a "copy of the attachment" that law enforcement viewed. VanDyck, 2022 WL 17689168 at *4. Therefore, there was "simply no warrantless physical trespass." Id. The court suggests that the trespass must be "tangible" property. The theory that copies of a file are not property because the original binary file properties are in the original email account is not supported.

There is no case law that only protects originals. "An individuals copied data on a government-owned hard disk drive is still property of the individual under the data-rights theory." Roderick O'Dorisio, "You've Got Mail!" Decoding Bits and Bytes of the Fourth Amendment After Ackerman, 94 Denv. L. Rev. 651, 672 (2 (2017) ("You've Got Mail!"). Now-Justice Gorsuch stressed that sent "images, video or audio files" are part of the "email," and are constitutionally protected as a sender's papers and effects. Ackerman, 831 F.3d at 1304. There was binding authority that emails had property-based protection. Cotterman, 709 F.3d at 964; see also Joffee v. Google, Inc., 746 F.3d 920, 931 (9th Cir. 2013) (sent email attachments are protected). The district court erred by applying the third-party doctrine.

This finds further support in that email is considered a "virtual container[9] which had Fourth Amendment property and

9) Courts have held for some time that "disk(s)" or "computer files" are containers, and "standards governing closed container files are applicable." United States v. Barth, 26 F.Supp.2d 929, 936 (W.D. TX 1998).

possessory interests. See also Ackerman, 831 F.3d at 1306 (email is a virtual container capable of storing all sorts of private and personal details). This is constitutionally significant because "[t]he act of double clicking to open a previously unopened file is analogous to the act of physically opening a closed container." You've Got Mail! at 674.

Law enforcement violated this protected legal interest. Opening the closed email attachment (file) was like law enforcement opening private mail in my home without a warrant. This Court has warned, "obtaining by [] technology any information [from] the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search[.]. Kyllo v. United States, 533 U.S. 27, 34 (2011) (citation omitted). This is the modern equivalent of common law trespass. Jones, 565 U.S. at 419 ("At common law, a suit for trespass to chattels could be maintained if there was a violation of the dignitary interest in the inviolability of chattels") (Alito, J., concurring) (internal quotes and citations omitted). And "[t]he Fourth Amendment is no less protective of persons and property against govermental invasions than the common law was at the time of founding." Ackerman, 831 F.3d at 1307.

Trial counsel had ample caselaw to support that emails were digital 'papers' and 'effects.' This failure was based on a failure to research and investigate. This error harmed me because absent this excludable evidence, the outcome of my case would have been different.

The lower courts erred because by applying the Third Party Doctrine; they departed from binding caselaw.[10] see Forrester, 512 F.3d at 511 ("subscribers enjoy a reasonable expectation of privacy in contents of emails that are stored with, or sent or received through, a commercial ISP").

Because the courts did not follow binding authority and the appellant court did not acknowledge my property-based argument (unchallenged by the government), I request relief.

B. Law Enforcement Violated My Privacy Rights in Email Content

To determine if a person has an expectation of privacy, this Court crafed the Katz test. To establish an expectation of privacy, you must satisfy two-fold requirement[.] [F]irst that the person has exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361.

At the outset, the district court determined there was no Fourth Amendment search because "there was no reasonable expectation of privacy" in the email attachment because it "contain[ed] child pornography." VanDyck, WL 17689168 at *6. The court acknowledged citizens "generally" have a reasonable expectation of privacy in emails, but here, the mere presence of contraband eliminated it. Id. at *7. Thus, the court retroactively justified the search based on discovery of the contraband. This

10) Miller v. Gamie, 335 F.3d 889- 899-900 (9th Cir. 2003) Banc) (District courts and three judge panels of the Ninth Circuit are bound by prior 9th Circuit authority unless it is clearly irreconcilable with intervening authority from the en banc Ninth Circuit or the Supreme Court).

Court has prohibited this approach. See United States v. Jeffers, 342 U.S. 48, 53-54 (1981) (rejecting the theory that a search tha that uncovers contraband is not a Fourth Amendment search); Wong Sun v. United States, 371 U.S. 471, 484 (1963) ("[A] search unlawful at its inception many [not] be validated by what it turns up").

The presence of criminal activity does not diminish an expectation of privacy. See United States v. Wilson, 13 F.4th 961, 963-64 (2021) (expectation of privacy in email attachment despite child pornography); United States v. Anderson, 154 F.3d 1225, 1233 (10th Cir. 1998) (expectation of privacy in office despite child pornography); United States v. Owens, 782 F.2d 146, 150 (10th Cir. 1986) (expectation of privacy in hotel room despite drugs); Jacobsen, 466 U.S. at 114 (expectation of privacy in box containing contraband prior to private search); Byrd v. United States, 138 S.Ct. 1518, 1529 (2018) (reasonable expectation of privacy in rental car, despite drugs). Because the trial court retroactively justified the search, the entire Fourth Amendment analysis was tainted.

The district court determined the subjective expectation of privacy was lost due to AOL's terms of service "monitoring" policy. The courts opinion does not cite to the record where AOL's monitoring policy is. The Court created a distinction to say, "even if [AOL] did not read the text of emails, it monitored the contents of emails and attachments...." VanDyck, WL 17689168 at * *7. This is a mistake of fact. There is no such language in AOL's privacy policy. Instead it states the opposite: "... when you use

AOL's communication tools, AOL does not read your private online communications without your consent." (2-ER-190). An AOL user would reasonably expect their communications are private. The Court also opined that an emails subject line "please trade," and the email not being marked "confidential" reduce an expectation of privacy. VanDyck, WL 1768168 at *7, 9. However, these findings are contrary to binding caselaw.

A subjective expectation of privacy under the Fourth Amendment is established if "the individual has shown he seeks to preserve something as private." Smith, 442 U.S. at 740 (quoting Katz, 389 U.S. at 351. See also United States v. Chavez, 423 F.Supp 3d 194, 201 (W.D.N.C. 2019) ("courts consider whether the defendant 'took steps to avoid' 'allowing the public at large to access' pertinent evidence") (citing United States v. Borowy, 595 F.3d at 1048.

Steps were made to remain private. The email address was anonymous - associated with no particular person. The account owner - "Kym Doudy" was a pseudonym. Both NCMEC and TPD were unable to determine who owned the email account.[11] The email was password protected - preventing public access. Compare United States v. Morel, 922 F.3d 1, 9-10 (1st Cir. 2019) (no password to protect access to files) or Borowy, 595 F.3d at 1048 (Using a program that allowed widespread public access to folders). There is no doubt steps to remain private were employed here.

11) This anonymity runs contrary to the district court's opinion. VanDyck, WL 17689168 at *9. see also (2-ER-172, 150-51)

The court's conclusion that emails have to be marked "confidential" to be protected also conflicted with binding caselaw. Surely a parcel travelling through the US mail system without confidentiality signage (even with a marking "please trade") would not invite warrantless inspections. Emails should be treated no different. see Forrester, 512 F.3d at 511 (protections of physical mail and email are identical).

As an example, in Walter v. United States, 447 U.S. 649, 651-52 (1980), this Court examined a case where mail parcels were examined by law enforcement with labels on the individual film boxes indicating they contained obscene pictures. Id. There was also suggestive drawings and descriptions of those contents. Id. This Court concluded the warrantless search was "an unreasonable invasion of their owner's constitutionally protected interest in privacy." Id. at 654. The box in Walter provided a lot more inferences of criminal activity than the email's subject line "please trade" in this case. Therefore, I had a subjective expectation of privacy in the email attachment.

Additionally, emails have an expectation of privacy that society is willing to recognize as reasonable. This is because "email, like physical mail, has a package of content that the sender presumes will be read only by the intended recipient. The two forms of communication are identical." Forrester, 512 F.3d at 511. Society would expect that any "subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP." Warshak, 631 F.3d at 288. See also Grand Jury Subpoena v.

Kitzhaber, 828 F.3d 1083, 1090 (9th Cir. 2016) ("emails are to be treated as closed, addressed packages for expectation of privacy purposes"); United States v. Mohamud, 843 F.3d 420, 442 (9th Cir. 2016) (same).

Trial counsel in this case had ample caselaw to support that email content (including this attachment) had Fourth Amendment protections. Forrester, Cotterman, Warshak, and Keith all existed prior to the time trial counsel would have been evaluating his suppression options. Trial counsel's failure to research TPD's illegal acquisition of evidence led to my conviction and was constitutionally deficient.

3. The Terms of Service does Not Reduce an Expectation of Privacy

A. The Terms of Service here, were Not in Effect

The government submitted an AOL terms of service (TOS) in the district pleadings. (2-ER-178-186). However, the effective date on the TOS is September 15, 2014. (2-ER-182). The alleged violation occured March 30, 2014. Therefore, this TOS was not in effect.

The government may argue that I waived this challenge. (see A.B. at 20-21)[12] This is incorrect. I did challenge the TOS in my district court reply: (1) the government provided no proof that I was required to agree to such terms at the time of account creation, (2) the government did not prove that I agreed to "any such terms of service" and (3) no "exact terms of service" was presented to the court. See (FER-16). Because the TOS submitted was post-dated, it was not the "exact" TOS I allegedly agreed to.

12) see Answering Brief (A.B.) [Ninth Cir. No. 23-15198, Doc. 26].

The government was not prejudiced by this challenge and they provided a rebuttal on appeal. Their proposed TOS says, "Effective September 15, 2024, the AOL terms of service and privacy policy will be updated. By continuing to use AOL's online properties, you agree to these updated documents." (2-ER-182) (emphasis mine). Agreements are only binding when they are executed. Therefore, the district court relied on an improper agreement.

B. There was No Announced Monitoring Policy

On appeal, the government avowed throughout their entire brief that AOL's TOS had a "monitoring policy" and that "AOL monitored the contents of emails and attachments." (A.B. at p. 25) (see also pp. 20, 23-25, 28, 30-31, 33, 37). They stressed the district court's adoption of this position. see VanDyck, 2022 WL 17689168 at *9. But neither the government nor the court cite where this monitoring provision is. This significant error impacted the Fourth Amendment analysis in the district court. The Circuit court provided no review.[13]

The TOS provided required a user's "compliance with applicable laws..." to not "participate in, facilitate or further illegal activities;" or "post [] content that contains explicit or graphic descriptions or accounts of sexual acts." (2-ER-182). It also provides that AOL can take "legal" or "technical action" to "prevent," "enforce," "any violations." Id. AOL also prohibits "post[ing] content that is offensive" (listing examples) and to

13) The government may argue the "uncertainty of AOL's policies" fall on me. see A.B. at 21. However, the government relies on AOL's TOS for a warrant exception. See Jeffers, 342 U.S. at 51 (burden is on party seeking warrant exception).

"refrain from activity harmful to [AOL] and [others]....," and any other misuse of AOL's infrastructure." Id. The remaining part of their policy speaks to a user's device compatibility, the ownership of content on AOL's server, trademarks, fee based services, liability and resolutions. (2-ER-183-185). While there are rules against illegal activity and explicit use, no where does it say that AOL audits, scans or monitors for this activity.

Incorporated in the TOS is AOL's privacy policy. One relevant section states that under good faith belief or knowledge of a crime on AOL's platform, contents of online communications may be disclosed in response to legal process. (2-ER-190). But this is no indication of "monitoring." To the contrary, AOL makes this plain in their privacy policy, section: How is your AOL information used," saying, "AOL does not read your private online communications." Id. This is clarified again in the Privacy FAQ: "AOL does not read your private online communications when you use these communication tools without your consent." (2-ER-196). Therefore, there is no impression left to the user that AOL will audit, scan or monitor their private content.

In my Circuit, the Court held an expectation of privacy was maintained where limited instances for access were permitted to protect the university computer's integrity. United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2017). When that Court evaluated the TOS in "their entirety" and found there was "no announced monitoring policy," they held the defendant's expectation of privacy was reasonable. Id. AOL likewise does not have any monitoring policy.

The government will likely argue United States v. Ackerman, 296 F.Supp.3d 1267 (D. Kan. 2017) applies, holding that AOL's TOS reduced an expectation of privacy in email containing child pornography. Similar to my case, the Ackerman district court does not cite any monitoring provision in its opinion. The court supports its ruling on two cases: United States v. Stratton, 229 F.Supp.3d 1230 (D. Kan. 2017), and United States v. Wilson, 2017 U.S. Dist. LEXIS 98432 (S.D. Cal. 2017). However, these cases had clear monitoring language in their TOS.

In Stratton, a playstation network's TOS explicitly said: "[Sony] reserves the right to monitor and record any online activity and communication..." and the user "give[s] [Sony] your express consent to monitor and record your activities." 229 F.Supp.3d at 1233. The district court in Wilson, likewise observed that Google had an "express monitoring policy...." 2017 LEXIS 98432 at *19 and n.6. That is not the case here.

Under Strickland, my district court's application of Ackerman is misplaced. Ackerman was decided after trial counsel would have been preparing his suppression motions. Under the performance prong, the inquiry looks at counsel's perspective at the time the mistake was made. Strickland, 466 U.S. at 689. This case would have no impact on his decision.

The district court erred by concluding AOL informed users of a "monitoring" policy. This tainted the expectation of privacy analysis. The Ninth Circuit conducted no analysis or review. It simply stated trial counsel would have abandoned the warrantless search matter because of "AOL's monitoring policy." VanDyck, 2024

WL 1477398 at *2. However, the concern remains - the court did no not cite AOL's "monitoring" provision from the record and the authority relied upon in their opinion was inapposite.[14]

C. Terms of Service Does Not Affect the Fourth Amendment

A private TOS between an ESP and private user does not reduce an expectation of privacy. If this was possible, ISP's would determine the parameters of the Fourth Amendment; not the Courts. This would lead to an absurd result. This Court has cautioned "that arcane distinctions developed in property and tort law... ought not to cotnrol" the analysis of who has a "legally sufficient interest in a place." Rakas v. Illinois, 439 U.S. 128, 142-43 (1978). The Katz anaylsis is designed to determine "well-recognized Fourth Amendment freedoms," Smith, 442 U.S. at 740 n.5, not the interests of private ESP's with a standard TOS.

Major ESP's such as Google, Microsoft, et. al, maintain, "[t]he Fourth Amendment generally protects a users' reasonable expectation of privacy in the contents of emails held by a Third party service provider from a warrantless search and seizure from the government irrespective of whether the service provider has terminated the user's account or whether the user violates the terms governing his relationship with the service provider." Breif of Amici Curiae, Electronic Privacy Information Center

14) The Court cites United States v. Ganoe, 528 F.3d 1117 (9th Cir. 2008) and Borowy, 595 F.3d 1045 (9th Cir. 2010) claiming there were "express terms notifying users that AOL monitored their accounts and would disclose suspected activity." VanDyck, 2024 WL 1477398 at *2. These cases don't discuss the impact of an ESP's TOS on an expectation of privacy.

United States v. Miller, No. 18-5578, at 6-7 (6th Cir. 2018).[15]

Many courts have declined to allow private contracts to reduce an expectation of privacy under the Fourth Amendment. One court held stating "[a]ll motel guests cannot be expected to be familiar with detailed internal policies and bookkeeping procedures where they lodge." Owens, 782 F.2nd at 150. My Circuit held that a "technical violation of a leasing contract" did not compromise an authorized user's legitimate expectation of privacy in a rental car. United States v. Thomas, 447 F.3d 1191, 1198 (9th Cir. 2006); see also United States v. Walton, 763 F.3d 655, 656-57 (7th Cir. 2014) (violation of rental car agreement does not effect expectation of privacy under the Fourth Amendment).

This Court appears to agree with these Circuit's approach to a private terms of service not impacting the Fourth Amendment. This Court agreed that an unauthorized use of a vehicle "constitutes a breach of a rental agreement, and perhaps a serious one, [but] the government fails to explain what bearing this breach of contract, standing alone, has on expectations of privacy in the car." Byrd, 138 S.Ct. at 1529. This Court admonished, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation. Smith, 442 U.S. at 747. This Court should not permit private agreements to effect the Fourth Amendment. see also Warshak, 631 F.3d at 287 (an ability or right to monitor contents through standard service agreements do not diminsh an expectation

15) https://epic.org/amicus/algorythmic-transparency/miller/us-v-miller-6th-cir-corp-amicus-brief.pdf.

of privacy in email contents).

4. The Private Search Exception Can Not Apply to This Case

The Circuit court erred by concluding trial counsel would have abandoned this claim because the private search exception applied. No authority was provided for this conclusion. The government also argued the private search exception applied. However, these cases were not applicable to my case.[16]

A warrantless search is per se unreasonable under the Fourth Amendment, subject to only a "few specifically established and well-delineated exceptions." Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (citing Katz, 389 U.S. at 357). One of those exceptions is the "private search exception." The Fourth Amendment protects citizens with these types of searches from governmental actors, not private action. Burdeau v. McDowell, 256 U.S. 465 (1921). To distinguish these types of searches, this Court developed the private search framework in two cases: Walter v. United States, 447 U.S. 649 (1980) and United States v. Jacobsen, 466 U.S. 109 (1984).

In Jacobsen, FedEx employees discovered and opened a damaged package, found suspicious bags of powder, and invited law enforcement to inspect the parcel. 466 U.S. at 111. DEA agents repeated the same search: opening the package and inspecting the powder. Id. Additionally, the DEA chemical tested the powder to determine if it was cocaine. Id. at 111-112. This Court determined the initial search was lawful because the DEA

16) The government did not preserve this argument. They only suggested trial counsel may have concluded it applied to my case. No argument was provided. see District of Arizona Case No. 4:21-cv-00399-CKJ, Doc. No. 10 at p. 14 n. 5.

repeated the same search as FeDEx. Id. at 118. However, "[t]he question remain[ed] whether the additional test occassioned by the field test ... was an unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment." Id. at 122. This Court decided it did not because "the federal agents did not infringe any constitutioally protected privacy interest that had not already been frustrated as the result of private conduct. Id. at 126. The chemical test was conducted on powder in plain view.

In my case, the district court applied Jacobsen determining, "[t]he government's conduct at issue in [my] case can only reveal whether an image is child pornography. No other private fact is revealed when the government opens an image reported to it in a cybertip." VanDyck, 2022 WL 17689168 at *11. The court further opined that the government's conduct was based on a limited investigative procedure (like IDFP) and could only reveal that the file at question was illegal. Id. However, the government's conduct here was a warrantless search, not IDFP. Compare Borowy, 595 F.3d at 1048 (detective comparing hash values of files to his own database of known child pornography).

In Wilson, the Ninth Circuit reviewed a case nearly identical to mine. Google used proprietary technology (IDFP) to identify four images of suspected child pornography. Wilson, 13 F.4th at 965. With this technology, Google compared the has values of content uploaded to their servers against a repository of hashes previously suspected to be contraband. Id. Google sent a cybertip to NCMEC which included the four attachments, and NCMEC sent it to local law enforcement who opened it without a warrant.

Id. The Circuit Court concluded the government's search (viewing the email attachment in the cybertip) exceeded "the limits of the private search exception as delineated in Walter and Jacobsen and their progeny." Id. at 971 (footnote omitted). The actual viewing of the image attachment allowed them to determine exactly what the images depicted. Id. at 973-74. Like my case, the "government learned new, critical information that it used to obtain a warrant and then to prosecute [the] defendant for possession and distribution of child pornography." Id. at 972. The Circuit court erred, rejecting binding authority - applying a private search.[17]

Walter much better relates to law enforcement's actions in my case. As explained before, in Walter, sealed packages containing films were delivered to a wrong company, who opened and examined the package, finding boxes with "suggestive drawings" and "explicit descriptions of these contents." 477 U.S. at 651-52. The FBI picked up the packages, and without a warrant viewed the films. Id. This Court held, "the unauthorized exhibition of the films constitutes an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had no consented; and there was no exigent circumstances." Id.

The Keith court agrees, a case directly on point with my issue. AOL detected a hash value match in an email and forwarded a cybertip to NCMEC. Keith, 980 F.Supp.3d at 36-38. Unlike my

17) To reduce confusion, the district court applied Jacobsen (private search exception) in the expectation of privacy analysis. VanDyck, 2022 WL 17689168 at *11. The court erred by applying Jacobsen in the Katz analysis.

case: at the time, NCMEC physically reviewed cybertip attachments prior to forwarding them to law enforcement. Id. at 37. Still, the Keith court explained even if NCMEC had not opened the image but instead law enforcement viewed them first, under Walter, "it could not seriously be contended that the law enforcement agency could open and inspect the contents of the file without regard to the Fourth Amendment's warrant requirement. Id. at 41-42. Keith goes on to explain why Walter is controlling:

> "Although the media in which criminally obscene material was stored are different in Walter and this case, the pattern is the same. A label (here, a hash value) that is examined without opening the film or file, suggested the nature of the contents. For that reason, concerned private parties provided the film or file to the government without first reviewing the contents themselves. Government personnel then examined the contents of the film or file by opening and viewing it. Id. at 42.

Legally, a hash value matching cannot frustrate a person's expectation of privacy.[18] "[M]atching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of a file. What a match says is that two files are identical; it does not itself convey any information about the contents of a file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. Id. at 43.

---

18) The government below argued that AOL's determination method reliability and any gaps in the record to this regard is my burden. (A.B. p. 35 and n.4). The government did not preserve this argument. However, even if they had, it is the government's burden to show AOL's involvement constituted a private search. See Jeffers, 342 U.S. at 51 (burden is on party seeking exception). They did not in this case.

A private party's conduct must "frustrate[] the original expectation of privacy." Jacobsen, 466 U.S. at 117, 126. The files matched by IDFP remain closed and unseen by AOL and arrive that way to NCMEC and law enforcement. "[U]ntil [TPD] viewed the image[], [they] had no image at all; the entire composition was hidden." Wilson, 13 F.4th at 974. No privacy of the attachment was frustrated. This is especially true in the absence of human participation in the hashing and reporting procedure. Only a human can violate another human's privacy interest. If a human doesn't know what software flagged, there is no frustration of privacy. AOL cannot tell you what the suspect file contained, when or why it was hashed. You cannot even reverse-generate a hash into an image. That is why a hash value cannot provide probable cause for a warrant or sustain a conviction.

Hashing is insufficient under the Fourth Amendment.[19] This is why law enforcement continually look at cybertip images, because they don't know for sure if the file is illegal. A physical viewing of the image tells you everything: who, what, where and other details. See Walter, 477 U.S. at 659 n.14 (It was "clearly necessary" for FBI to screen the films because the private party had not, to complete their "law enforcement objectives"). When TPD view these cybertip files, they learn more information "not previously ... learned during the private search." Jacobsen, 466 U.S. at 120. This Court should find that software detection is

19) The government provided no reliability of IDFP, thus presents a Daubert related problem with untested "proprietary" (secret) technology AOL uses. This is relevant to the probable cause determination. Further, the government provides no proof of AOL's employee training in detecting contraband. This raises serious Fourth Amendment concerns.

not constitutionally sufficient to invoke the private search exception to warrant requirements. To do so would put citizens in a vulnerable position for digital trolling by the police.

Below, the government suggested "[J]acobsen illustrates how far offiers may got beyond the initial private search." See A.B. at 29. However, their reading of Jacobsen overlooks the state of two separate searches. See Wilson, 13 F.4th at 978 ("conflat[ing]" Jacobsen's first holding about the private search with this Court's second holding about the field test on "already exposed and seized contraband substance").

In Jacobsen, FedEx (private actor) conducted the initial search, examining and discovering the bags of powder. This frustrated the expectation of privacy in the package. The only remaining thing for the DEA to do was to conduct the chemical test on cocaine bags in plain view. Here, the situation is in the inverse. AOL performed the limited, non-invasive scan of the attachment and police expanded on the search by examing the file contents. Jacobsen simply cannot apply to this case. Trial counsel would have easily discerned this distinction.

The government below likened Rann v. Atchison, 689 F.3rd 832 (7th Cir. 2012) and United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) to my case.[20] In Rann, the victim personally testified that she knew the defendant took pornographic pictures

20) The Ninth Circuit would have rejected the government's reliance on Runyan and Rann because it ignored the Circuit's approach to digital devices and recent decisions from this Court including Jacobsen, Riley, and (listing others). Wilson, 13 F.4th at 977.

of her and gave police the memory card she knew contained the images. Rann, 689 F.3d at 837-38. In Runyan, multiple private searches were done by the defendant's ex-wife and her friends that turned up child pornography on multiple devices. 275 F.3d at 452-53, 463. Police had direct statements from private parties about the content of the files. However, the Runyan court was sure to note that police exceeded the scope of the private search when police looked at disks the private party had not examined. Id. at 464. Here, AOL could tell you nothing about the hash mark or suspect images. These cases are inapposite.

The private search exception does not apply. In the context of the Strickland inquiry, there was no caselaw contrary to my claim to deter trial counsel from running the issue. The Circuit court's finding that trial counsel would have reasonably abandoned the issue is also undermined by his supplemental motion to suppress in state court on the same exact grounds. (FER-46-51).

5. Suppression of Evidence is the Proper Remedy

There was no warrant, no statute, and no binding precedent authorizing TPD's warrantless search of the email image in this case; therefore, suppression is the proper remedy. The government did not argue they are entitled to this exception below.[21]

21) The government may argue that trial counsel may have abandoned the issue anticipating the "fruits of the poisonous tree" argument to fail, and the remaining information in the affidavit would have provided probable cause. (A.B. pp. 34-35). The government did not preserve this argument. However, the district court concluded that absent the image, probable cause would no longer exist. VanDyck, 2022 WL 17689168 at *3. see also Wilson, 13 F.4th at 973 (if search warrant "excised" of "tainted evidence" probable cause would be lacking).

This Court has historically provided an exception to exclusion where an officer reasonably relied on a judge's mislead decision to grant a warrant. United States v. Leon, 468 U.S. 897, 922 (1984). However, this case involves a warrantless search and is outside the context for the basis of the good faith exception.

The only other exception that potentially had relevance to my situation is if TPD had relied on another person's negligent mistake. Herring v. United States, 555 U.S. 135, 147-148 (2009). However, Herring is not applicable here because that officer relied on the county clerk's statement about the defendant having an outstanding warrant, which was based on another law enforcement employees' negligence. However, in my case, it was law enforcement's own negligence that led to the violation of my rights.[22]

The exclusionary rule effects not only the immediate fruits of this illegal search but also the subsequent evidence discovered associated to the illegality or "fruit of the poisonous tree." Segura v. United States, 468 U.S. 796, 804 (1983). "It 'extends as well to the indirect as the direct products' of unconstitutional conduct." Id. (quoting Wong Sun, 37 U.S. at 484.

Here, all evidence in this case originates from law enforcement's initial warrantless search of my email attachment file. The image attachment must be suppressed. With that, all evidence seized must be suppressed that was found in the state

22) This Court has never applied the good faith exception to excuse an officer who was negligent himself, resulting in a violation of a defendant's rights. See United States v. Camou, 773 F.3d 735, 744 (9th Cir. 2014).

and federal search warrant. Further, all statements during the police interviews would require suppression because without the evidence discovered from this illegal search, law enforcement would not have conducted these interviews.

6. The Court Improperly Denied an Evidentiary Hearing

In my Circuit, it is binding law that when a petitioner files a motion under 28 U.S.C. §2255, the district court shall grant a request for an evidentiary hearing "[u]nless the motion and the files and records of the case conclusively show that the prisoner is entitled to no relief. United States v. Howard, 381 F.3d 873, 877 (9th Cir. 2004). This means, "a hearing is mandatory whenever the record does not affirmatively manifest the factual or legal invalidity of the petitioner's claims." Baumann v. United States, 692 F.2d 565, 571 (9th Cir. 1982).

Here, an evidentiary hearing was absolutely warranted. Most importantly, under the Strickland inquiry, the lower courts opined that trial counsel strategically omitted this claim. But in fact, evidence was presented on record that trial counsel did pursue this exact ground in state court after his error was discovered in my direct appeal. The lower courts ignored this evidence. However, I was deprived the opportunity to confirm this in court.

Other important matters should have been resolved in the evidentiary hearing and was not conflicted by an established record. This included the terms of service monitoring language issue and other important matters relevant to the legal issue. This error was plain and effected the fairness of my proceedings.

Therefore, I am also entitled to relief for the lower court's departing from binding authority denying me an evidentiary hearing. Although I do request this Court to grant relief on the merits of my entire petition, I would alternatively request to remand for an evidentiary hearing on the entire grounds.

Conclusion

For the reasons set forth above, I humbly and prayerfully request this Court to grant this writ.

Respectfully submitted this 23rd day of December, 2024.

Ryan Galal Van Dyck
Pro Se Petitioner

No. _____

IN THE SUPREME COURT OF THE UNITED STATES

RYAN GALAL VAN DYCK, Petitioner,

vs.

UNITED STATES OF AMERICA, Respondent.

ON PETITION FOR A WRIT OF CERTIORARI
FOR THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CERTIFICATE OF COMPLIANCE

I, Ryan G. Van Dyck, appearing Pro Se, certify that to the best of my ability this Petition for a Writ of Certiorari complies with the requirements of this Court provided in Rules 32.(g), 33.2 and 34. To my best estimate, this Petition is under 9,000 words, excluding the sections of the Petition exempt under Rule 33.2(b).

Respectfully submitted 12/23/24

Ryan G. Van Dyck, Pro Se Petitioner